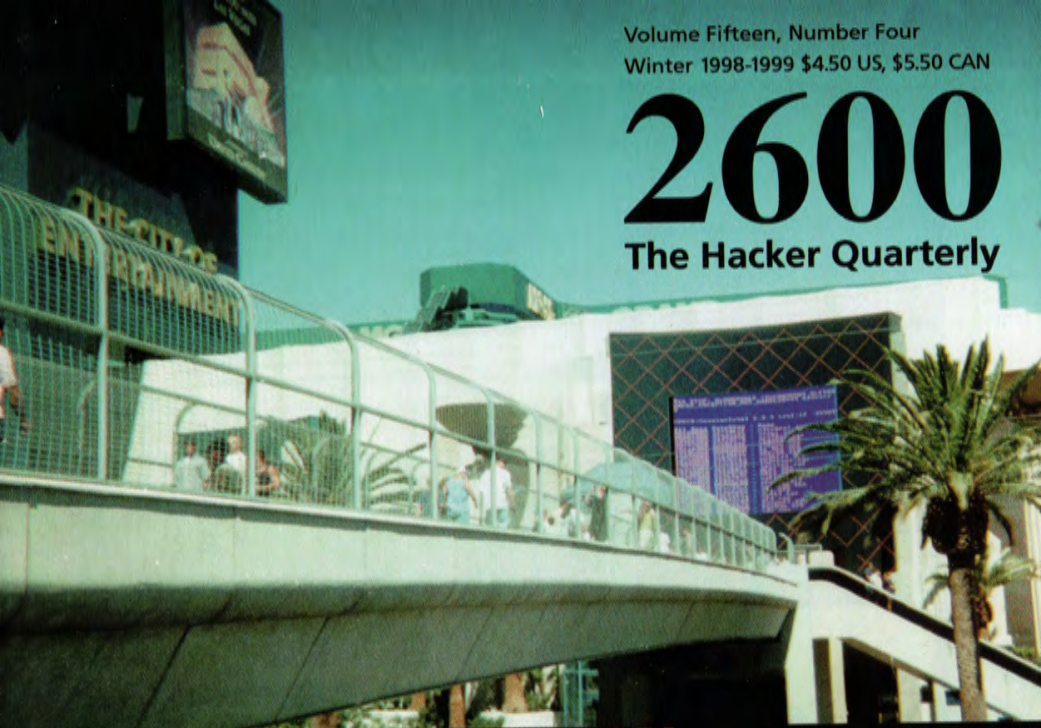
Volume Fifteen, Number Four
Winter 1998-1999 $4.50 US, $5.50 CAN

2600

The Hacker Quarterly



FREE KEVIN

0 74470 83158 7
8 47

"We will not engage in any assaults or hostile physical contact, physical intimidation, verbal threats of physical harm or violence, or any other actions that are threatening or hostile in nature. We will not carry weapons onto company property, in company vehicles, or while conducting company business, even if we have a permit or license to carry them." - Page 17 of the Bell Atlantic Code of Business Conduct.

STAFF

Editor-In-Chief • Emmanuel Goldstein

Design and Layout • Ben Sherman

Cover Design • Szechuan Death, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter
Network Operations • Wicked, Izaac
Broadcast Coordinator • Porkchop
Webmasters • Kerry, Kiratoy, Macki.
Inspirational Music • eno, Edith Piaf, Negativland & The Weatherman, Desmond Dekker, The Shaggs, Mood Setters, Pet Shop Boys, Collapsing Structure
Shout Outs • Zarya

RIP • Tron

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 - $21 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate. Back issues available for 1984-1997 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 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.**

2600

Winter 1998-1999

The Hacker Quarterly

Pearls of Knowledge

The Victor Spoiled

What could possibly threaten the hacker world more than government raids, selective prosecution, Orwellian surveillance, and mass hysteria? The answer will no doubt come as a shock to many. Success.

Success a threat? What kind of insanity is this? Success is what everyone *dreams* about; it's the *goal,* after all.

Well, yes and no. There's a difference between *true* success and *perceived* success. One is a lot easier to come by than the other. And one is a great deal more likely to be obscured.

The unusual problem we face is that much of our curiosity and talent has led to a good deal of marketability. In other words, hackers are now in great demand. This is a rather recent phenomenon. Despite initial misgivings and warnings from people who really never knew what they were talking about, "reformed" hackers are being hired in great numbers by corporate America for everything from system administration to research and development to tiger teaming.

This in itself isn't a bad thing. We've long known that hackers are a great resource and it's certainly a lot better to be hired than thrown into prison. But too often, this allegiance comes at a price that isn't realized until it's been paid.

Hackers tend to be an idealistic lot. Some might even say naive. We believe in freedom of speech, the right to explore and learn by doing, and the tremendous power of the individual. Unfortunately, this doesn't always synch with the corporate world, which oftentimes sees an individual aware of free speech with a desire to explore as their biggest threat.

It may seem like a trivial notion to dismiss this corporate world when it conflicts with your own values. But what happens when you realize you can make a tremendous amount of money because your skills happen to be in demand? Would that be worth... suppressing your ideals a bit? It's very hard to say no. Ideals don't pay the bills and it's not unheard of for high school dropouts to wind up making 100 grand with the talents they've picked up while not attending classes.

Plus, in our money-based society, stature is everything. The more you make, the more of a "success" you are. That is the perception.

But what we define here as true success is so much harder to achieve. To believe in something, to not compromise your ideals, to be at peace with yourself... these are the elements of that success. Yeah, it may sound like a vision left over from Woodstock. But it is an important and an enriching aspect of life. Not very many of us manage to get there and remain there.

The people who have it easy are those who don't have that many ideals to begin with. You'll find them in abundance in politics or the music industry where insincerity and changing what one believes in at the flick of a switch are par for the course. We wish them luck.

Things are so much more complicated in our weird little community where there are people with all kinds of strong beliefs and values. With a combined intelligence and an awareness of where technology is heading, the importance of our perspective cannot be overstated. In the years ahead, we are going to be facing some milestones in human development with regard to free speech, communications, access, and privacy. It will be the equivalent of the civil rights movement, the American Revolution, and the Age of Enlightenment all mixed together. How it pans out will depend in large part on who is around to help steer the course. And that is what's worrisome. Imagine if all of the Cypherpunks were whisked away to Microsoft to work on a high-paying project that took all of their skills and all of their time? Who would make encryption safe from the prying eyes of governments? What if hacker organizations like the L0pht, cDc, or the Chaos Computer Club went out of existence because its members feared losing lucrative corporate positions if it were revealed that they were part of a community of hackers? Who would show the public how insecure Microsoft really was?

The result would be obvious and very sad. We would lose a perspective that we need quite badly at a critical turning point in the world's history. And those people would lose touch with something unique that they would be unlikely to find again.

The simple cliche tells us that money isn't everything. In fact, when looked at objectively, it's very little, in some cases even a negative thing. Finding people who share your true beliefs, expanding your mind, learning and exploring - these are the precious things that can be forever wiped away when success becomes a commodity. In the hacker world, this is doubly tragic as we have so much to gain from each other for an almost indefinite period.

In some ways, what we are facing parallels what has been happening to the Internet. Vast commercialization has completely changed the net's tone in recent years. We see the same corporate powers slowly gaining a stranglehold on every element of connectivity, at the same time merging, engaging in takeovers, and gathering strength. The future of the net as a safe haven for individual thought and independent development of new and competing technologies is very much in jeopardy and this is without even introducing the government's efforts to muck things up. By finding yourself in a position where the money is good but the work is a waste of your brain, you're experiencing a variation of the same thing.

It's a good idea to occasionally ask yourself a few questions such as what is really important to you, what is your definition of real success, and where do you want to be in the future? There are a great number of people who can answer all of those questions with a high-paying corporate career and who have always felt that way. And that is just fine. But then there are the

others, the ones to whom we are addressing this, who face a conflict at some point. It may seem as if the only logical course to follow is to sacrifice your ideals for the sake of materialism, especially when you're young, impressionable, and watching a lot of television. It's what everyone would do - the path of least resistance. Looking out for number one. And most of all, it's what's encouraged in society because idealists are the ones who cause all the trouble.

But there are alternatives. It's not impossible to get the best of both worlds especially if your skills are truly in demand. You can set conditions and draw lines that you absolutely will not cross. You can use some of the money you make to somehow strengthen the community that helped bring you to this point. And, most importantly, you can remain a part of that community and not lose touch with those heading down different paths. The learning process never ends.

We've deliberately avoided mentioning all but the most general goals since everyone has different priorities. The only real common goal we should all share is keeping our community alive in some form and using our gains to advance the future.

And for those who reject the corporate allure altogether, you have a real opportunity to channel your talents to places and people who need them the most. And to do it entirely your way. Anyone suggesting you're a failure for taking this road deserves nothing more than your pity.

Oddly enough, one can actually draw a comparison between this dilemma and credit card fraud. You're young, you can get virtually anything you want if you play the game, and all you have to do is throw away a few of your values, which you may or may not have in the first place. It can be almost impossible to resist, especially if you feel you're owed something. Most people who bow to the temptation of credit card fraud eventually wake up and realize it's wrong one way or another. Far fewer get such a wake-up call from the all-enveloping corporate mentality.

If nothing else, the spirit of hacking can teach you to hold your head up and maintain your values no matter the cost. If you take this approach into the corporate environment, you might even have a chance to change the system from within and make a real difference.

The thinkers and dreamers of our little niche in society have an interesting ride ahead. There will be all kinds of triumphs and defeats and what comes out of all this will change history. It's entirely up to you where your knowledge and skills take you. Not us. Not the Fortune 100. Not any government. You're at the steering wheel. And we wish you *true* success.

Mitnick Update

At press time, the trial of Kevin Mitnick had been moved from January 19, 1999 to April 20, 1999 to allow him time to look at the evidence, which the government had failed to provide by the agreed upon deadline. Oddly, the prosecution was not chastised by the judge for this violation, yet Mitnick's lawyer was scolded for requesting a delay. In addition, it was found that an FBI informant may have had access to the offices of Mitnick's previous attorney with the full knowledge of the government. This action also has not been addressed by the court. What *was* addressed was the fact that a *2600* staffer had requested the financial disclosure documents of Judge Mariana Pfaelzer, something entirely within our rights and a routine method of looking for conflicts of interest among judges. Pfaelzer's reaction, however, was anything but routine, demanding to know from Mitnick who was behind this and implying that something nefarious was going on. No doubt she believes that Mitnick will mastermind the destruction of her financial records by whistling touch tones into a Walkman. It's become rather difficult to believe in the impartiality of this court.

For continued updates, check
www.kevinmitnick.com

Statement required by 39 USC 3685 showing the ownership, management and circulation of *2600 Magazine*, published quarterly (4 issues) for October 28, 1998. Annual Subscription price $21.00.

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	50,000	50,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	42,097	44,070
2. Mail Subscriptions	2128	1880
C. Total Paid and/or requested circulation	44,225	45,950
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	44,875	46,600
H. Copies not distributed		
1. Office use, leftovers, spoiled	5125	3400
2. Returns from news agents	0	0
I. Total	50,000	50,000
Percent paid and/or requested circulation	89%	92%

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

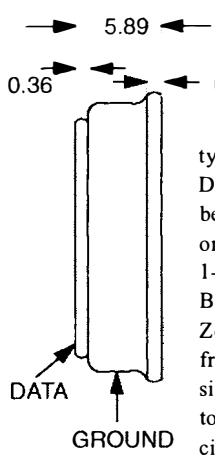
Touch Memory Primer

by Kingpin
LØpht Heavy Industries
kingpin@lØpht.com

Have you ever wondered what those small coin-like devices attached to a person's key-chain or ID badge are for? No? Well, you will. Dallas Semiconductor iButton Touch Memory devices are cropping up all over the world. Used as a replacement for smart cards, barcodes, magnetic stripes, and RF tags, these devices contain a combination of non-volatile RAM, EEPROM, real-time clock, temperature, cryptography, and Java features that are used for applications ranging from debit to access control to medicine tracking. These devices are specified to have 10-year data retention and are housed in a rugged stainless steel can.

Sun Microsystems recently gave away iButton Java Rings to attendees of the Java One conference in California. The ring has 32KB of ROM, 6KB of non-volatile SRAM, a real-time clock, "math accelerator" for RSA encryption, and a Java Virtual Machine. Upon check-in at the conference, one entered data into the ring - personal information and preferred coffee type. Similar to a college ID, one used the iButton for identification and debit throughout the conference. Walk up to the coffee machine, insert your ring, communicate via an encrypted channel, and receive your favorite coffee. One can program their own Java applets into the ring to exchange and store "business card" information or other data. Trivial, yes, but think of what may come. The possibilities are endless.

There are many types of iButtons, allowing for a practically unlimited range of use, but they all have the same underlying technology and all communicate in the same way. This article will give you a basic overview of the functionality and methods of communication with the iButton.



Functionality

The iButtons use a novel type of "1-Wire Interface," created by Dallas Semiconductor, to communicate between the button and the host - a PC or other type of embedded system (see 1-Wire Networking Protocol section). By using minimal circuitry, often just a Zener diode for port pin protection from static discharge and a pull-up resistor, one can easily interface the iButton with a microprocessor. The internal circuitry of the iButton lends itself to

easy, albeit timing-sensitive, communications. The data are both read and written with a single pin plus signal ground. By toggling the direction of a port pin (input or output) on a microprocessor, one can transmit commands, serially, bit by bit, to the iButton and read its responses. The communication protocol is very clever. Dallas Semiconductor actually uses the 1-Wire Interface for some of its other components as well, not just the iButton.

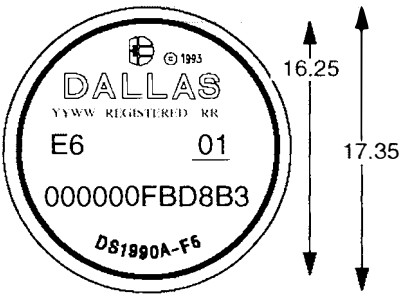
Each iButton, no matter what type, is assigned a 64-bit ID etched into the silicon. It can be broken down in the following fashion:

Family Code (8 bits) • Serial # (48 bits) • CRC (8 bits)

The 1-byte family code identifies the specific type of iButton.

The 6-byte serial number is unique and no two buttons will have the same number. This may lead to Big Brother-type thoughts in your head because of its complete traceablility, but there are actually many instances where the unique ID is necessary.

The 1-byte CRC (cyclic redundancy check) is just that. A checksum. This can and



should be used by the host system to verify proper data transfer.

Currently, this 64-bit number is not a secret. It is printed directly onto the stainless steel case of the iButton. Although it's very helpful for testing and debugging, this may lead to a security problem if identification is based solely on the ID and someone finds a way to "clone" the iButton. Of course, someone could just steal it. As with any security implementation, you want to try and raise the bar to prevent the "ankle biters" from unauthorized access.

Along with the unique ID, each iButton can contain NVRAM, EEPROM, real-time

Part Number	Description	Memory
DS1920	Temperature iButton	16 bits EEPROM
DS1954	Crypto iButton	Secure coprocessor with 6 Kbyte RAM and 32 Kbyte ROM
DS1963	Monetary iButton	4096 Bits NV RAM
DS1971	EEPROM iButton	256+64 Bits EEPROM
DS1982	Add-Only iButton	1024 Bits EPROM
DS1985	Add-Only iButton	16,384 Bits EPROM
DS1986	Add-Only iButton	65,536 Bits EPROM
DS1990A	Serial Number iButton	Not Applicable
DS1991	Multikey iButton	1344 Bits NV RAM
DS1992	Memory iButton	1024 Bits NV RAM
DS1993	Memory iButton	4096 Bits NV RAM
DS1994	Memory iButton + Time	4096 Bits NV RAM
DS1995	Memory iButton	16,384 Bits NV RAM
DS1996	Memory iButton	65,536 Bits NV RAM

Table 1 - iButton Product Selection Guide

clock, or a temperature sensor. See table 1 for a listing of iButton types (graciously borrowed from http://www.ibutton.com/data-apps.html).

You would, of course, choose the iButton that most closely fits your needs. The prices are all relatively cheap and may run between $1.00 and $4.00 if purchased in quantity.

The United States Postal Service has recently started to use the DS1990A Serial Number-only iButton as a replacement for the barcode technology that was used for many years. The iButton can withstand being out in an open environment, unlike a barcode that will rapidly wear. There is an iButton mounted on the inside of every blue mailbox across the country, which is used to easily identify the mailbox and track the movement of the mail. It might also be a way to keep tabs on the postal workers to make sure they retrieve the mail from each of the locations. The DS1990A iButton consists of the 64-bit unique ID only and doesn't support any type of memory. The postal workers carry a portable, pen-sized reader, which records the time and identification of each mailbox along the route.

Operation

There are three basic software routines that are used to communicate with the iButton. There is example code available (see table 3) in assembly language for the Intel 8051 and in C for the PC with a standard UART. Communications with the iButton are half-duplex (either transmitting or receiving, not both at the same time) and extremely timing sensitive. If the system is interrupted during iButton communications, it will fail. For my particular application, I simply disabled global interrupts while the iButton was in action. In some cases, this isn't possible to do, and you'll have to write your code to keep resetting and re-attempting the communication until it finishes undisturbed.

• **TouchReset(void)**

This procedure transmits the Reset signal (480uS low pulse) to the Touch Memory and watches for a presence pulse (low pulse) returned from the iButton (see figure 1). When the iButton is inserted into its socket, it is powered by the 1-Wire Interface. It immediately sends out a "presence

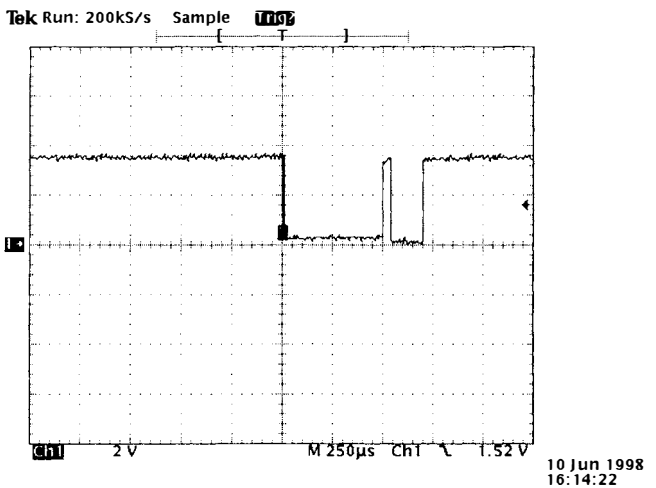


Figure 1 - Touch Memory Reset Pulse and returned Presence Pulse

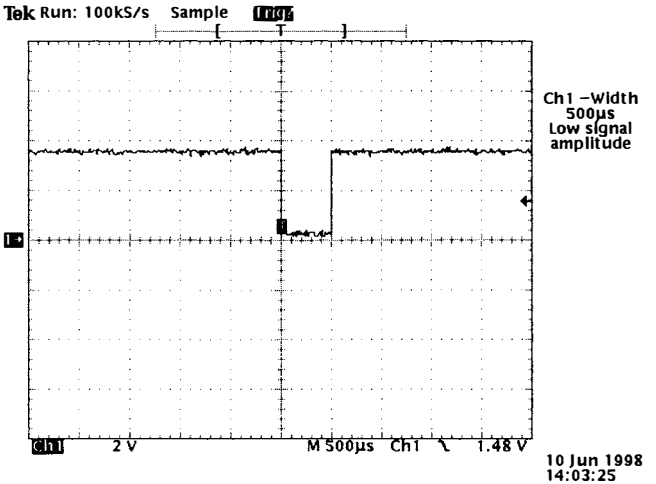


Figure 2 - PulWidth EPROM Touch Memory Programming Pulse

pulse," which says, "I'm here" to the host. This initial presence pulse can be tied to an active-low interrupt line of the processor. Once the presence pulse is detected, the TouchReset() function is called to reset the iButton and confirm that the button is still there and ready for communications. This is similar to debouncing a mechanical switch.

- **TouchByte (unsigned char outch)**

  This procedure sends a byte, outch, to the Touch Memory and simultaneously returns one byte from the Touch Memory to the calling routine. Specific one-byte, iButton-specific commands are transmitted serially, bit by bit, to the Touch Memory (Read ROM, Write to Memory, etc. - see tables 2 and 3). This is the most important piece of the puzzle. Sending and receiving specific commands using this routine will allow complete control of the Touch Memory.

  TouchByte consists of eight calls to a TouchBit routine, which transfers only one bit of information between the host and the Touch Memory. Using a single port pin to both send and receive data fits exactly with the bi-directional port pin hardware philosophy. Configuring the port pin as either an input or output will affect how the data is interpreted by the iButton. The state of the port pin is varied many times during a data transfer.

- **PulWidth (void)**

  This procedure, unused in most implementations depending on the family of iButton, generates a 0.5ms low pulse (see figure 2). This routine is used to generate a programming pulse for the EPROM (one-time-programmable, not erasable) Touch Memory devices.

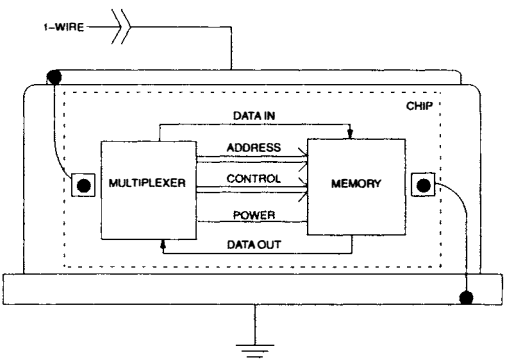
1-Wire Networking Protocol

The Dallas Semiconductor 1-Wire Networking/Interfacing protocol consists of an OSI layered-architecture, similar to TCP/IP or IrDA. The 1-Wire Interface supports having multiple iButton devices on the bus at any given time. It is necessary to look at this protocol, since it defines all of the communications and standards of the Dallas iButton. The following information was taken from the Dallas Semiconductor Book of

DS19xx iButton Standards, which goes into greater detail than what is provided here.

1-Wire Protocol Layered Architecture

- **Physical Layer**
  This layer defines the electrical characteristics, required logical voltage levels and timing constraints of the Touch Memory interface.
- **Link Layer**
  This layer defines the basic communication functions of Touch Memory: TouchReset and TouchByte, described in the Operation section above. Once the iButton responds to the TouchReset command with a Presence Pulse, communication continues with the Network layer.
- **Network Layer**
  This layer handles the commands responsible for identification of the Touch Memory device, known as "ROM Commands" (see table 2). All iButtons support these commands, with the exception of the DS1990A, which support only a subset.
- **Transport Layer**
  This layer handles the commands responsible for non-ROM features of the Touch Memory device - Non-volatile RAM, scratchpad, temperature sensor, and other special functions. Each iButton family supports only a subset of these commands (see table 3) depending on its capabilities.
- **Presentation Layer**
  This layer provides a DOS-like file system supporting functions like Format, Directory, Type, Copy, Delete, etc. This allows the Touch Memory device to be treated like a floppy disk. By using this layer, one can avoid using the "low-level" commands from the Network and Transport layers.



Command	Hex Value	Description
READ ROM	$33 $0F (DS1990A)	Responds with 64-bit unique ID
SKIP ROM	$CC	To broadcast data to all Touch Memory devices connected to the bus
MATCH ROM	$55	To address a specific Touch Memory device on the bus
SEARCH ROM	$F0	All devices on the bus respond with its 64-bit unique ID
OVERDRIVE SKIP ROM	$3C	To set all capable devices to "overdrive" speed and broadcast data to all Touch Memory devices connected to the bus
OVERDRIVE MATCH ROM	$69	To address a specific Touch Memory device on the bus and set it into "overdrive" speed

Table 2 - Basic Touch Memory Command Set

Table 3 - Advanced Touch Memory Command Set

Command	Hex Value	Description
READ MEMORY	$F0	To read one or more consecutive bytes
EXTENDED READ MEMORY	$A5 (EPROM)	To read one or more consecutive bytes with inverted CRC16 response
READ SUBKEY	$66 (DS1991)	To read one or more consecutive bytes from a password-protected page
WRITE SCRATCHPAD	$0F, $96 (DS1991)	To write one or more consecutive bytes to the scratchpad
READ SCRATCHPAD	$AA $69 (DS1991)	To read one or more consecutive bytes of the scratchpad
COPY SCRATCHPAD	$55, $3C (DS1991)	To copy scratchpad data to a location in memory
WRITE SUBKEY	$99 (DS1991)	To write one or more consecutive bytes to a password-protected page
WRITE PASSWORD	$5A (DS1991)	Set the password of a password protected page. Erases all data within that page
WRITE MEMORY	$0F (EPROM)	To transfer, verify, and program one or more consecutive bytes
WRITE STATUS	$55 (EPROM)	To transfer, verify, and program one or more consecutive bytes to the "status memory" section
READ STATUS	$AA (EPROM)	To read one or more consecutive bytes from "status memory" section with inverted CRC16 response

You Want More?

If this article has piqued your interest, which I hope it has, I'd suggest reading through the data books and application notes, which explain the devices more thoroughly than I have.

- **Dallas iButton Home Page**
  http://www.ibutton.com
- **iButton Product Selection Table**
  http://www.dalsemi.com/Prod_info/AutoID/touch.html

You should also read through the application notes for iButton interfacing and standards. You will find timing diagrams and detailed data sheets here. They are available in both .PDF and printed form:

- **App. Note #74 - Reading and Writing iButton via Serial Interface**
  http://www.dalsemi.com/DocControl/PDFs/app74.pdf
- **Book of DS19xx iButton Standards**
- **Automatic Identification Data Book**

An iButton Development Kit is also available, which includes many types of iButtons and sockets and comes with a nice serial port interface and PC software for iButton experimentation. Although not free (less than $100, I believe), it is highly recommended if you decide to do development or take a deeper look into the iButton.

You can talk to and request information from a real human being by calling the Dallas Semiconductor/iButton office at 800-336-6933. Please be nice.

THE FACTS OF SSN

by Kermit the Hog

The social security number (SSN) is a number used by the government to tell us apart from each other, as well as a method of giving us a guarantee of retirement funds.

Many companies now use your SSN as an identification number, and to check with the government to confirm that you are who you say you are.

On to the good stuff: the number 078-05-1120. The SSA used this as a sample number back during ad campaigns, and you can use it too. I'll be using it as an example, but this used to be a popular method of SSN forgery. The IRS and any government official will recognize it, but most people have probably never heard of it.

We'll start with the first three digits: 078. These three digits, the state combo, represents (you guessed it) the state in which the SSN was applied for. 078, if you check on the list below, is within the realm of New York. On to the next digits.

The second set of digits is 05, the group combo. This is just a way for the government to keep track of the SSNs more efficiently. It can also give an estimate of how early in the year the card holder was born.

There is a strict order in which this combo progresses. It begins with odd numbers, 01 to 09, followed by even numbers, 10 to 98. This is usually as far as it goes, and I would never pick a number much more than 50 for the center.

Be wary, though. Try to make your group combo coincide with the birthday that you are using.

A guide would be that 01 to 09 will be assigned, along with 10 to 16 within the first 3 months of the year, usually. 18 to 36 is a good estimate for the next three, and 38 to 50 is an average for the third three months. 50 to 62 is a reasonable estimate for any remaining cards.

But if the last three months are above 50, why don't you recommend those, you may ask. I don't recommend using them because you have no guarantee that the state you are choosing had that many people apply in the year you have chosen. Some years it has gone into the next section, even numbers, 02 to 08, but some years it has only gotten to about 44. I would strongly recommend either trying to get that year's SSN application amount (a difficult task, I am sure) or just staying low and using an early fake birthday.

In preparation for the future, the SSA (Social Security Agency) has created the third and fourth groups, the third being mentioned above (even numbers, 02 to 08) and the fourth, odd numbers, 11 to 99.

The last four numbers in the SSN are 1120. This is just a random sequence. Some believe that they are assigned in order, starting from 1001 and going up. I have not seen, however, any proof of this.

Now that you have an idea of the underlying structure of an SSN, here are the states and their coinciding numbers. The first list is by state, the second is by number.

U.S. STATES

Alabama	416-424
Alaska	574
Arizona	526-527, 600-601
Arkansas	429-432
California	545-573, 602-626
Colorado	521-524
Connecticut	040-049
Delaware	221-222
District of Columbia	577-579
Florida	261-267, 589-595
Georgia	252-260
Hawaii	575-576
Idaho	518-519
Illinois	318-361
Indiana	303-317
Iowa	477-485
Kansas	509-515
Kentucky	400-407
Louisiana	433-439
Maine	004-007
Maryland	212-220

Massachusetts 010-034
Michigan 362-386
Minnesota 468-476
Mississippi 425-428, 587-588
Missouri 486-500
Montana 516-517
Nebraska 505-508
Nevada 530
New Hampshire 001-003
New Jersey 135-158
New Mexico 525, 585
New York 050-134
North Carolina 237-246
North Dakota 501-502
Ohio 268-302
Oklahoma 440-448
Oregon 540-544
Pennsylvania 159-211
Possessions 586
Puerto Rico 596-599
Rail Road Retirement . . . . . .
(valid, but outdated) 700-728
Rhode Island 035-039
South Carolina 247-251
South Dakota 503-504
Tennessee 408-415
Texas 449-467
Utah 528-529
Virginia 223-231
Virgin Islands 580
Washington 531-539
West Virginia 232-236
Wisconsin 387-399
Wyoming 520

NUMERICAL ORDERING

INVALID 000
New Hampshire 001-003
Maine 004-007
INVALID 008-009
Massachusetts 010-034
Rhode Island 035-039
Connecticut 040-049
New York 050-134
New Jersey 135-158
Pennsylvania 159-211
Maryland 212-220
Delaware 221-222
Virginia 223-231
West Virginia 232-236
North Carolina 237-246
South Carolina 247-251
Georgia 252-260
Florida 261-267
Ohio 268-302
Indiana 303-317
Illinois 318-361
Michigan 362-386
Wisconsin 387-399
Kentucky 400-407
Tennessee 408-415
Alabama 416-424
Mississippi 425-428
Arkansas 429-432
Louisiana 433-439
Oklahoma 440-448
Texas 449-467
Minnesota 468-476
Iowa 477-485
Missouri 486-500
North Dakota 501-502
South Dakota 503-504
Nebraska 505-508
Kansas 509-515
Montana 516-517
Idaho 518-519
Wyoming 520
Colorado 521-524
New Mexico 525
Arizona 526-527
Utah 528-529
Nevada 530
Washington 531-539
Oregon 540-544
California 545-573
Alaska 574
Hawaii 575-576
District of Columbia 577-579
Virgin Islands 580
INVALID 581-584
New Mexico 585
Possessions 586
Mississippi 587-588
Florida 589-595
Puerto Rico 596-599
Arizona 600-601
California 602-626
INVALID 627-699
Rail Road Retirement
(valid, but outdated) 700-728
INVALID 729-999

A Guide To VMS'pionage

by EZ Freeze

When the subject of hacking comes to mind, many people think of UNIX shell accounts and the possibilities within. UNIX has always retained a reputation of flexibility and a good starting system for countless new hackers. But a shell account with UNIX is not always the easiest place to start. In my opinion, VMS, in terms of hacking, has been neglected. VMS has the capability for a good deal more security than UNIX, but it remains the case that many administrators don't really understand VMS enough to bring it to its full security potential. In a VMS environment, there are many sources of important information which can give users a wide set of opportunities. Therefore, many ways of guarding these sources can be employed. Here's a simpler way of phrasing this: The bigger the fence, the more valuable the building within it. Pretend that the building's occupants are the server's files. Now what if the fence wasn't put in place? Opportunities for spying and sneaking around the network have been set up, hence the concept of VMS'pionage.

This guide will show you a few ways to exploit a system running OpenVMS and a MultiNet server (or a server similar to MultiNet). This guide is not a how-to on operating or managing a VAX, and does not explain every command affiliated with VAX/VMS. In this guide, I felt it was important only to include and explain commands which can be used to exploit the server the reader plans on hacking. If you want on reading a full explanation of OpenVMS, the Legion Of Doom technical journal on the subject is an excellent resource. It is quoted from in this article. Like many aspects of hacking, simple techniques will be employed to reveal greater results. When reading this guide and using what you've learned from it, there are a couple of essential things to keep in mind. Make sure the administrators are at least relatively lax. Don't try to match wits with admins obsessed with security because you will get caught. OpenVMS keeps many system logs with everything that occurs in the network recorded. You had just better hope that you will only be prosecuted to the full extent of the law.

The first thing you should do is get an estimate of the user population. You can pretty much assess this by using the "finger" command. Use finger at several times of the day, mostly times when you know a good deal of users should be connected (such as lunch and dinner times). Remember, hacking when very few people are on is only a good idea if the network is generally unoccupied. If there are always very few users and the network is not usually maintained, a hack should be a pretty safe bet. But if you're the only one on at one given moment on a normally occupied network, you will definitely stand out in the logs. Also, when you log into some VMS networks, you are informed of which operator is on duty. If this is the case with your target, try to choose a time when there is no operator on duty or when the operator is at lunch (yes, you can be informed of that as well). Once you've burned holy incense or made a ritual sacrifice for good luck, it's time to start.

VMS networks with MultiNet do not often allow anonymous ftp access, since a MultiNet server is structured differently than many others. However, if you have access to an account in the network, you can manipulate the MultiNet ftp process. If you don't happen to have an account, there is a list of default passwords at the end of this guide. If the correct security measures aren't taken, users can view other users' directories. As well as viewing, a user with normal privileges can delete, add, and transfer files to their account. However, a user can usually only access the accounts on their disk. You can find the disk you're in by typing "directory" or "dir" at the DCL prompt, and the disk is usually labeled something like "$DISK(#)". To view all the devices in the network, type "show devices" at the prompt.

The list which will follow is a set of fully functional devices. The disks in a device list usually come first. If a device is active, each column will have an entry and, most importantly, a volume label. If a device is listed but does not contain a volume label, the capacity for the device exists but the device itself was never installed. A listing can exist however, but be marked "Offline" as a status. On a server, sometimes each disk is reserved for a specific purpose. For instance, in a college or university, one disk may be reserved for faculty while another may be marked as student. The following is a transcript of a sample FTP session, illustrating the scenarios described earlier:

```
VMSVAX.LAZYADMINS.COM MultiNet FTP user process V4.0(118)
FTP>VMSVAX.SIMMONS.EDU
Connection opened (Assuming 8-bit connections)
<VMSVAX.LAZYADMINS.COM MultiNet FTP Server Process V4.0(15) at Sat 15-Aug-98 5:58PM-EDT
```

```
VMSVAX.LAZYADMINS.COM>LOGIN
Foreign username: DARKHACK
<User name (DARKHACK) ok. Password, please.
Password:
<User DARKHACK logged into $DISK3:[DARKHACK] at Sat 15-Aug-98 5:58PM-EDT, job 202222e8.
```

This is the user DARKHACK's main directory. DARKHACK's disk is $DISK3. Note: When entering your directory or someone else's, it is received as a non-interactive login. When a user logs into their account, they are presented with the last time they made an interactive (direct login) or a non-interactive login (accessing a directory via FTP, for example). The exact time the directory was entered will show up as a non-interactive login.

```
VMSVAX.LAZYADMINS.COM>DIR
<List started.
$DISK3:[DARKHACK]
PASSWORDS;1                    0  13-AUG-1998 13:40 [ELITE, DARKHACK]
```

This is the listing of DARKHACK's main directory, with the file PASSWORDS;1. The text in brackets indicates ownership. ELITE is the group DARKHACK belongs to; the group $DISK3 is set aside for. DARKHACK is also the file's owner. From here, DARKHACK can view his directory, delete files, and view specific files.

```
VMSVAX.LAZYADMINS.COM>CDUP
<Connected to $DISK3:[000000].
```

000000 is the root directory of $DISK3. From there, a user with normal privileges can enter the directories of any account in that $DISK3. Chances are you will only be able to view the root directory of the disk your directory exists in.

```
VMSVAX.LAZYADMINS.COM>CD GOVAGENT
<Connected to $DISK3:[000000.GOVAGENT].
VMSVAX.LAZYADMINS.COM>DIR
<List started.
$DISK3:[GOVAGENT]
MOSTWANTED;1                   0  13-AUG-1998 13:40 [BIGBROTHER, GOVAGENT]
```

This is the listing of GOVAGENT's main directory, with the file MOSTWANTED;1. The text in brackets indicates the same as the text from DARKHACK's listing above. From here, any user can view the file MOSTWANTED;1, delete it, or download it to their directory.

```
VMSVAX.LAZYADMINS.COM>TYPE MOSTWANTED;1
ATTENTION!
A man going by the alias "DARKHACK" has infiltrated hundreds of VAX/VMS mainframes across
the country. We think he may be residing, with a special file of stolen passwords, in
yours. Your mission is to track him down and bring him to justice! Good luck!
```

This can't be good for DARKHACK! Hopefully, if GOVAGENT hasn't checked his directory yet, DARKHACK can just remove the file and GOVAGENT will never hear about it. GOVAGENT could realize the date and time of the most recent non-interactive login though.

```
VMSVAX.LAZYADMINS.COM>RM MOSTWANTED;1
<File deleted ok, file $DISK3:[000000.GOVAGENT]MOSTWANTED;1.
```

However, if DARKHACK had wanted to warn his friends about GOVAGENT, he could have downloaded the file and then deleted it.

```
VMSVAX.LAZYADMINS.COM>GET MOSTWANTED;1
To local file:
<VMS retrieve of $DISK3:[000000.GOVAGENT]GROUP.;7 started.
```

```
<Transfer completed.  334 (8) bytes transferred.
VMSVAX.LAZYADMINS.COM>
```

If any user with normal privileges wants to try and access the server's root directory (probably without success), simply type the string below. Notice the six zeroes. Those stand for the root directory, and can be found in, for example, the string "$DISK3:[000000]". However, when the zeroes stand alone in a string, this stands for the server's root directory, not the root directory of any disk.

```
VMSVAX.LAZYADMINS.COM>DIR <000000...>
```

If all goes well, a listing of the directory should appear. Security measures can be taken to stop this action though. If these measures have been taken, the string below will replace the directory listing. The string below is also used anytime the user tries to violate their privileges or delve into protected files.

```
<%RMS-E-PRV, insufficient privilege or file protection violation
```

These commands will create a directory with the name specified by the user. This feature might be protected. If this is the case, these commands will only let you create a directory with the same name as the one owned by you, or will only let you create a directory with a different name inside the one owned by you.

```
MKDIR, CREATE-DIRECTORY TEST
257 "$DISK3:[000000.DARKHACK.TEST]" Directory created
MKDIR, CREATE-DIRECTORY TEST
257 "$DISK3:[000000.TEST]" Directory created
```

The following commands will delete a directory from the server. Depending on the security, you may only be able to delete a directory you have created.

```
RM, RMDIR, REMOVE-DIRECTORY GOVAGENT
<"$DISK3:[000000.GOVAGENT]" Directory deleted
RM, RMDIR, REMOVE-DIRECTORY CLASSIFIED
<"$DISK3:[000000.GOVAGENT.CLASSIFIED]" Directory deleted
```

The last section in this article tells you how to hack into someone's directory with stealth. It is very risky, but if the user you're dealing with is ignorant enough, you should be able to pull this off. First log on during a busy night and wait until another user enters the network. Don't even touch a user who's already there. Once you have the potential user, wait until they enter a telnet session or something else which will keep them occupied, particularly with their attention away from their directory. If the user doesn't enter a telnet session within a couple of minutes, move on and wait for another user. Once you have a match, you can enter their directory and read or download files. Make sure not to delete or upload anything, or create any new directories, for obvious reasons. The logic behind this technique is the similarity between the interactive and non-interactive login date and times. If the times and dates of someone's interactive/non-interactive logins are too far apart, the user will be suspicious. But if the dates and times are close enough, some people will just assume the non-interactive login was invoked by some routine command they typed. It might sound ridiculous, but it can work extremely well.

VAX/VMS Default Password List:
(Taken from "The Ultimate Beginner's Guide To Hacking And Phreaking")

Username:	**Passwords:**
SYSTEM	OPERATOR, MANAGER, SYSTEM, SYSLIB
OPERATOR	OPERATOR
SYSTEST	UETP, SYSTEST, TEST
SYSMAINT	SYSMAINT, SERVICE, DIGITAL
FIELD	FIELD, SERVICE
GUEST	GUEST, unpassworded
DEMO	DEMO, unpassworded
TEST	TEST
DECNET	DECNET

Samba
Lion King or Software Suite?

by VmasterX

This article on Samba is meant to teach the everyday hacker more on the SMB protocol and how it relates to the Samba utility suite. (No, it's not just a dance!) I also hope that this article educates you about the basic elements of the Samba suite.

What is Samba?

Samba is a suite of programs designed to allow clients to access file and printer sharing via the SMB (Server Message Block) protocol. SMB, like almost all protocols, is based on the client/server model. Originally designed to run on the standard UNIX platform, Samba now is compatible with NetWare, OS/2, and even VMS (does anyone still really use VMS?). As you can see, this allows Windows and UNIX integration at the file level, which is a constant topic among many system administrators. This means that the Samba suite is capable of redirecting disks, printers, and directories to UNIX disks, printers, and directories and vice versa. SMB can be run with many other protocols including TCP/IP, NetBIOS, and IPX/SPX. Even Samba's LAN manager is a good fix for a LAN running multiple OS's, such as Linux, UNIX, OS/2, Windows for Workgroups, Win95, WinNT, etc. All in all, Samba has been a blessing for many sysadmins.

Key Components of the Samba Suite

smbd: The SMB server. (This needs no more explanation.)
nmbd: Name server for NetBIOS.
smbclient: UNIX hosted client program.
smbrun: The program that enables the server to run externally.
testparms: Tests the server's config file.
testprns: Tests access to a shared printer on the network.
smb.conf: The config file for Samba.
smbprint: a script that enables a UNIX host to print to an SMB server.

Holes in the SMB Protocol

The most commonly and easily exploited hole in the SMB protocol is yet another denial of service (DoS) attack. Any hacker using Samba can simply send the message "DIR..\" to an SMB server on an NT 3.5 or 3.51 machine and it will simply crash. (Obviously a gaping hole that didn't win any new Microsoft fans.) Microsoft has since issued a patch for this problem. The second hole is much less likely to be cracked by your everyday hacker, as it requires knowledge of advanced spoofing methods that are not widely available to many of us. An article entitled "Common Internet File System Protocol (CIFS/1.0)," written by I. Heizer, P. Leach, and D. Perry explains:

"Any attacker that can inject packets into the network that appear to the server to be coming from a particular client can hijack that client's connection. Once a connection is set up and the client has authenticated, subsequent packets are not authenticated, so the attacker can inject requests to read, write, or delete files to which the client has access."

As you can see, such an attack is rarely seen but can prove a significant challenge to anyone willing to try. The fact is: The Internet is full of little holes and glitches just waiting to be exposed. That's what we as hackers do.

Conclusion

All in all, I hope this article explains a few things to you and I hope you may have learned something from it. I know that many hackers out there are fairly uneducated in proper use of the SMB protocol, and some don't even know what it does. This article was written in order to inform the many uneducated hackers about a protocol that can be extremely useful to the educated hacker. Have fun, and happy hacking.

Reference on SMB (Samba)

The RFC entitled "Common Internet File System Protocol (CIFS/1.0)" is available in its entirety at http://www.thursby.com/cifs/file/.

Sys Admin Volume 7, Number 9, explains some aspects of SMB that I may not have touched upon, but they are mainly from a security standpoint. The Samba suite is available at http://samba.anu.edu.au/samba/

As a side note, the suite also includes full source and is a very useful little bundle of software to learn more about the SMB protocol.

COPPER COLOR PAIR CODING

by Catatonic Dismay

When you're in a phone cable that houses 25 pairs of wire or more (sometimes 250 pairs), how do you figure out which wire belongs to the other and which is ring and tip? And why would you want to know this? Well, if you wanted to set up your own junction box in your back yard (for whatever purpose that may serve, and it is not my fault if what you do isn't legal), or if you wanted to tap a line or mingle with the telco staff or pass as one of them, it might be worthwhile to learn a little of this. Now as for the first question, it is quite easy if you commit two sets of five colors to memory. The wires have a main (or a base) color and a stripe (or a secondary). When the main color on the wire is in Column 1, it is ring. When the main color on the wire is in Column 2, that wire is tip.

Figure 1

Column 1	**Column 2**
Blue (BL)	White (W)
Orange (O)	Red (R)
Green (G)	Black (BK)
Brown (BR)	Yellow (Y)
Slate (S)	Violet (V)

"This is all great but how do I find a pair of wire amongst 100 others in the first place?" Well, if you have a wire where the main color is orange and the stripe is black, you would find the wire that has the main color black and the stripe color orange. You now have your ring and tip, respectively. With this system you could have 25 pairs. Now what happens if you get into a cable that has 200 wires making 100 pairs? If you cut off about a foot of the outer covering you would see that a type of lacing or colored twine separates the pairs of wire into four section of 25 pairs of wire (when dealing with phone lines of 100 pairs of course). The cord, or twine, commonly called a "binder," is wound spirally around each section of 25 pairs of wire. In each of the binders you will undoubtedly find one of the wires in Figure 2. In this table notice each pair is given a number.

Figure 2

Pair	**Main-Stripe**
Tip 1	White-Blue
Ring 1	Blue-White
Tip 2	White-Orange
Ring 2	Orange-White
Tip 3	White-Green
Ring 3	Green-White
Tip 4	White-Brown
Ring 4	Brown-White
Tip 5	White-Slate
Ring 5	Slate-White
Tip 6	Red-Blue
Ring 6	Blue-Red
Tip 7	Red-Orange
Ring 7	Orange-Red
Tip 8	Red-Green
Ring 8	Green-Red
Tip 9	Red-Brown
Ring 9	Brown-Red
Tip 10	Red-Slate
Ring 10	Slate-Red
Tip 11	Black-Blue
Ring 11	Blue-Black
Tip 12	Black-Orange
Ring 12	Orange-Black
Tip 13	Black-Green
Ring 13	Green-Black
Tip 14	Black-Brown
Ring 14	Brown-Black
Tip 15	Black-Slate
Ring 15	Slate-Black
Tip 16	Yellow-White
Ring 16	White-Yellow
Tip 17	Yellow-Orange
Ring 17	Orange-Yellow
Tip 18	Yellow-Green

Ring 18 .....Green-Yellow
Tip 19 .....Yellow-Brown
Ring 19 .....Brown-Yellow
Tip 20 .....Yellow-Slate
Ring 20 .....Slate-Yellow
Tip 21 .....Violet-White
Ring 22 .....White-Violet
Tip 22 .....Violet-Orange
Ring 22 .....Orange-Violet
Tip 23 .....Violet-Green
Ring 23 .....Green-Violet
Tip 24 .....Violet-Brown
Ring 24 .....Brown-Violet
Tip 25 .....Violet-Slate
Ring 25 .....Slate-Violet

Experienced linemen know this table by heart (well... some of them). When they talk about pair 22, they're talking about wires orange and violet. If you want to know a lot more than you really need to know (or you want to mingle with the linemen and/or pose as one) than read on.

Pairs of wire are identified sometimes by a number as you have seen earlier. Pair 20 would be yellow and slate. But how do you identify wires by number when there are over 25 in the cable? Remember binders that wrapped around 25 pairs of wire? They are colored to distinguish between them as well. The first binder is blue, the second is orange, the third is green, etc. Sometimes the binders have two colors. The colors follow in the same order as they do in Figure 2. The first binder would be orange and blue, the second would be orange and white, the third would be orange and green, etc.

If there are 100 pairs of wire in a cable and four binders separating them into sections of 25, what would pair 78 be? It would be the third in the fourth binder - or the green and white wires in the brown and white binder.

Yes, this is a lot to soak up in one reading and only someone dedicated to telephony would know this. I don't know what pair 102 would be without a reference. I personally don't really need to know that. If I wanted to pass off as a linemen, I would go through it. Hacking open a cable (please know what you are doing and don't cut into power lines), to tap or whatever it is you're going to do, and finding a ring and pair isn't all too hard with this information.

FREE KEVIN

Get The Word Out!

Free Kevin bumper stickers are now ready to be spread around the planet. It's time the world starts hearing about Kevin Mitnick's plight, locked in prison for over three years without a trial and without being accused of a violent or even financial crime. Enough is enough!

We're selling these stickers at a slightly inflated price of $1 each, **minimum order of 10**, and donating 100% of the money to the Mitnick Defense Fund.

What better way to show your support?

Make all checks payable to Kevin's grandmother - **Reba Vartanian** - and send them to us at:

2600 Bumper Stickers
PO Box 752
Middle Island, NY 11953 USA

DO NOT MAKE CHECKS OUT TO 2600! They will be returned if you do. Also, don't mix this with any other 2600 order or you will cause all kinds of confusion.

a security hole at s-cwis

by Phineas Phreak

From the book *Maximum Security,* published anonymously, I had received the impression that university computer systems were to be among the properly secured systems of the world. I found this impression confusing when I discovered a significant security flaw in the Student Campus Wide Information Service located at the University of Nebraska at Omaha. Especially bad was the fact that the hole I discovered was not inherent in the software but was instead caused by poor administrative policies. This flaw allows unauthorized access to the system by anyone with a minimum of effort and knowledge. Most important is the fact that this flaw shows a poor knowledge and implementation of security that would extend to other campus computer systems and perhaps to the computer systems of other campuses.

The computers at the University of Nebraska at Omaha can be accessed by calling (402) 554-3711 or (402) 554-3434. They can also be accessed by telnet (specific system).unomaha.edu. The s-cwis system is used for students. Cwis is for faculty. Revelation is for library staff Thor is a special system for programming students. The purpose of the zeus system that exists on campus is unknown to me. Telnet s-cwis.unomaha.edu would allow anyone with telnet access into the system because of the security hole, not just UNO students. The other systems are not vulnerable to this specific security flaw as far as I know, but this gaping hole reveals possibilities for other holes in systems maintained by the same people.

S-cwis runs osf1, which is of course BSD with a small amount of system V thrown in for kicks. The shell provided is tcsh (a c shell version). Standard unix services are offered: shell, ftp, lynx as a web browser, tin for newsgroups, pico or fpted for text editing, and pine or elm for mail. Of course, the shell access is most important for the unauthorized user because of the unlimited tasks that a user could make it perform.

When users first get a s-cwis account, their student number is the default password. A good proportion of users never use the service at all, or never again once osf1 unix greets them. If they never use the service or only use it once, good security features such as password aging and reminders to change the password to something other than the student number become ineffective. This hole would not be a big one if student numbers were secret things that just anyone couldn't find out. They aren't. Law states that the university cannot ask for the social security number of a student in order to track them. Instead they use the student number. Curiously, the student number happens to resemble the social security number exactly. Stupid. If you found an account where someone had never changed the password from the original default and you knew the social security number, you would be inside. What if the account has lain dormant for at least 90 days? Well, then it would need a new password. Does this mean you could not access the account? If the password was the social security number then it does not. Enter the social security number and then create a new password. The owner may never sign on again to discover that they cannot access their account.

Discovering users to get social security numbers for is not that difficult. User names are mere name corruptions. Roman Polanski might become polanskr. Brandi Clinton might become bclinton. Seeing as s-cwis accepts finger quenies finding user names should not be a problem. Also, finger reveals much about a user including real name and other such goodies. Sometimes it even reveals the last sign on date. This could be a big clue to accounts that still have the default password on them. If access is already obtained, then one can access the special finger utility. This utility can print whole user name lists. You could search for all users whose user name starts with an a. In this way you could have a list of all the users on the system whose accounts you can attack.

Once you have the login names and the social security numbers (available from such pay sites as http://kadima.com/ or other places that I am unfamiliar with), you're in. Once you're in you have a clear shot at the shell. Only your personal skill level could determine what you could do from there. Lax security can only be cured if the system is forced to change by being breached. I would not advocate breaching the computer, as that would be a violation of law. I also cannot advocate lax security, which is just plainly moronic. Perhaps the administration of UNO will eventually see this. Then they may be forced to bring their systems up to par.

POCKET CONNECTIVITY FOR FRUGAL HACKERS

by Mr. Curious

When the Sharp Zaurus 3500X first hit the market, its list price was a hefty $399. Today, about a year later, it is possible to find a refurbished model for a mere $99. This price drop, which exceeds even Moore's Law of computing depreciation, is due to two things: first, the engineering department at Sharp designed the casing in a chintzy way and the hinge where the machine opens tends to break shortly after opening and closing it a few times (but is quite fixable with superglue), and second, the market is being flooded with assorted handhelds, most of which run the market-heralded windoze CE, the handheld OS of choice for your button-down suit types.

The Zaurus, on the other hand, has an OS all its own - one which is neither great nor horrible, but somewhere in-between But for $99, hackers would be challenged to find a better mobile computing and hacking tool.

The lowdown on the machine, in 50 words or less: size of a checkbook, 2MB RAM (1 MB of that is FLASH, for backup), on-screen drawing, calendar, scheduler, phone book, data bank, outliner, spreadsheet, fax modem, backlit 320x200 monochrome LCD).

The unit's most powerful feature, in my opinion, is the internal 9600/14400 fax modem. Documents can be typed with the built-in, relatively powerful word processor, and sent from anywhere you can find a phone jack. The fax cover sheet setup is very versatile, and documents and images faxed through it come out looking pretty good and authentic - a handy thing to have in your pocket for social engineering, or just a good, old-fashioned prank.

The terminal feature is fairly bare-bones, but practical. It supports speeds of up to 14.4kbps, but the monochrome LCD has trouble keeping up with speeds faster than 4800 baud. It supports vt100 and tty terminals, the former suitable for UN*X sessions. File transferring is limited to ASCII and Xmodem. Combine this portable terminal with the decent backlighting, and you've got a machine that might as well have been designed for clandestine beige-box telecom in some dark alley.

For what it's worth, it also comes with a scaled down version of the Compu-$erve software - which I've never used, but might be handy for somebody who has access to it.

Also, the unit supports infrared data transfer, using both IrDA and ASK protocols. As we're beginning to see infrared appearing more and more in our daily lives (most recently, in parking meters), a feature like this is ripe for street hacking. My current IrDA project is trying to hack my Furby's brain with it.

And where the Zaurus' small keyboard is a bit awkward to use at first, I've developed a six-fingered keying method and I can pump out about 30 words per minute on it. Not blazing, but still a lot faster than one can do with the market-standard of stylus-based character recognition.

The Zaurus runs on two batteries of the ubiquitous AA variety. The manual warns against using NiCad rechargables, citing risks of fire and explosion, but mine hasn't spontaneously combusted in several months of using only them. If you're maxing it out powerwise (using the terminal or fax with backlighting on), the unit works for about four continuous hours... though they last much longer if you just use it for brief sessions in the other, less power hungry programs, like the scheduler, phone directory, database, spreadsheet, or drawing programs.

The data entered into these features are doubly-secure, so if you lose the unit somewhere, it's not an open book of all your deep, dark secrets. It can be set up to require a password (up to 7 digits) at startup - and even then, the unit must be unlocked again in order to show any entries designated as secret. I'm sure that the boys at Sharp have a backdoor password, though.

Unfortunately, the 3500X does not support many of the after-market software and development tools that come with some of the more upscale Zaurus models. Programmability is pretty much limited to the spreadsheet function.

So whereas one can easily find many more powerful handheld computer options, most of them list for six to eight times the cost of the Zaurus. Also, little black boxes tend to be dropped, lost, or have coffee spilled on them sooner or later. It's just a fact of life. So getting into the game with a relatively disposable rig helps there, too.

Oh, I almost forgot. It also has a calculator.

Fun With NetWare 5

by Khyron

Novell has been used for many years as a network operating system. The advantages that it has enjoyed in the past are low hardware requirements, speed, and security.

"In early fall of 1997, Novell successfully completed the National Computer Security Center (NCSC) Class C2 security evaluation of NetWare 4.11, the server operating system included in IntranetWare. As announced on October 7, 1997, NetWare 4.11 is the first "off-the-shelf" commercial operating system to be granted a Class C2 rating under the NCSC's Red Book of network criteria. It is thus approved for use in both government agencies and private sector organizations that require secure network solutions." – Novell AppNotes November/December 97 - "Achieving C2 Security in a Network Environment"

This is a quick overview of what NetWare is, what is changing, and what the current attacks are that can result in damage and or greater privileges to users.

NDS (Novell Directory Services)

NetWare uses a Directory (spelled with a capital D to avoid confusion with the DOS directories, and are dependent upon the machine that they are based upon.) Think of the NDS directory like a telephone directory i.e., the white and yellow pages. Both contain information on where, what, and who. NDS is based closely on the x.500 Directory standard. This allows for users, printers, and applications to log into a Directory rather than an individual PC, server, etc. The advantages to this are many primarily reduced administration because users no longer need logins for every server on a network.

As a side note, Novell has released NDS for NT which allows for the use of Novell's Directory on an NT server (replacing Microsoft's domain structure and brining it into NDS), allowing for one logon, one password.

Pure IP

NetWare 5 has moved from IPX/SPX to TCP/IP as its core protocol. TCP/IP is now a native protocol (although you can still install IPX/SPX as the core protocol). This could create some new and interesting security issues.

The X windows Connection

NetWare 5 has an entirely rewritten kernel from the previous versions. This kernel has support for Java and is able to run JVM (Java Virtual Machines). As such they have been able to port a java version of Xfree86 (X windows for those who don't know). This X windows environment allows java applets, java script, or javabeans to run in the X windows environment. The big advantage (or disadvantage) is that now with the java applet CONSOLEONE, administrators are able to log into, and administer, the NetWare server from the console using a GUI. CONSOLEONE allows the creation,

deletion, and modification of *any* attribute you can manage with NWADMIN.EXE (Novell 4.x's admin utility). An improperly secured server will be an extreme liability. Also with the java console comes the biggest limitations. You need a minimum of 64MB of ram to install and run NetWare using X. Also, it suffers from java's biggest flaw. It is slow. On a Pentium 200 with 128MB of RAM, it took a full 15-20 seconds for the screen to refresh between modifications in CONSOLEONE.

NSS (Novell Storage Services)

NSS is a replacement file system. NSS is based on the Andrews File System (AFS), which is considered to be the most advanced file system in the world. Novell has created 3 terabyte volumes with over 1 billion files on it. NSS only requires 8MB of available RAM, and with this can mount ***any*** size volume, from 1GB to 10TB, in less than one second after a clean shutdown, and less than a minute after a crash, regardless of the number of files contained on it. It is also abstracted from NetWare - in actuality NSS emulates the Novell File System, and because of this abstraction, NSS can and is being developed for AIX, UnixWare, Solaris, and NT. NSS is not installed by default, but Novell has stated that a convert utility will be available with the shipping version of NetWare 5.

BorderManager (IP to IPX gateway)

BorderManager is Novell's Web-caching Firewall product. It allows logins from remote locations to NetWare resources using LDAP (Lightweight Directory Access Protocol). The big advantage to this product would be in the way it can be used to protect NetWare servers from external Internet attacks. The easiest way that this is handled is using BorderManager's IP to IPX gateway. BorderManager talks to your router, ISP, or whatever in IP, and passes this information back to the client.

Security Issues

The default administration account for NetWare 2.2 through 3.12 (the most common flavor found in small businesses and schools, but being replaced by NT and NetWare 4.1x) is supervisor with no password as the default setup. For 4.xx servers the default account is admin, but it requires a password to be assigned at installation time. So there is not much hope of gaining access this way. Or is there?

The best hope is to have physical access to the server. There are many utilities and other nasties that you can do if you have physical access to the location of the server. This is especially true now that NetWare 5 will allow administration and execution of java directly at the server. The burglar NLM (you can find it floating around the flotsam of the net) will allow you to grant *any* account supervisor equivalency rights. This attack exploits a weakness in the logon and netBIOS timings that NetWare uses to access the bindery. Under NetWare 4.x there is no bindery, so the container you are logging into must have its bindery context set. Also, under NetWare 4.x Support Pack 3 or higher (the C2 certified stuff), burglar does not work.

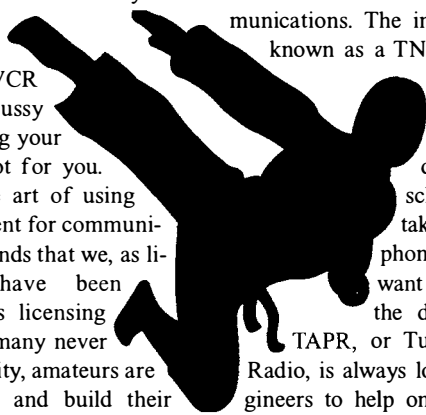
Novell has a ton of good information on how their product works and the security issues that need fixing in their AppNotes. These are available at their web site http://www.novell.com.

become a radio ninja

by Javaman

Recently many of my ninja hacker friends have been asking me for infos on one of my big hobbies: radio, or to be more specific, amateur radio. This article will hopefully dispel some of the myths and shed a bit more light on what amateur radio is all about, from "our" perspective.

Before continuing, I have to say that if you spent more time in front of a keyboard and had no interest in playing with a carburetor, never took a VCR apart, and was just a pussy when it came to getting your hands dirty, this is not for you. Amateur Radio is the art of using and designing equipment for communicating on frequency bands that we, as licensed operators, have been granted (more on this licensing stuff later). Although many never test their technical ability, amateurs are encouraged to design and build their own antennas, pick up soldering irons and whip up devices to help get themselves on the air, and take electric shocks from vacuum tube equipment that needs servicing. Once you have a station together, be it handheld, flowing out of the dashboard of your car, or taking up a corner room in your house, there are several ways to modulate your signals.



As it is today, Amateur Radio operators have developed numerous ways to communicate with each other. The most frequent method seen amongst the script kids of radio (people I consider lame because their lust for knowledge ends at what is superficial) is VHF/UHF FM, which basically means local, high quality voice. Most radio geeks start with this mode as well, as I did myself. After time, different modes of communication grabbed my interest, such as satellite (yes, amateurs have their own satellites), HF Phone, short-wave worldwide communication, ATV or Amateur Television, and packet, or wireless, digital communications.

You can get as deep into any of these facets as you want. Entry level packet radio allows for 1200 or 9600bps mobile communications. The input to the interfaces, known as a TNC, is standard RS232, with the output being either audio tones for 1200bps, or a slightly different modulation scheme that does not take well to the microphone jack. For people who want to spend more time on the digital side of things, TAPR, or Tucson Amateur Packet Radio, is always looking for talented engineers to help on their projects, like a 115kps spread spectrum 900mhz transceiver, using TCP/IP as the underlying protocol. Input to the rig is Ethernet and output is an antenna. For me, that concept is cool as shit. I am a big fan of HF SSB, or worldwide voice communication. During times of good solar activity, I have been able to talk to the remnants of Yugoslavia with little more RF power than it takes to light up a light bulb. Once again, individuals who are hard core into this facet of the hobby may have talked to one person in every single nation on this planet. Morse Code, which is a requirement for higher class licenses, allows you to communicate with very simple equipment. I have seen some Morse Code only transceivers being built into Altoids tins. It's all well and good that cell phones

are that small, but equipment like this was hand built by another amateur. It takes teams of people to design a cell phone. Message boards (think USENET groups) are ripping around the earth right now, available on only the amateur frequency bands. These birds are built by amateurs for amateurs, and it takes a great deal of talent and skill to communicate with these systems.

Some of you may be asking "Yo, why not just buy like CB radios and then we will be cool!" Well, in Amateur Radio, the opportunity to learn about and build a great deal of electronics presents itself. Unlike CB, or Citizens Band, where you must purchase a pre-approved radio that has only 40 channels and allows 4 watts out (that is 36dBm, for those with RF in the blood), Amateur Radio operators are encouraged to build their own equipment, and are permitted to radiate a maximum of 1500 watts in pursuit of long distance communication. Note: This much power is rarely needed, except in moonbounce. Yes, it is possible to bounce your signals off the Earth's largest satellite.

I seem to be getting off track from my main point. The reason why most of us installed Linux, then further installed a BSD variant or BeOS, was to learn about a new OS. This is a hobby that encourages you to design and construct innovative circuits. To build anything permanent, you will need soldering skills. This is not for the weak of heart, or those who think that coding is good since you can't be hurt. You may inflict pain here. This is all in the spirit of learning and innovation. Innovation brings faster methods of communication. Communication is good.

Now, as I mentioned before, you need a license. I realize that half of you rootshell brats are thinking "Bite me Big Brother, I don't want you to track my 12 year old hide with a license, yo, cause I'm leet like dat." The test required to get the license is multiple choice and the question pools are published. (Note: the manuals are available at Radio Shack. The entry level test does not require Morse Code anymore.) You stand to learn more from studying for your amateur radio tests than from a lot of high school physics classes. Don't get a license and you piss people off. Get a license and you learn something and are able to put a good hobby on your resume. Probably the main reason why I have my job right now is because of the road I started upon when I was 14 and receiving my Tech-No Code license.

I realize that I cannot cover all the material that should be discussed, but hopefully this will provide you with a good starting point.

Fire up your copy of Mosaic or Lynx for these URLs:

The largest Amateur Radio club, the ARRL, or Amateur Radio Relay League:
http://www.arrl.org

A good URL for the basics of radio:
http://www.irony.com/ham-howto.html

Tucson Amateur Packet Radio (TAPR):
http://www.tapr.org/

If you are interested in practicing for the tests:
http://www.biochem.mcw.edu/Postdocs/Simon/radio/exam.html

If you have a scanner, here are the frequencies that amateurs are allowed to operate on:
http://www.arrl.org/field/regulations/bands.html

Hopefully I am going to help open a door for some of you. This is another opportunity to learn, and when I was a young one crackin the shit on a C64, that was my only goal.

CABLE MODEM SECURITY

by Fencer
fencer@nudist.org

Cable modems are becoming increasingly popular among the Internet Connected for a variety of reasons, not the least of which is the availability of a cheap, high-speed, high-bandwidth connection on request. I have observed a resonant social reaction within the computer enthusiast community here in the Boston area with regard to cable modems. It's a tired cliche - but we now have the economic reality of the "haves" and the "have not's" respective of cable modem access. Some areas of Boston have it, some do not. The concept of luck really doesn't play into it so much as misfortune, an admittedly pessimistic view of the situation. You either live in an area that has it or you don't.

Along with the surge in popularity cable modems bring, a growing "urban myth" is forming as well. It is widely believed that no cable company installer will install the cable modem if they discover you are running Linux (or some other form of UNIX). This is, in part, true insofar as I have been able to determine through reviewing the advertising material available on the web sites of the various cable companies. Some of them don't allow UNIX. Some don't really say one way or the other, they simply and arbitrarily list Windows and/or MacOS as a requirement. There are a handful, like Adelphia Cable, which list Linux as an acceptable OS, although it may not in fact be. The reason I say this is that when I had the cable modem installed at my office in Plymouth, the installer reacted very oddly to his discovery of a large Linux partition on the computer he was installing the modem on.

The majority of cable TV companies who offer cable modem Internet access use the MAC verification option as their security and identification model. This is a simple process. It is also one of the oldest, and found its origins in token ring networking, though the cable modem networks are not token ring.

Basically the cable modem serves as a bridge respective of the MAC address for the ethernet card in the computer and communication to the node routers. The MAC address is recorded by the central office and is used to identify your system. This is used in place of a login/password process. It saves the cable company time and the hassles of having to help people who forget their password.

Essentially, all ethernet interfaces are hand entered into a database based upon their MAC address as the controlling feature. This is done in the activation phase of the installation - the installer records the MAC address of your NIC and calls it in to the cable company CO. Part and parcel, this database contains the MAC address along with the account and user information identifying that NIC as belonging to you. Amazingly enough, the MAC address is *not* paired to the cable modem, introducing some interesting possibilities for abuse - which I will briefly explore later.

The actual login process works along these lines. The cable modem is switched on first. This needs to happen because the modem itself needs to establish its communications with the domain server in order to be able to synch and forward MAC identification and receive DHCP offers. Once the cable modem itself shows a synch light, you can turn on the PC. Under normal circumstances, the cable modem is supposed to be left plugged in and turned on 24/7 so the order in which the connections are made should never be an issue. When the PC is turned on, it makes its UDP an-

nouncement to the network which triggers the DHCP process request. The request, under normal circumstances, is answered by the domain server with a DHCP offer. The PC will then record the IP number, config up with it and the appropriate subnet mask, etc., and ack the domain server indicating that it is there. Periodically the domain server may or may not send out a change of IP in the form of a DHCP offer. This depends on whether a TTL (time to live) has been set on the original offering. It has been my experience that the majority of cable companies do use TTL's as a method of discouraging the customer from running httpd and ftpd.

This is essentially the cable modem login procedure. Once the IP has been assigned, you are ready to use the Internet through the cable modem. When the IP changes, you will not be informed of it. That is to say, unless you are using an IP watcher (a plethora of these are available from winfiles.com), you will not know that your IP has changed. It is possible to use dynamic domain names with cable modems (see http://www.ml.org/ml/dyndns/ for more information) although this is frowned upon by the provider. All that is left for us is to examine why the cable companies use the MAC address as the security and login control.

Up until recently, the majority of ethernet cards were non-addressable respective of the MAC address. The NIC essentially performs the functions of the first layer of the ISO model - the physical layer. It performs TR and TX, CRC checks, and monitors collisions in order to request resend. That's pretty much it in a nutshell. The more complex job of filtering, reception via destination address, and packet distribution is handled by the OS.

Since the modern cable modem Internet system used by most cable companies is built around head-end systems, the data is moving in restricted spectrums over the same wire as the rest of the cable content. A modern cable modem takes two "TV channels" and converts them into a 10Mbps network. One channel is used to send packets from the head-end to subscribers. The other is used to send packets from the subscriber to the head-end. A standard router is used at the head-end, acting as a bridge between the nodes, and a smart router is used to combine all of the individual nodes into the Internet exchange. Thus you have essentially a physically connected Wide Area Network operating under the principles of Local Area Networks but possibly spanning several hundred miles of cable.

When you factor in the ability of the cable company to limit your use of bandwidth by remote SNMP management of your cable modem, you have a system that is hard to continually abuse. Which means you have to be careful how you behave. Setting up an MP3 site and sucking up a major amount of bandwidth may not cost you your connection, but the cable company might crank down the QOS (quality of service) levels on your modem to prevent you from hogging the bandwidth. The answer to this is simple - don't set up the MP3 site using your MAC address.

The MAC address on older NIC's is a hard-coded address in the PROM. On newer cards and most 10bT/100bT selectable cards, the MAC address can be set using the NIC's configuration software. Upon powering up, the MAC address is recording by the domain controller at the CO, and compared to the database table. If it is found in the table, it is then sent a DHCP offer (an IP address), which is also stored in the database with a TTL entry. In addition to providing basic security that does not require a login server, this process also records hosts that are not in the MAC database. This is useful for flagging accounts that are violating the terms of service. The important thing to remember is that the process does not record which cable modem the request passed

through at the present time.

Think in terms of misconfiguration. To use more than one computer on the cable modem, you have to either run a 95/NT App like WinGate, or you have to configure your Linux/UNIX box as a firewall/router. If you misconfigure it - an example would be using IP forwarding without quenching at the interface - the MAC addresses of the other NIC's on your network might leak to the CO domain server. It would record this event and the path to the unregistered NIC's and you would discover you no longer had service. The cable companies are serious about this. They view any abuse of their ToS as lost profits.

On the other hand, if you intentionally misconfigure it with someone else's MAC, you are them for all intent and purposes. At least as far as the cable company is concerned. Obtaining the MAC addresses of the other subscribers on your *node* is not all that hard, but serious care must be taken while doing this. It has long been thought that a network administrator cannot tell when a NIC has been throw into promiscuous mode, in order to sniff traffic. This is simply not true. There are a variety of ways in which to detect that a NIC has been brought up in promiscuous mode. As a matter of fact, this area is so complex that it really deserves its own article, so I am only going to briefly touch upon this now.

You will want to use a commercial sniffer to obtain MAC addresses. There are a variety of them out there. The one common denominator among them all, whether they are 95/NT based or UNIX based, is that they throw the NIC into promiscuous mode. Depending upon how much snap your cable company has, this might be what gets you into trouble. A large number of cards based upon the DEC (Lance) ethernet model make a UDP announcement when they are brought up in promiscuous mode that is different than the normal one. Some in fact do not broadcast their MAC when in promiscuous mode. Others send a specific ARP - which certain switches and routers are able to detect. The Cisco 2501 and 4000 series are two that are known to be able to detect this. Subsequently you would need to approach this with discretion.

The easiest way would be to use a dial-up connection to the Internet to sweep (scan) the Class C('s) assigned to your node, and than query these using Netwatcher or an NTScope with ARP/RARP ability. Under UNIX you can interrogate the IP address using a variety of free utilities designed for this purpose, and available from sunsite. Build your list of MAC addresses from outside their network so that there is no trail leading back to you inside their network. Once you have your list, it's a simple matter of reconfiguring your Ethernet card with the MAC address of a legit user who is not currently logged onto the network.

If you pick a MAC address that is currently in use, or the person logs onto the network while you are configured as them, that could create a problem. At the very least, it will knock you both off the network, and you will have to fight for the IP address assigned by the domain server. At the worst, the domain server recorded this impossible event, and you can count upon their admin. wondering how that happened and perhaps investigating it.

There are limitless possibilities for exploration here. It is possible to have both your own and the real system up using the same MAC/IP providing you don't originate any traffic on the same ports as the other guy. That would of course mean that anything *he* does will be visible to you and vice versa. That in and of itself is an interesting idea for further study. If I were interested in knowing what you were doing, I might want to develop software to facilitate that type of monitoring. And if I were Big Brother, well... you might start thinking that using encrypted clients is a good idea from now on.

how to handle the media

by nex

I've heard way too many hackers gripe about how the media has screwed us over, which is in fact true, to a degree. But it's not all their fault. We as the subject matter have a duty to represent ourselves in a much better light. So if you don't want to make fools of the hacker community, here are some things to remember when chatting with the public and the media.

When you talk to the media you not only speak for yourself but you also speak for every other member of the hacker community. If you say something that is threatening, inflammatory, or just plain dumb, you make the community look stupid as well.

Ask to see a copy of the article before it is distributed. This is not always possible for the reporter to do but ask anyway. When and if the article is published and you do read it, give the reporter some feedback.

Set rules for what you are going to talk about and not talk about. Understand what is on the record and what isn't. Be perfectly clear about these rules.

Treat the reporter with respect and kindness, no matter how naive and/or rude they are. Live by the golden rule when dealing with the media.

Set up a time and place for your interview that is comfortable for both you and the reporter. Your favorite hangout may not be their favorite place. Show up on time.

Don't threaten the reporter. It's childish activity that only makes you look lame.

Remain cool. This does not mean be an ass or be "elite," or using jargon. It means remaining levelheaded and in control of yourself. Consider your words carefully - saying something inflammatory or threatening will make you look lame and make all other hackers look the same way. Take your time in answering the reporter's questions. The media has a nasty tendency of twisting words; don't let them twist yours.

The media is built on a favor system. Understand and use this. If the reporter is good to you, be good to the reporter. If the reporter is an ass, be a saint, but don't let them walk all over you.

The media is not your enemy. The media is a tool and like any tool it can be used for positive or negative results.

800-555 Carriers

by MSD

After dialing a total of 10,000 phone numbers in the 800-555 exchange, I have come up with a list of numbers with a carrier (that answer with a computer). This took about 50 hours to complete and is as accurate as possible. If you dial and get garbage, try adjusting the baud rate, parity, etc. Hope you have fun.

1-800-555-

5220 4820 9690 0990 4401 2211 8121 7721 1821 6041 6741 6671 8081
3681 6291 7802 8912 3682 8782 0833 9043 4153 5187 4228 9748 7039
7449 1159 3869 8779 5879

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099
or
letters@2600.com

More on "Free" Software

Dear *2600:*

One of my friends works for Software Etc. and attests that reports of employees being able to check out software is true. His store even had a PC in the back with a CD-R to burn copies for people. He also told me that when a software package was returned by a customer, they shrink wrapped it and sold it as new. Only when the carton was damaged did they discount it at all.

Please withold my name.

Dear *2600:*

I am writing in response to the letter in 15:2 written by Greyhare about being able to get software for free while working at Babbage's and Software Etc. I used to work for the company which owns Babbage's and Software Etc. and can confirm that you are correct sir. Allowing the sales associates to take home any piece of software is considered an employee benefit. Under this system, employees are allowed to take home two products but must return them in three days. The product would then be wrapped again and put back on the shelves for sale. This was the system back when I left the company in 95. Another thing to note is that back when I started with the company, software was still primarily on 3.5" floppy diskettes and this policy was in effect. Their belief is that an employee is supposed to remove all the files that were copied or installed when they were finished checking out the software. Now whether it is legal or not I do not know. This does bring up some interesting legal issues because where I live, there are some video stores in the area that rent computer games. Another thing to note is that representatives from the software companies will come to the store and talk to you about their products to try and find out what you know about them. If you're nice to the reps you can receive a full legal copy of their software for either an extremely cheap price ($5 to $10) or even sometimes for free.

Figaro

None of this surprises us. But we find it amazing that organizations like Software Publishers' Association cry bloody murder when anyone else does similar things. SPA is strangely silent on this issue yet they emphatically state that schools aren't allowed to copy software they've already bought and individuals face a $250,000 fine and five years in jail for every piece of software they "illegally" copy. And they're talking about after you already paid for it! After all, they reason, when you buy software, you aren't really buying the software - you are only buying the right to use it! And we all know how Microsoft was crippled by all those people who made illegal copies of their products. Clearly, such policies are greed-motivated. How much money can possibly be brought in from the sale of the same copy of software? And how much will this go up if fear and intimidation are factored into the equation? Fortunately, there aren't all that many people who take these threats seriously - the employee policies of the retailers simply add further evidence to this.

Data

Dear *2600:*

I haven't seen any mention of SCC Communications Corp. in your mag so far. They just went public in NASDAQ under the symbol SCCX. They handle the routing of about 85 percent of the 911 call traffic for North America. Their website is www.scc911.com. The actual street address is 6285 Lookout Road, Boulder, CO 80301. The main number is (303) 581-5600. They have another webserver at www.nrc.sccbldr.com and it appears that they handle file transfers from telcos over this website. This server seems to query a database that has all of the names, addresses, and phone numbers of everyone in America and I suspect that it is directly connected to their network backbone. It is an IIS 4.0 server, has a *guest* account (!!) and is behind

a packet filtering router that only allows ports 80 and 443 through. Their network gateway is at 199.117.205.35 and is obviously a Gauntlet 4.1 firewall. All of this is behind a pair of 3Com Netbuilder IIs (199.117.205.31-199.117.205.33 and 199.117.205.32-199.117.205.34). My demon dialer doesn't find anything useful in the range of the main number, but (303) 581-6037 might be the dial-up to their network. Enjoy.

nobody

Gee whiz. You don't mess around, do you? This is interesting info but it's doubtful that this is part of a database with everyone's phone number. What we found was a list of Public Safety Answering Points (PSAP) - the people who answer 911 calls - throughout the country, as well as lists of regional, local, and wireless carriers. Definitely interesting stuff. Thanks for the pointer.

Dear *2600*:

Check out: www.ameritech.net/users/ghtrout/Telecom_Links_.html. This appears to be a personal web page of a guy named Gene. He has collected an impressive number of telecom-related links that makes it convenient for a beginner hacker like me to learn a lot very quickly.

Mark Milgrom

Dear *2600*:

I just got done reading your article on fake ID's and I have found this site to have very good templates for ID's: www.fakeid.net.

Nighthawk

Dear *2600*:

I'd just like to open by saying that I'm a regular reader of your periodical and think it's great. I find it very interesting. I'm not a hacker although I may well have many of the skills for it. Fear of prosecution keeps me from doing so as it could affect my employment status. I currently hold no less than 800 pages of sensitive documents regarding internal information on one of the largest computer companies worldwide (the name I prefer to keep private for the moment). These documents contain intranet security polices, topographies, configuration, systems administration, etc.

Now you may be asking "what could he possibly want in return for this info?" The answer is nothing. I would be happy to send this to you entirely at my own expense. Disgruntled employees can be such a detriment.

On the other hand, you may have no interest in this documentation whatsoever as it may already be common knowledge to you folks. Whatever the case may be, if you or someone you know has an interest in this, I'll be happy to fedex it in one neat bundle. I figure the section on password policy would be especially interesting.

KC

We'll gladly look at your info. Just send it on in - no need for fedex as they won't deliver to a post office box anyway.

Dear *2600*:

Have you ever wondered what the hell they're talking about? Here's a great resource for DoD and other military organization acronyms: tecnet0.jcte.jcs.mil/htdocs/dodinfo/acronyms/index.html. Another site with info on SIPRNET as well as other DoD standards is: www-library.itsi.disa.mil.

Long live Walter!

Shahn

Questions

Dear *2600*:

How easy or practical would it be for an overseas hub to prosecute a hacker in the states? I assume they could talk with the hacker's local ISP in the states by tracing the IP, but what kind of red tape would they have to go through to actually get anything done?

RavOn

Without knowing specifics, it's hard to be conclusive. If the crime in question is serious enough, foreign governments will cooperate in the investigation and prosecution. While you may not find yourself being shipped to Botswana for prosecution, you could still have federal marshals at your door if you mess around with their power grid. If this is more along the lines of ping flooding some Aussie off the net because he insulted your mother, you may get yelled at or even cut off by your local ISP, depending on how impressed they are by angry people with accents on the phone.

Dear *2600*:

Is it possible to hack a callback system if it is using another telephone line to call out? If yes, how?

analyzer

Contrary to popular belief, it is possible to defeat callback systems. The most obvious method involves simply staying on the line and waiting for the system to dial out, thus intercepting the callback. This obviously only works on those systems stupid enough to use the same line for incoming and outgoing calls and for systems that don't bother to check for a dial tone before making the call. In cases where a different line is used, the same result can be achieved by finding out the number of the outgoing line and dialing into that. Again, this is dependent upon the remote system not checking for a dial tone or an incoming ring. One other method not often thought of is to simply have remote call forwarding installed on the number receiving the call so that such calls can be routed to literally anyplace.

Dear *2600*:

Why is Janet Reno on the cover of 15:2?

smokescreen

Sometimes you have to scare people to get their attention.

Dear *2600*:

Is there really something hidden behind the pay phone images on the back of *2600* like you hint about, or is it just a joke?

Matt

Look behind them and see.

Dear *2600*:

I am interested in a lifetime subscription but I don't want to shell out $260 and then find out that you guys

close down in a year due to WIPO becoming law. So... I guess the question would be what effect will WIPO have on you if it becomes a law?

Keebler

It's an interesting thing about beliefs. If somebody comes along and tells you to alter your beliefs and you obey, then you never really held them to begin with. The time to stick to your beliefs is precisely when someone tells you not to. That's the only time when it really matters. We hope that answers your question.

Dear *2600:*

I went to a nightclub the other night and the security guard had a new ID verification machine. I unwittingly gave my ID to the guard - he "zipped" and up came all of my info. It looked like a Trans330 (credit card authorization box) but all it did was read the mag stripe on the back of my ID and then verify that it was valid. There was also an antenna hanging off the side. So now someone somewhere knows simply that I drink or go out but where does it go from there? Does it know about outstanding warrants or unpaid parking tickets?

the medik

It certainly could if it were programmed to do this. What we need to find out is what information this thing is currently looking for and what records are kept of each query. While it may not be a privacy invasion yet, there is little to prevent it from becoming one in the future.

Dear *2600:*

Is there anything I can do with a mac.

NAME

Somehow we doubt it.

Dear *2600:*

I am an avid reader of *2600* and I am trying to start an underground newspaper at my school to spread alternative information to the students such as how to destroy the school and what to do about teachers who discourage free thought. I was wondering two things: Do you have any tips for a bunch of kids trying to start a newspaper like this and is it OK if we copy certain articles out of *2600* (such as the various "screwing with... store" articles)? Thank you and keep fighting for Kevin!

KLoWN

While being popular obviously isn't your goal, it might be a bit much to define destroying your school as "alternative information." Destroying the fraudulent ideals upon which your fascistic institution is based? That's better. Ask yourself if your goal is to provoke free thought or meaningless confrontation? You're welcome to reprint an occasional article if you put our name and address next to it and send over a copy. But we hope you're doing this to educate people, not to incite them to be malicious. That's not what we're about.

Dear *2600:*

I snail-mailed a letter to you without a return address, and I saw my letter in print in the next issue. My question is was there a reason I was given a new handle and my words edited to say the same first two sentences but the next couple altered? If this is because of monitoring you guys are under and don't want to get your readers in trouble, I understand. But if it's not wouldn't it be just like the censoring your mag is against? If this thing is common just tell me, because it does make sense to safeguard your readers. I'd also like to know if once you've given a reader a handle if future letters are appended with the same handle. And if I'm just dumb and paranoid and your response is that it was another guy's letter, then *why* is the reason why we only see his? You guys don't have to print this but at least reply to this via e-mail.

RANT-o-MATIC

We can't reply individually to letters. Letters are signed with the handles or names that we are given. We don't make substitutions. We have no idea what letter you're referring to so we can't address specifics. We edit for clarity, literacy, and, in rare instances, to protect the writer from revealing something damaging about themselves. It's pretty far from censorship.

Dear *2600:*

Please forgive my last e-mail to your magazine. I was drunk at the time.

RANT-o-MATIC

Dear *2600:*

I am an Office Max employee and the other day an unusual thing happened when I was using their computer system. I went to get a price for a customer and I put in the username and password and apparently they had changed it again. So, being the disgruntled Office Max employee I am, I beat on the keyboard. Somehow I got a UNIX shell in \root\storemax\. So I looked around and found all the files that made up the storemax readonly system. I also found that from the main menu screen if you press F12 and go into utilities, they have an option called UNIX SHELL. I believe this to be a root account but it is password protected. I tried for an hour with everything I could think of. How did I get into the shell and how do I get a root account? If anyone knows the password, please tell. (Nine times out of ten the username is store and the password is also store.)

vsr600

We'll beat on some local Office Max keyboards and get back to you.

Dear *2600:*

I've only been reading *2600* for a couple of issues and have found it to be very informative and well written. I've tried to help out the Mitnick cause by buying shirts, bumper stickers, and passing around information sheets about his situation.

The reason I'm writing is because my parents are total dicks and they don't want me learning all those "illegal things." So the question at hand is: how do I get a subscription to *2600* and keep it out of my parent's grubby hands? If they found out I had it, they'd confiscate it, burn it, burn the ashes... you get the idea. Any suggestions would be helpful.

Envision
Anaheim, CA

We can suggest buying 2600 at a bookstore and hiding it someplace in your house but eventually you're going to have to explain to your parents why you don't see anything wrong with reading this material. Perhaps the work you're doing on the Mitnick campaign may open their eyes on this

front. If you're using knowledge for positive ends, you stand a good chance of getting through to them. It becomes a lot harder if you've got all kinds of devious plots going on.

Dear *2600:*

Is it just a coincidence that Janet Reno's eyes (cover of 15:2) are exactly like those of the "congressman" on the cover of 14:2?

TydiLFluX
Wisconsin

The things people discover....

Radio Shack Antics

Dear *2600:*

I just wanted to comment on the article in 15:3 entitled "Screwing With Radio Shack and Compaq." We tried it at the Radio Shack in our local mall and it was hilarious. The guys at Rat Shack flipped out. It was funny as hell! They were like how the hell?!? We told them to buy the new *2600* and find out for themselves. Thanks.

Jestah
Orlando, FL

Teaching Radio Shack employees how technology works has always been something we've striven for. Thanks for helping to educate them.

Fun on the Phone

Dear *2600:*

If I submit an article, will you notify me in the event that is published or do I have to wait until the magazine comes out? Also, will you notify me if it is not published?

Now, onto the best way (I've found) to spoof Caller ID. All this requires is access to an operator and a calling card. You'll need an operator who will dial 1-800-225-5288 (AT&T). Have the operator dial AT&T for you. You'll get an AT&T operator right away instead of the usual recording. She'll ask for the number you're calling from. You can give any number you want. Now you'll have to use a calling card to make your call. This method works great for revenge purposes. If you have the victim's number, you call, give his number to the AT&T op, then call phone sex or other expensive numbers. He'll have a hell of a time denying charges when they came from his number.

NERO

First, to answer your question, we notify people when their articles are being printed. We don't notify people when their articles aren't being printed but if two issues go by and your article hasn't appeared, it would be safe to pretend that we did notify you to say we weren't printing it. As for letters, your only notification of those is actually seeing them in print. We will be printing your letter in this issue.

Your little phone trick has been around for a while but it doesn't do all you say it does. First of all, this has nothing to do with Caller ID. This method will not change the number that shows up in the called party's CID display. (In all likelihood, since you're going through an operator and/or making a calling card call, the display won't show a number at all.) What you are doing is spoofing the calling number that will show up on phone bills. But you will still need a valid calling card number and the only person who will see the spoofed number is the owner of the calling card. Your trick can be used to implicate an innocent person in calling card fraud since it would appear as if the calling card call was made from their number. The reason this works is because your number isn't passed on to the 800 number when you go through an operator. The AT&T operator who answers the 800 number needs a phone number to process the call and, since the call isn't actually being billed to that number, they generally take your word for it no matter what number you give them.

Dear *2600:*

I picked up my first issue of *2600* not too long ago and I'm already hooked. Recently I was shopping at Lucky's, a supermarket chain, and noticed a phone attached to their in-store ATM. I immediately thought of you guys. The setup in Lucky's is this: The ATM occupies an independent kiosk just inside the door, and attached to the side of the little beige hut is a phone, and two little walls to give you a bit of privacy. Handily, the booth is positioned so no cameras nor any employees can see you, just a steady stream of inattentive shoppers. The purpose of the phone is to give customers easy access to their bank. (Press 1: Bankers on call ... Press 4: New loans... Who takes out a loan from a booth at a grocery store?) I was bored and playing with phones tends to get you in less trouble than rolling watermelons at the elderly, so I had a clear course of action. After pushing random buttons for a while, I hit the zero button five times, and a recording informed me with remarkable enthusiasm, "MCI!" The phone was connected to the outside world, not a direct line to your friendly B of A. From that point on, the phone became a normal phone, same as the one in your house, but brown. (They had wisely blocked 900 numbers.) The other thing was that its built numbers failed to work, so just pushing 4 and hoping to finance that new house got nothing but another recording saying my call could not be completed. I wonder if perhaps Bank of America's "Self Service Center" is a service they forget to check and just let deteriorate over time.

Knotfil

Dear *2600:*

I've recently discovered a neat little trick that works at least on Bell Atlantic pay phones in the 716 area code. I can't verify that it will work anywhere else, though it's worth a try. 10-10-220 offers extremely discounted calls from pay phones. 10-10-220 and then the number rings through and works on local and long distance numbers. I found this the other day while screwing around with a pay phone and tried called someone using 10-10-220. To my surprise it connected without asking for money!

Innominate
Buffalo, NY

Don't be surprised if this stops working.

Religious Advice

Dear *2600:*

I read your magazine and enjoyed most of the information. In light of the attitudes and commentary, I have

several comments.

In the Bible, James 1:16-17 says, "Don't be deceived, my dear brothers. Every good and perfect gift is from above, coming down from the Father of the heavenly lights, who does not change like shifting shadows."

Is hacking a good thing? Are those involved gifted in their computer pursuits? Is the government fickle in the application of the law? Your readership says, yes I believe.

If hacking is inspired and the seed for all our gifts planted by God, why not take the next step and seek the source of the wisdom, knowledge, and understanding you possess?

Patrick

Good idea. When they come for us, we'll just say God is the ringleader of the conspiracy. Get us some more Bible quotes so we can justify this.

Dear *2600:*

Let me set you straight pal, the ICOC is the best church anywhere! My family has been in this church for 10 years and we have devoted our lives to sharing the gospel with other people. The Bible teaches us better then what your web site lets on. I laughed when I was shown your web site and let me say that is the lowest I have seen anyone stoop to get some popularity for a hacker web site. I bet you've never been to a church service. You would understand what we're all about.

Deryc

You do a pretty good job of showing us exactly what you're all about.

Dear *2600:*

I came to www.2600.com and enjoyed looking at all of the hacked pages that you have listed, for I, myself, am a hacker. But upon going into your hacked page, International Church of Christ, I was quite upset at what I found. I am a believer and follower of God and when I saw what you did to the page, I was angered *deeply*. In no way do you have the right to do such a thing to a group of religious people trying to make the world a better place. I have a riddle for you. See if you or your "little hackers" can figure it out: There once was a man, or woman at that... who decided stupidly to do himself a little hack. And what he hacked was something of good nature... and what happened to the man is that he was put at low stature. There was after this, a certain web page forged by the tedious mind of a certain webmaster, and upon doing so, formed himself so much rage put upon a hurtin pastor. Now... who is the webmaster, and what is the web page that the Riddler is referring to? Oh, and send your comments, if you're a *real* man, to *my* e-mail address.

Riddler

We have a riddle for you: Who cares?! Get with it, please. For some reason, none of the people complaining about this page seem capable of grasping the fact that we had nothing to do with hacking it. We just reported it. You were looking at other hacked pages and enjoying them so obviously you have some sense as to how the collection is set up. Or do you believe different rules should apply when a religious site gets hacked?

Scary Stuff

Dear *2600:*

Have you or any of your friends hacked a military site which contained information on neural implants, aka brain/nerve chip? Have any of you guys gone through Los Alamos Labs, MIT, or Illinois Institute of Technology? The reason I ask is because: 1. it's a mind blowing concept; 2. it's a new form of threat for government infiltration of organizations like yours; 3. this supposed device could be injected or ingested (radio pill) without the subject's knowledge.

This is no fantasy. It's real and very dangerous. I would like to get some feedback on this notion that there is some military device capable of monitoring brain neural activity remotely. With the use of a neural network computer program to interpret brain wave activity, the device could then modify, mimic, and provoke behavioral changes in an individual. A virtual computer brain interface via GPS satellite tracking is not unbelievable.

Check: www.au.af.mil/au/2025/volume3/chap02/v3c2-4.htm#implanted_microscopic_chip. This is the best example of what our tax dollars are paying for.

jagxr

Both scary and amusing. This site contains a summary of the Air Force 2025 project which was undertaken by the Air University at Maxwell AFB "to identify the concepts, capabilities and technologies the United States will require to remain the dominant air and space force in the 21st century." Some of the more priceless bits:

"The chip creates a computer-generated mental visualization based upon the user's request. The visualization encompasses the individual and allows the user to place himself into the selected battlespace."

"Why the Implanted Microscopic Chip? While other methods such as specially configured rooms, special helmets, or sunglasses may be used to interface the user with the IIC, the microscopic chip is the most viable. Two real operational concerns support the use of implanted chips and argue against larger 'physical' entities to access the Cyber Situation.

"First, future operations will demand a highly flexible and mobile force that is ready at moment's notice to employ aerospace power. The chip will give these forces the ability to communicate, visualize, and prosecute military operations. Having to manage and deploy a 'physical' platform or room hampers mobility and delays time-sensitive operations. US aerospace forces must be prepared to fight or to conduct mobility or special operations anywhere in the world on extremely short notice although some of these operations may be staged directly from the continental United States.

"Second, a physical entity creates a target vulnerable to enemy attack or sabotage. A highly mobile information operations center created with the chip-IIC interface makes it much more elusive to enemy attack. These reasons argue against a larger physical entity for the Cyber Situation.

"While this is a reasonable portability rationale for the use of chip, some may wonder, 'Why not use special sunglasses or helmets?' The answer is simple. An implanted microscopic chip does not require security measures to verify whether the right person is connected to the IIC, whereas a room, helmet, or sunglasses requires additional time-con-

suming access control mechanisms to verify an individual's identity and level of control within the Cyber Situation.

"Further, survey any group of commanders, decision makers, or other military personnel if they enjoy carrying a beeper or 'brick' at all times. Likely, few like to carry a piece of equipment. Now, imagine having to maintain a critical instrument that allows an individual to access the Cyber Situation, and thus control the US military forces. Clearly, this is not an enviable position, since the individual may misplace or lose the helmet or sunglasses, or worse yet, the enemy may steal or destroy it. These are unnecessary burdens.

"Ethical and Public Relations Issues. Implanting "things" in people raises ethical and public relations issues. While these concerns may be founded on today's thinking, in 2025 they may not be as alarming. We already are evolving toward technology implanting. For example, the military currently requires its members to receive mandatory injections of biological organisms (i.e., the flu shot). In the civilian world, people receive mechanical hearts and other organs. Society has come to accept most of these implants as a fact of life. By 2025 it is possible medical technology will have nerve chips that allow amputees to control artificial limbs or eye chips that allow the blind to see. The civilian populace will likely accept an implanted microscopic chips [sic] that allow military members to defend vital national interests. Further, the US military will continue to be a volunteer force that will freely accept the chip because it is a tool to control technology and not as a tool to control the human."

Injustices

Dear *2600:*

In the August 3rd issue of a rag called *Smart Reseller,* an article was published called "Risky Business." The article is about Justin Petersen, a "reformed" hacker as they put it. They blow text on and on about how he hacked this and that, how he went to prison, how the FBI picked him up as an informant and then they pose the question of would you hire him?

Whatever. The part of the article I find upsetting is that, as they are glorifying this guy's rap sheet, which includes credit card fraud, car theft, and other crimes, they make reference to Kevin Mitnick as "notorious."

Correct me if I'm wrong, but Kevin's alleged crimes are nowhere near the doings of Petersen, and Petersen is now free and working as a consultant! It is a sick judicial world.

wrath

At press time, Petersen had become a fugitive once again.

Dear *2600:*

I usually have trouble at the bookstore buying your magazine. It's usually hard to find because of size, and then when I go to pay for the thing, the people almost refuse to sell it to me because of some "moral ethics and society's downfall" cockNballs bull. I got so pissed at them I went over to the rack to every issue of *2600* (there were many) and I spread them out over every magazine shelf, making it seem like it was the only book in there. After being yelled at, I took up and left. If stores don't want people having the mag, why do they sell it? Anyway, who would I write and bitch to about this store almost refusing the sale?

Toxygenn

If you can stay calm, your letter to the head of the company may actually have an effect on the idiot who tried to inject their morals into you. By interfering with what they do, you pretty much negate that possibility.

Dear *2600:*

I heard some terrible words on the news today. I write to you from Vanier, Ontario, Canada (right beside Ottawa). On CJOH, a local station, this morning's news involved some coverage of gun control hullabaloo taking place on Parliament Hill (our White House, if you will). The anchorman asked a figure on "The Hill" what some concerns were on the registering of all personally owned weapons. Instead of using the precious seconds to speak on the issues of personal freedoms or public safety, the "person in question" (I say as I bite my tongue), said roughly the following: "Well, computer hackers can get into anything these days: the military, NASA, the police computers. So what we worry about is that they will access the computers that we keep these records on. They could find out everyone who has weapons and where they live. Criminals could also find out who doesn't have weapons and go to their houses with a greater degree of security and rob or molest them."

My shock when he said "rob or molest them" was indescribable. To comment on anything other than personal rights in the 15 seconds he had is baffling enough, but I wonder what force was working behind the libelous assault that so stung me, and by extension, hackers as a whole.

We all know that the general paranoia and irrational fear that the media creates is harmful enough as it is. It's already difficult to explain the "thirst for knowledge" principle to someone when all that "hacker" means to them is giving someone phone bills from Australia. On top of being called thieves and criminals, "molesters" is something I think we can do without.

What is there to do but wring our hands in frustration? Our plight goes on.

hex

Olympic Fun

Dear *2600:*

I lived as a resident athlete at the OTC (Olympic Training Center) in Colorado Springs, CO for a couple of years. Keeping the Wrong People Out of the Athletes' Dining Room was a constant issue. They decided to put in a biometric system involving smart cards. We would get measured by the machine that recognized us when we put our right hand on a glass plate in a box, and the machine would also remember a set of dimensions. We also carried smart cards - these were white and a little fat; they merely had to be held next to a sensor to be "picked up" although the machine would often pick up the smart card OK when it was still in your pocket. Nothing's funnier then seeing an Olympic athlete waggle his/her butt at the

machine because their hands are full and they're going into the dining hall and the machine only needs a little help to read the card in their butt pocket. Unfortunately, the only card I "lost" was really lost, so I don't have a sample to send in. Cards are lost often, though, and any hackish readers out there might not find it too difficult to arrange a situation where an athlete simultaneously "finds" a $20 bill and "loses" his/her card. They all carry them, along with coaches and other support personnel. The system works fairly well, unless it's being zorched by the famous Colorado Springs lightning. I do know that the place doesn't have diddly for security, either physical or, I'm sure, electronic. The guy in charge of suckurity is ex-Secret Service, and overall, I would say that personnel there are notable for their lack of sense of humor.

Informagnet

Miscellaneous Mitnick

Dear *2600:*

Hackers of The World Unite. We must find the address of the prison computers in which Kevin Mitnick is being held. Get the best hacker, and have everyone else use their best viruses to bring down parts of the system, then have the hacker hack the security and open the doors leading to his cell. Afterward, crash the power company that the prison uses. This plan is basic, but I think it's possible.

denileofservice

Thanks for the confidence. We'll get a team on it. In the meantime, turn off the TV and introduce yourself to real life.

Dear *2600:*

I don't know how much you all keep up with the news groups and stuff like that, but lately I've seen some posts that just disturb me. Some with titles such as "Screw Mitnick, get your facts straight" and others. The thing that bothers me is that some people don't care what happens to Kevin. They think that defending him is ignorant.

I don't think they understand how this is going to affect them and the people around them. Even if what Kevin did wasn't right and went against the hacker's code of ethics we should still defend him, because whatever happens in this case is probably going to affect all hackers. If the government can keep *anyone* behind bars for more than three years for a non-violent crime, the system is even more fucked up than a lot of people could ever imagine.

In conclusion, slap those "FREE KEVIN" stickers on your car and get the word out because strength comes in numbers and we can't afford to lose.

Anthony T. aka SYCO

What some people fail to realize is that the Free Kevin campaign isn't claiming Mitnick never did anything wrong. But it seems blazingly clear that the penalty so far heavily outweighs all of the crimes he's accused of, let alone the ones that he's actually guilty of. But even if he was guilty of every one of these crimes, it's a very dangerous precedent to lock someone like that away for so long. There's no question that this will come back to haunt all of us if left unchallenged. For that reason and that reason alone, the words "Free Kevin" should have meaning.

Dear *2600:*

I was reading the paper this morning and I stumbled upon an article about the hack that took place yesterday. It was written by Chris Allbritten, and distributed by the Associated Press. I found it amusing (yet troubling) that not only did the article make the overbearing generalization that hackers are malicious, but they forgot to mention the most important fact of the story. While they did state that Mitnick has been in prison since 1995, they failed to mention that he has been there over three and a half years *without* a trial. Man, the press sucks.

TetterkeT

Whenever something like that happens, write to the person who wrote the story and tell them what they got wrong. It may seem fruitless but individual letters do mean something, especially to individuals.

Dear *2600:*

I'm new to computers and the Internet. I was reading the news when I saw an article about the *New York Times*. Then I read why it was "hacked" - because a man named Mitnick is being held prisoner wrongfully. So I put his name in the search thing and then I came to your page and read a bit. How can the government hold a person for over three years if they didn't bring him to trial? What is he supposed to have done and do they have any evidence of whatever? I totally don't get it. Go ahead, call me backward. I don't even know what hackers do! All I know is to beware of viruses and I'm still paranoid about that! (People always say hackers give you viruses.)

exhalibut

Your questions get to the very core of the issues we're involved in every day. Answering them in this small space isn't possible but if you continue to read the facts as reported on our web site and in these pages, you will at least get another perspective on these things. In the end, you will have to decide for yourself who's right.

Dear *2600:*

This is a copy of a letter I sent to NPR's "All Things Considered."

Once again the media has done a disservice to Kevin Mitnick. When I heard tonight's report on the hacking of the *New York Times* web site, I was hoping that for once a mainstream media outlet would tell the whole story. I thought that of all media, NPR would have dug down and reported the actual story, but no. There was no mention of the fact that Kevin Mitnick has been imprisoned for over three and a half years without a trial. If this had been the story of Chinese dissidents imprisoned without a trial we would have gotten all the details. But no mention was made of false imprisonment or the fact that the *New York Times* was hacked due to the unethical behavior of *Times* writer John Markoff. Markoff has consistently written about Mitnick, in both books and the paper, and his struggle with computer security expert Tsutomu Shimomura. Markoff's writing never mentioned that he is friends with Shimomura or that he played an active role in helping Shimomura track down Mitnick. I invite everyone to check the web site of *2600* at www.2600.com for a different view of the story.

Shawn Morris

Thanks for speaking up.

Dear *2600:*

I have just started reading your magazine since spring this year and I have to say that it's worth every penny. Consider my subscription on its way once I get my grant cheque! I would like to pledge my support for your Free Kevin campaign in spreading the word here in England. I'll do my best to see that everyone I know hears about him. Could I suggest that you make a leaflet containing the facts and include it on your web site? That way people can print them out themselves and distribute them. It would make for a good campaign if everyone distributed the same or similar leaflets... people hopefully would see different people shouting the same message and I think it would show some unity within the hacking community.

Timba Wulf

We're already doing this. Clicking on the "Free Kevin" button will bring you to the Mitnick section of our site where you will find flyers to print out.

Dear *2600:*

My mom's been following the whole hacker scene for a while and (surprisingly) she's very supportive. Anyway, she came up with a great idea to get publicity for the Free Kevin movement.

Wherever President Clinton goes people show up to protest. And they get on TV. So whenever the President goes somewhere people should show up with big neon colored poster board that says "FREE KEVIN" in big letters. This would get the info out to a lot of people who wouldn't normally come across it.

Eppie

Not a bad idea. It's getting to the point where "Free Kevin" is being said enough so that, while one person may not know what it means, someone they ask has heard of the case. Getting those stickers up on cars and web pages is more important than ever.

Dear *2600:*

In my Global Issues class which I love so dearly, we're currently on the subject of Civil Rights. So I asked my teacher if she had heard of the name Kevin Mitnick. She said that it sounded familiar, but didn't have a clue. I told her the deal with Kevin Mitnick and she said that indeed was violating human rights. So she gathered up some info on Mitnick and said that it looked fair to her what has happened to him. I showed her a few copies of *2600* and she read all of the Mitnick letters. She still thought he was treated fairly, so I told her to go to your site where she saw the lockdown clock. She said she would look further into Mitnick, but until she was convinced that he was being violated she wouldn't have a discussion on him. So my goal is to get her to tell other teachers about him and have discussions about him so the public is notified about this act of civil rights violation. I encourage all of you students out there to let your teachers know about Mitnick. Maybe one will give a damn.

snachbot

That's really the only way we will get to the majority of people. If you're able to convince a teacher that this is an injustice, you will have an easier time once you start trying to convince more people. Don't give up.

Dear *2600:*

This letter is in response to the article in last month's magazine entitled "Lies." I wish that article could be given to every opponent of the hacker community. Not only did it clarify and further bring to light the issue of Kevin Mitnick but it also defined hacker existence. This article, if expressed to the general public would, in my opinion, diminish the general hate of hackers. I only wish the millions of people who think hackers are just here to give the general public a hard time could read this article. I congratulate you on what I consider a work of art.

Little Bobby

Dear *2600:*

I recently went to Hawaii and I have pictures of places I put Free Kevin stickers. I have one on a customs sign and other cool places. I also have one with a security guard lady holding a sticker. Along the main road on the big island of Hawaii everyone writes things in white stones. I wrote decently large "FREE KEVIN." I took a picture of that too. I think some of these pictures could make some great covers. Is there a specific address where I can send them in to be on covers?

TelePhreak

Just send it on in to our regular mailing address. If it's good enough to be a cover photo, we'll be in touch.

Dear *2600:*

I'm just curious, but do you feel that by going to see *Takedown*, we would be helping those who hurt Kevin? Or do you think that everyone should see it in order to see what's being said by these goons? I'm just curious what you think should be done.

Pago

We can't answer this for you. For one thing, the story isn't over yet so what we say today may not hold true in six months. The one thing we can say with certainty is that you should do whatever it takes to become more educated on the subject. For some people that will involve exposing themselves to things they know to be false. For others it will involve trying to get a different message out. Whatever it is you wind up doing as an individual, be sure that you know why you're doing it and that it's something you really believe in.

Dear *2600:*

This is in response to the massive amount of letters *2600* published in 15:3 about the Kevin Mitnick situation. I personally believe that Kevin should be punished if he did in fact commit the crimes of which he is accused. Also, I do believe that he is guilty of most, if not all of the charges brought against him. As you have repeatedly pointed out in your magazine, everybody is entitled to their own opinion and this is mine.

As for my response to the way he has been held for so long, I believe that he should have been released, charged, or given bail by now. But what *2600* does not seem to want to point out is that, in reality, it seems he has committed some serious crimes (not as serious as murder, rape, etc., but serious nonetheless) and he should be punished for them. Once he is actually tried in the US court system, I am certain that he will be sentenced to time served and will be released.

Concerning your response to Malkor's letter, the credit card file was in fact distributed to many many peo-

ple around the Internet, but that does not provide any evidence whatsoever that one of those numbers was ever used by Kevin. Kevin's pleading guilty to having cellular MINs and using them to make unauthorized phone calls is exactly the same thing as stealing something tangible because he stole money from the owners of those MINs. That in no way is making "real theft" more excusable because that is "real theft." If Kevin did not realize that he could simply go out of his way to use a pay phone and call whomever, then that is his own fault.

Over the past few months, your zine has become more of a "Free Kevin" banner than a magazine for hackers. I say we get back on the subject. Sure, updates on the Mitnick case are greatly appreciated but there is no need to devote more than five pages to this subject especially when the space could be better used to write about more interesting topics.

Jade

Well, we've given you space to speak on the subject, so others should be allowed to give their views as well. The Mitnick case is by far the most important issue facing the hacker community right now. We focus on plenty of other things in a typical issue - this subject tends to leap out and stick in the minds of our readers. This is a good thing. We would debate the MIN issue with you but it's no longer an issue. Kevin pleaded guilty to this and has long since served the penalty for it. So let's get back to the real matter at hand - namely why he is still being held.

Dear *2600:*

Hey, just wanted to let you know that I've handed out a little over 1000 flyers to help support Kevin Mitnick. All of us down here in Indiana are in his corner. I'm doing everything I can to get the word out about Kevin.

DaRkSiDe
Richmond, Indiana

We all appreciate it.

Dear *2600:*

First off, I'd like to say that when I got your last issue and discovered the Free Kevin sticker inside I immediately taped it in my car's back window (I didn't want to face having to scrape it off when Kevin is freed). I can't count how many times I've had to explain the saga of Kevin Mitnick to the curious. I've actually had people pull next to me in traffic and ask who Kevin is. I've been stopped in the school's parking lot and asked who Kevin is. (Fortunately, I haven't been harassed by the cops.) In fact, I got so sick of repeating myself that I was on the verge of taking it down when 15:3 arrived and re-inspired me. I figure I've educated about two dozen people (at least) about Kevin, and gotten mostly favorable responses. When my car's drive pulley fell off (don't ask) the tow truck driver reacted to my story by saying that KM should be released on time served, since what he's been put through is the equivalent of 10 years of regular prison time in his opinion. While I was explaining KM's story to him somebody walked by and said "I pass by this car every day - who's Kevin?" I had at least one person promise to pray for him, for what it's worth.

Desaparecido

We know it's a pain in the ass to constantly explain this to people. But it's through people like you that we are reaching so many others. Mass awareness is the best shot we have of ending this nightmare and preventing others. Thanks for the effort.

Dear *2600:*

I would first off like to thank you for existing. The more I read and hear every day, everywhere, from the newspaper to the 6 o'clock news to my telephone bill, it makes me happy you people are around to sound the klaxon that all is not right with the world. I am glad that you are there to warn us that if more people don't wake up to the fact that everything is not as "American" as the U.S. government would like us all to believe, then things are only going to get worse. Things like the Bill of Rights, innocence until guilt is proven, freedom from unreasonable searches and seizures, speedy trials, and free speech will be concepts our grandchildren will not even know enough to ask us about. I for one do not want to live in an America where people can be held for four years without a trial.

In that spirit please expect, under separate cover as requested in 15:1, a check in the amount of $100.00 payable to Reba Vartanian to help defray Kevin's legal defense costs by purchasing 100 Free Kevin bumper stickers. After four years the matter of his guilt or innocence is of minimal importance to me. I want the man to have a (dare I hope, fair) trial. I also hope that the government's appetite for revenge on this man is sated by the time the trial takes place. If not found outright innocent, then if there is any justice left in America at all, the conditions of his sentence will be met by time already served.

I imagine many of you have heard about Amnesty International's inclusion of the U.S. in its list of countries with governments engaging in human rights abuses. Kevin's case certainly qualifies in my eyes. I plan on sending them a check, too, with a short note asking them to do anything they can on his behalf. On that note, has anybody approached them for possible help? I'm sure they have their hands full here in the U.S. with protesting the death row cases, but they might be able to give Kevin and his supporters a few ideas on how to set up mailing campaigns, fundraisers, etc.

I also want to let you know that I, for one, enjoy and appreciate your magazine carrying a political message like you are. Malkor (15:3) says that *2600* should "get back to... inform, educate, and entertain." Well, what could be more informing than pointing out injustice? What could be more educational than teaching about freedom and privacy? And what could be more entertaining than reading letters written by nanocephalics like Malkor? I'd like to take a second to touch on one of the items that Malkor mentions: the credit card file. Why is it that multimillion dollar companies like Lexus/Nexus, basically an information fencing company, are allowed to legally amass and trade in massive databases of credit card numbers, social security numbers, and cardholders' mother's maiden names, and yet Kevin, who in all likelihood copied a list of card numbers off the net out of sheer curiosity, is held in jail four years without a trial or bail?

Baaaa
Waltham, MA

Fingerprinting

Dear *2600:*

This letter is in regards to "Fingerprinting at the Precinct" (15:2). The IMC describes in his article the Identix fingerprinting system used by the NYPD, among others. He mentions that, upon performing a system reboot - with much help from the IMC - the officer entered the login NAMIS and the password MORPHO. I took a look at the company's website and, while browsing their press releases, discovered that Morpho is an authorized reseller of Identix's! It's quite obvious that the login and password had never been changed from the default! The very competent NYPD obviously realized the pointlessness of such a maneuver. Who'd ever want to fuck with them? After all, they're the police! (The site is at www.identix.com/corporate/news/1998/may2898.htm)

The Fryar

Nice catch.

Barnes & Noble Feedback

Dear *2600:*

I have been a reader of your magazine for a long time and I greatly enjoy it, but I am disturbed by the many negative letters I have read in your letters column regarding Barnes & Noble and "big bookstore chains" in general.

I've worked for Barnes & Noble for over two years and since my earliest times at work, I've always seen *2600* available in our magazine section. Because of the limited space that we have, a few copies of each magazine are always put on the shelf and extra copies are either put below in large wooden drawers, or are kept at the magazine station in receiving. When any title sells out, the magazine coordinator goes below to the wooden drawers and puts more up on the shelf. More copies can also be found in the back. Each store has a magazine coordinator, so if you would like a copy of *2600,* all you need to do is speak to that particular individual and ask for one. The coordinator always has vast quantities of magazines to maintain. It is one of the biggest jobs in the store. If any customer doesn't see *2600* (or any other magazine) on the shelf please just ask.

J.A. Hasse

We couldn't agree more. The problem comes when the magazines never make it out onto the stands from those wooden drawers or equivalents. This happens everywhere, not just at your chain. It's awfully frustrating when people contact us to complain about our issues not being at a certain store, then that same store claims a credit for 50 unsold issues.

Dear *2600:*

This letter is in reference to the "newsstand updates" in the summer 98 issue of your wonderful magazine. It is directed towards "Javelin." I would just like to say that I also work in a Barnes & Noble in the Midwest, and when a magazine is placed in the drawers below the racks, that *does not* mean that we don't want people buying the magazine. Extra copies that don't fit on the shelf go there. At the time Javelin came in to buy a copy, I'm sure that the last copy on the shelf had sold out recently and nobody had a chance to put any others out. It is painfully obvious that Javelin has *never* worked in a retail establishment because of the harsh way (it seemed rather uncalled for to me) he treated the employees. It *is not* the policy of *any* Barnes & Noble to censor what the public is reading.

Bendar the Barbarian

Dear *2600:*

I work for Barnes & Noble (I am a head cashier at one of their superstores) and I can guarantee that there was no corporate edict telling us to remove *2600* from our shelves. I love reading in your letters pages all of the people claiming that such and such store is hiding *2600*. There are easier ways of keeping people from buying a mag. The store just has to stop carrying it. There is no nationwide conspiracy to keep "you" from finding the newest issue of *2600*. Customers mess up the shelves and put magazines in front of other mags. This is why you are having a hard time finding it. No other reason. We proudly display our copies of *2600* in the computer section (of Magazines) on the front shelves. Unfortunately, customers check out the section, grab a mag from the back of the display, and are too lazy to put it back where it came from. So they leave it out on the front of the display.

As for your innocent act about publishing the letters about the WINGS system (B&N's computers), publishing that information can and probably did cost the company quite a bit of money. Do you know how hard it is to return books to a publisher? There is a restocking fee. I have not seen the two new letters - I only saw the first one about a year and a half ago. This letter advocated breaking into the system and ordering books. It also advocated trying to break into the registers! How can you say that that is not destructive?

cloak

When did we ever say it wasn't destructive? We deplore such activities. At the same time, we're not going to cover up a major security hole just because we don't like what people may do with it. That may make us some enemies and may even hurt us financially but revealing these things happens to be what we believe in. If we give that up, we may as well stop entirely.

Dear *2600:*

I wanted to put in my own two cents about Barnes & Noble, Borders, and all that ilk of store. They are slowly killing small bookstores like ourselves by "bargaining" for (i.e., demanding) better margin from publishers. That means that they make more, dollars and dollars more, on a book they sell for the same price that we do. However you feel about economic survival of the fittest, this concerns me for another reason altogether, and that is that they do not have any ideology backing up what they do. They carry what is profitable and legal, not what is important. I have come to suspect that their decision to carry fringey material is part of their overall strategy to reduce competition. Meaning putting small stores out of business. If they can siphon off enough of our business, we won't be able to compensate. But they have no commitment to the material they are carrying, so if things ever

letters continued on pg. 48

Why Anonymous Phone Cards Aren't

Here is extracted testimony of the FBI, relating to the tracing of a telephone debit card found in the possession of Timothy James McVeigh. The card had been purchased in the name of Darryl Bridges, an apparently fictitious person, from a right wing newspaper called The Spotlight. It was the government's contention that the card was used to call for bomb making materials and transportation in the months prior to the bombing of the Oklahoma City Federal Building on April 19, 1995.

May 7th, 1997
in the UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Criminal Action No. 96-CR-68
(...)
THE WITNESS: My full name is Frederick Raymond Dexter, D-E-X-T-E-R.
(...)
DIRECT EXAMINATION BY MR. MACKEY:
(...)
Q. For whom do you work?
A. I'm employed by the FBI.
Q. And how long have you worked for the FBI?
A. A little over 23 years.
Q. Has that 23 years of experience been largely dedicated to a single area of specialty?
A. Yes. The majority of my work has been working with - stationed in Washington, D.C., but working with field offices on major cases doing all kinds of automation work, always in the data-processing area.
(...)
Q. Are you a special agent?
A. No, I am not.
(...)
Q. What is your current position?
A. I'm the unit chief of the Investigative Intelligence Support Unit.
Q And in that position, do you supervise or oversee other computer specialists?
A. Yes, I have 23 - approximately 23, maybe 24, computer specialists that work for me.
Q. Tell the Court and the jury a little bit about your present-day duties.
A. The unit supports automation efforts for the FBI in many program areas. One of our tasks is to support major case investigations throughout the United States. When records are subpoenaed or whatever, we automate those records to support the analysis for agents in the field. That's one of the tasks.
(...)
Q. What sort of positions have you held in that field or in that unit over your 23 years?
A. When I came to the FBI, I was a programmer, wrote software for all kinds of investigations, white-collar crime, investigations in the early 70's through the mid 70's. And I became a computer systems analyst, which I was in charge or the team leader over some computer programmers. Then I became a project manager over that continued group and advanced through the same unit until where I am today to be the unit chief.
Q. In the course of those years prior - prior years, have you had the task of organizing, managing, and understanding large volumes of telephone records?
A. Yes, I have. In some cases, numerous cases, UNABOM investigation, the Judge Vance murder investigation in Alabama, World Trade Center investigation, numerous other investigations. I managed, analyzed, and helped write software to the tune of millions of records in - in numerous cases.
Q. And did such a task, although on a smaller scale, fall to you in this particular investigation?
A. Yes, it did.
Q. Tell the Court exactly what your assignment was as it relates to the present case.
A. My task which I was assigned around June 1 was to obtain records from WCT in California and take those records - all of the records that were needed and produce what would be an intelligible, easy-to-read summary of calls that were made against the debit card.
(...)
Q. I want to spend a little time now, Mr. Dexter, acquainting the court and the jury with the steps that you took in order to (...) produc(e) that summary. (...)
A. When I visited with the people from WCT initially, I found out that there were three sets of records from them. (...) I took those records and put them together. In addition, there was other information that was needed. There was a particular area of the country that did not pass the "from number" to the WCT place, so those records had to be subpoenaed and merged in with them. Once the telephone numbers were identified that were either originating numbers or terminating numbers, then the subscriber data had to be subpoenaed and then merged in with those records or matched to those so that we know who the subscriber was of that telephone at the time that the phone calls were made.
Q. Let's turn your attention to a series of computer disks that should be before you marked as 509, 513, and 511.
(...)
A. (...) (L)et's talk about 509 first. 509 is the incoming information into the WCT switch that is referred to a lot of times. You may have heard 3911. That is the information as it comes into the switch. The last set of disks that we obtained from them is the 3910 records, the file that they refer to as 3910, and that is the information of calls that are answered. If a call is not answered, then it would not be on these disks.
(...)
A. When a phone call is made in the left-hand comer there, you will see that the - the information - or when you dial the number, it goes to your local phone company. If you dial an 800 number and the other seven digits, that phone call will then go to NASC, the Number Administration and Service Center, for routing. And at the NASC, every time a call comes in there - there's one of those that's located somewhere in the United States. Every time a local phone company gets an 800 call, they send it to that place. It does a query for that local phone company, and it determines the routing for how it goes to the destination that it needs to go to.
Q. Let me interrupt and ask you, are you familiar with who managed the 800 number for the Spotlight debit calling card system? What company?
A. WCT (...) (m)anaged the - the information for them.
Q. All right. Thanks.
A. The - the routing on this particular chart that we have up here shows that the NASC routed it directly to the switch at - the Los Angeles switch, as the title says. So it would go then to WCT. Within the red box is a switch that is at Los Angeles, WCT's location. The information would come in on the left side into (...) the 3911, the incoming call group. (A)t that point, certain information is captured. (...) It logs, as it comes in, the date, the time, the number of the telephone that sent (...) the call to it. And at that point, it is assigned a particular number to follow its way through here. (...) (I)t then passes the information to OPUS. (...) There's a message that goes back to the caller and says, "Thank you for calling Spotlight," if that's. who it is, or whatever debit card they handle. WCT handles many debit-card systems or debit-card customers, and it welcomes them and it says, "Now would you put in your PIN number and also put in the 'to number.'" If you put in the "to number" right away, it doesn't

come back and tell you how much is on your balance.

(...)

A. In fact, (...) when you make the call to the local phone company, they create a record right there of the date and time of that call, and much information is done there. Then as it passes through the 3911, it captures the information there. A computer captures that. Once a person puts in a PIN number and their "to number," it would be then passed down (...) to make sure there's some money in the account that you can make a call..(...) It goes to one of the four computers down on the bottom from the servers in the middle and one of the four computers or processors. The 3911 is hardwired. A lot of wires go down and wires go to each one of those four (computers). And we'll refer to those as Processor 1, 2, 3, and 4 later on. Once the OPUS has those records, it then sends the information up - back to (...) the WCTswitch, to the 3910 and the number is dialed to go out to wherever you're calling. And when you do that, the information again is collected at the 3910 (...) Then the information goes to a local phone company and your phone rings. If you pick up the phone and answer it, (...) when you hang up, then a record is completed at the 3910. If you didn't answer the phone, no record is actually written at the 3910. When you hang up the phone, records are written (...) at each one of those locations.

Q. All right. As I understand your testimony, information is gathered in each of those three boxes, 3911, OPUS, and 3910. Is that information always the same?

A. There are certain pieces of information in each one of those files that are collected. The date is collected in each one of those files. There is a time that is collected in each one of those files. That time obviously isn't the same in each one of those files because it's a progression thing. When you dial the 800 number, the 3911 captures that. It's a little bit later when you put in the PIN number and the "to number," at the time you captured down in the (...) OPUS record, and then it's a little bit later, like a second later, that it would get captured in the 3910.

(Testimony presented out of sequence, for clarity)

Q. Incidentally, Mr. Dexter, in this diagram, there are names associated with the subscriber number. When you were working with the data, did you have any subscriber information?

A. When - when we worked with these three files, I had no subscriber information. And it was not until we had totally completed the process and handed it to the people to do the subpoenas for the particular numbers, which then they came back, that any of these numbers were identified or known to me. I did not know any of those numbers during the matching process.

Q. So as you were identifying choices for matches, you had no idea whether one of those choices was a name associated with the investigation or not?

A. I did not.

Q. You had numbers only?

A. Numbers. Dealt strictly with numbers.

(Second piece of testimony presented out of sequence)

Q. Mr. Dexter, can you tell the jury what tic time is?

A. Two of the files, the 3911 and the 3910, kept track of the time of day in what they call tics. And what that is is every 3 seconds as the clock goes by, starting at midnight, it adds one to a counter on the switch. So after - if you happen to look at a record that had the beginning tic time of 20 in it, you would multiply each one of those tics by three and you would know that it's actually 60 seconds or one minute past midnight. If you were to took at a record that had 1,200 tics in it as the starting time, then you would multiply 1,200 by 3 and have 3,600 seconds past midnight. In the computer, we put in an algorithm to figure out - to convert that to clock time so everybody could understand it, because looking at tics doesn't mean anything to anybody. It's a very simple algorithm in that once you've multiplied by the 3 seconds and know how many seconds it is past midnight - there's 3,600 seconds in an hour, so you just take that number that you have, divide it by 3,600, and you have how many hours you are past midnight. Whatever the remainder is, you have that many seconds left. You divide that by 60, and you have - that's how many minutes you are - that many hours and minutes past midnight. And then whatever the remainder is, that's how many seconds there are. And the clocks in 3911 and 10 kept the beginning and ending time in tics for each one of those. So every record there, when you look at it, you automatically had - you could never get finer than 3 seconds because they didn't capture anything other than 3-second intervals.

Q. And did you use this unit of measure, the tic time, in your preparation of the summary?

A. Yes, we -

Q. Why did you do that? Why did you rely on tic time?

A. We were - we were in - in meetings with WCT while they were explaining their records, they explained that there was a field in their records. You've seen the file layout for the 3910, 3911. There's a field called "Time," but that is not the actual time of the call. That was actually time of the customer, where they wanted to be billed. These computers were on the West Coast, but if you were a company that was in Mountain Time, then you would ask for your billing records to be offset one hour so the time in the record that they have under the field called "Time" was not really the time. It was always an offset. The tic time was always absolutely the time when a call started and ended according to Pacific either Daylight or Standard Time.

(End of testimony out of sequence)

(...)

Q. How many total records of telephone calls did you have to look at among or from those three disks or three sources?

A. Without looking at the exact numbers, there was over 100,000 in each one of the files. Approximately - I'm sure we have an exhibit that gives us the exact numbers.

(...)

Q. Lets spend a little time, Mr. Dexter, talking about the timing of events. You described three different sets of records, timing of events somewhat close but maybe never always the same moment. Did you find there were different times among the records you were looking at?

A. Yes, we did. And going back to the chart, the one thing that is common is that every - every call that comes in has to go through 3911. If - if every clock was synchronized on every one of these computers, the computer at the local phone company at the top, that would be the earliest time if they were all in synch. The time that is in the 3911 when it starts would be the next time if they were all in synch. When you get down to OPUS, if all four of those computers had the exact same time on it, then whichever one it went to, that would be a little bit later. (...) We're talking milliseconds or a second or two seconds this happens, very quickly after a person puts their PIN number and "to number" in. But there can be or usually is a minute or so from the time you put the 800 number in until you get down to the OPUS record, because a person has to put in the PIN number, the "to number," and the processing, etc. It takes that much time.

Q. And that all assumes that every computer that processes that call has a synchronized clock?

A. That's correct.

Q. And do they?

A. There were none of them that were synchronized.

Q. What did you - what did you do to address that problem of identifying an accurate time of telephone calls?

A. Well, since - since every call had to go through the WCT switch, no matter where it originated or where it went out, we used that as our constant clock. And then everything we worked with was a difference or a deviation from that particular WCT switch. The clock, by the way, in the 3911 and the 3910 is the same clock because it's in the same computer, the same switch.

Q So the first step was to use the same measure of time in pulling together the various items of telephone calls?

A. You use a constant clock, yes.

Q. In this case, you use the clock on the L.A. switch?

A. Yes.

Q. Faced with some - more than 300,000 records, what was the first step you took to reconstruct the activity on one account in the name of Daryl Bridges?

A. The first thing that we did since we knew that the account number is logged into only one of these files, and that is the file at the bottom called OPUS or where the debit card records are, we ran a program to go in there and pull off all of the records that were - had been stored in the database using that particular account number.

(...)

A. The OPUS file told us how many records there were in the OPUS file by all of the Spotlight customers. This particular exhibit shows us exactly the number of records that were stored in the OPUS file that had the Daryl Bridges account number in each of those records.

Q. So you could design a computer program to say from the 155,000 plus records, find just those with the Daryl Bridges account number?

A. That's correct.

Q. And what you started with then was down to 687 such records?

A. Correct.

(...)

METHOD 1

Q. Now, having focused on the Bridges records and the OPUS file, what was your next step in producing the summary?

A. The next step was to take each one of those records; and by looking at those records, we knew certain information. We knew a lot of information by looking at the OPUS record. We knew the date of the call. We knew the time of the call. We knew the terminating number of the call. We had the account number because we only pulled one account number. And we had a duration that came with the OPUS records. So we had all of those. The thing that we needed to match it was - was to find the "from number." The only file that carried the "from number" was, in fact, the 3911. So the first step would be to go in and match each one of those OPUS records, each one of those 8 - 687 records with a corresponding 3911, how it came into the L.A. switch.

(...)

A. We started with (...) the OPUS file - and the key to matching that up to the 3911 was the port (...) This port has a corresponding port number. And then the date, of course, would have to match the date down here. And the beginning time would match the beginning time here. To match a 3911 record, that was the key fields that you used to match.

Q. You made reference to associations between ports. What exactly was that relationship?

A. There is a - I call it a matrix, but it was a process that was developed by WCT and their contractor. If you would envision like 132 electric outlets. And each one of those outlets, you would plug a wire into it. And some of those wires in 3911 would go down to Processor 1, some of those wires would go to Processor 2, and some of those would go to 3 and some would go to 4. On the back of each one of those, it looks like electrical outlets, also. So from the 3911, there is a hard wire that goes from the 3911 down to - and I'll just use Processor 1. On the back of there, there's actually a number. Each one of those electric outlets, ports, have a number associated with it. And when you go down to the processor at OPUS, that has a number associated with it, also. So when a call comes in to the 3911, (...) it goes out of a particular port onto that wire and goes into a port into the OPUS processor; and each one of those are numbered so that it follows that constant path, depending on which one of the ports it selected when it came into the 3911.

(...)

A. We would start here with an OPUS record. And in that record, we would look at a date, a begin time, and a port. And we would be trying to match that with a 3911 record that has a corresponding port over here. The date would have to match exactly. And since the clocks were not synchronized, we would look for a record in the 3911 that is within 2 minutes of the - of the time in the OPUS record. Then we would take that pair down here, once we find that record, and we - we'd try to find if, in fact, that call was answered. If the call was answered, a record is created in the 3910 file. (...) The other thing is - is the end time in the 3910 and the 3911 are the same. They are to within one tic because when they hang up the phone, the WCT switch writes the record out, and it writes it at the same time or within 1 second of each other. So when you find a record in the 3910 that the end time matches exactly, you have absolutely locked in on the record.

Q. Mr. Dexter, how many phone calls did you find took place on the Daryl Bridges account after September 14, 1994, and April 19, 1995?

A. There were 604 calls.

Q. And how many of those calls were matched in the process you've just described?

A. Using the L.A. switch as this process?

Q. Yes.

A. There were - of the 604, there was around 500 of them that were matched in that process.

(...)

Q. So of the five fields of information, you relied on the 3911 for start time and called from and for the other three, the OPUS source?

A. That is correct with one exception. The length in the OPUS file, there was always a length of a call. If, in fact, the call was answered, then it was the talk time of the call. If, in fact, the call was not answered, then the duration in the 3910 record was the ring time of the call. So in our summary, if a call was not answered, we wanted to demonstrate that the call was not answered. So therefore, zero was put into the summary.

Q. Now, the method that you have described and illustrated thus far, did that allow you to match all of the data that you have before you?

A. No. That was the first of three different ways that the information had - had to be matched.

Q. And what was the second method?

METHOD 2 (the only difference in the entire process is that original port number is not available in the 3911.)

A. The second method was if - dealt with information that did not come directly into the Los Angeles switch. When the local call was made and it went to the NASC, the NASC routed that call to a switch other than L.A. first. And then it would be routed to L.A. so that was the second set of calls that had to be matched.

Q. And why did the fact that a call might start in the Chicago switch cause any special problems for you in your matching?

A. The - the problem there was - is that in the 3911 record, the information that was captured in each one of the records for a non-L.A. switch carried with it the time that it was and the switch where it came from. So if it was Atlanta, it carried East Coast time. That was stored in the record. Although those 3911 records that came through L.A., the time was always Pacific Time. If a switch was not L.A., then it - the record carried the time of the time zone where that switch

was located.

(...)

A. (...) WCT had, I believe, six of those switches around the country to help offload. You can't send everything to one switch. So they had information there that processed the information and then would send it on to Los Angeles. When the record left the non-L.A. switch and came to L.A., it would go to the 3911 side and it would go into a port there and the call would be handled within the record, although those records would be created, the 3911, the OPUS, the 3910, exactly the same way as the other one except that in the 3911 record, it captured information from the non-L.A. switch because they needed it for carrier billing and it didn't capture certain information that was available in the L.A. switch at that time. So the port that was used in the L.A. switch, in fact, was not captured in the 3911 record. (...) In each one of the records, there is a field that is called switch, and there's a number in it. If the number is a

10, then we know that record originated in the L.A. switch. If it was - I'll give two other examples. If it was a 2, it was - it told us it was - originated in the Chicago switch. If it was a 4, it originated in the Dallas switch. There was also switches in Philadelphia, Atlanta, San Francisco, and Seattle - I believe that was the other four places.

Q. So once you knew where that call had started, you knew how many hours to adjust in your calculations?

A. That's correct. (...) Okay. We would - we would in this case - first, you would have looked for - when you have an OPUS record, you would have looked to see if, in fact, the ports matched over to the 3911. In fact, if it did not, then what you did is you looked for a 3911 record with a - the same date and the same time; but the 3911 had to be adjusted for the number of hours, wherever that switch was. So you would be looking for a record that would be either 1 - there were no switches in Mountain Time so you'd be looking for a switch - a record that was two hours difference, if it was Central, or three hours difference if it was East Coast Time to do the match there. (...) Once you have matched an OPUS with a 3911 record to match a 3910 record, the ports now are available again. So that match guarantees when you go across, you have the OPUS record as it's hard wired up to the 3910. You have that port sequence that follows through. You have the ending tic time, and the 3910 matches the ending time in the 3911. And the "to number" in the OPUS record matches the "to number" in the 3910. So the only difference in the entire process is that original port number is not available in the 3911.

METHOD 3

A. This - this debit card for Spotlight has a process a lot like a lot of debit cards or calling cards that you can make or call a second number without redialing the 800 number again or without putting your PIN number in again. And how that works is on the original call, you dial the 800 number. Spotlight answers it and says put in your PIN number, put in your "to number." You do all that. The money is available. You connect with that call, talk to the person, or whatever. When they hang up, instead of you hanging up the phone, you can hit the pound sign. And when you hit the pound sign, that then you can dial another "to number," instead of having to go through the whole process of getting into the system again. And you continue to repeat this as many calls as you want as long as you have money in your account that will continue to be subtracted when you're making - calling that particular number.

Q. What's that feature known as?

A. We refer to that as the reorigination feature within the calling card.

(...)

Q. What was the consequence in terms of the records that you had available to match if that person had done a series of reorigination calls?

A. Well, the - the thing we want to remember is when the 800 number is called, a 3911 is created. (...) An OPUS record is created every time that a "to number" is put in, and a 3910 is created every time a call is answered. So if you use the reorigination feature, you end up with one 3911 record created in the file... you will end up with many OPUS records... and you will get a... corresponding 3910 record for each one of those that is, in fact, answered.

Q. So the answer in 3911 will encompass more than one call?

A. Yes, it will.

Q. And then it fell to you to figure out how many steps or how many parts there were to that total sequence?

A. Yes.

Q. Did you develop a methodology for doing that?

A. Yes. And it - it actually worked in reverse. We didn't go in with known 3911's. We had (687) OPUS records. And we matched up all the ones that would match up through the L.A. switch, because you had a 3911. (...) Then what you had is you had a certain number of records that did not match to a 3911. (...) It was very obvious on reorigination records, because once you were into the 3911 record, that port was selected for all of your calls that you made during that reorigination. So every call that you made used the same port in OPUS and if it was answered, used the port in the 3910, because you had that electrical connection that it just continued to use that same one path through there all the time.

(...)

Q. What steps did you take then to calculate the time of calls that took place in the series of reorigination calls?

A. (...) You always knew the start time of the call because it's (in) the 3911 when it came in. You always knew the ending time of the last call because you have the duration from the OPUS record, whether it's 5 seconds, it's a minute; and you know the ending time of the 3911. So all you have to do is subtract the duration from the end of it. So the last call in the series, you always know what (...) time it was. The one situation where you do not know the start time of the call is if it's in the middle of a series of more than two calls and, in fact, that call was answered. Then you had to come up with and we did come up with a standardized formula to calculate that time, so that it was the same across every reorigination call.

THE COURT. (..) What we have to do is caution the jury that these exhibits are not going to tell us who made the call or who received the call or what was said in the call and that with respect to the subscriber information, again, it's simply based on what these phone companies have in their records with respect to who they sent the bills to.

Commentary on the extracted testimony of Frederick Dexter

The first thing which becomes apparent in the FBI's testimony is that the suspect's use of the card was a misinformed attempt at subterfuge. The card was purchased with postal money orders in a fictitious name, and was "refilled" by money order twice. This indicated that the user was attempting to leave no trace of their identity when they used the card to make telephone calls from various locations around the country.

The major failing of this strategy was the continued use of the card for several months and the retention of the card beyond its operational utility. McVeigh apparently used the card too long, and left the card in the possession of a friend to whom he was easily traced. The FBI found the card, and thus was able to reconstruct several months of activity on it with only a single breach in operational security.

A more successful strategy would have involved the use and disposal of several prepaid phone cards purchased anonymously at gas stations. These cards would be used for a few calls each, short of their $10-20 face values, and discarded with the remaining credit intact so that they might be adopted by unsuspecting people. This would be an impediment to successful tracing even if an account number was obtained by a surveillance agency. Anyone following the electronic trail would be led astray as the person who found the card went her separate way.

The second lesson which this teaches us is the relative difficulty the FBI has in tracing these cards for ordinary cases or casual surveillance. The search which produced the card in question and allowed its tracing was conducted by almost 50 agents. The information used in reconstructing the call activity involved the subpoena of several bodies of evidence, including subscriber records, from each local phone company which handled the calls, as well as from the company which handled the 800 number and debit billing. Clearly this is not a real-time capability for the FBI, unless the account number is known in advance and the subject is essentially under close surveillance. From past experience this would only apply to espionage or terrorism cases involving suspects subject to infiltration or agents provocateur.

The third thing which this teaches us is that the records do not actually prove anything. As the court said in this case, these records cannot show who actually used the card, or what was said, or who was spoken to at the terminating end. They are primarily of use in inferring guilt, and are thus less useful the less any single card is used.

THE CRYPTOGRAPHY OF TODAY

by kriminal 3nigma

Governments have long understood the importance of keeping information private, both for military and economic reasons. What better way to do this than with an advanced computing cryptography formula? Past wars have been won or lost because the most powerful government on Earth didn't have the same cryptography that a 15 year old crypto-phreak can have on a PC today. I have extensively read books, studied formulae, and learnt the general methods of cryptography and am now known as a cryptography phreak (similar to a phone phreak), also known as a crypto-phreak or a crypto. Crypto-phreaks are all around the world, and many are programmers, scientists, or advanced mathematicians. Each of these people live to give the public better privacy from the bloodthirsty governments of today. In this article I will attempt to give you a good outline on cryptography and how each and every one of you can use it to your advantage.

Encryption For Everyone

Basically, every message or file you encrypt has a digital "signature" added to it. You and you only can apply this digital signature unless someone else has your password. The recipient will be able to be almost positive that the message or file is really from you, that it was sent at exactly the indicated time, and most importantly, that it hasn't been tampered with in the slightest and that others can't decipher it.

This is all based upon mathematical principles, including what we now know as "one-way functions" and "public-key encryption." The mathematical principles are very complicated, to the extent that even I, a crypto-phreak, do not understand bar the easiest concepts.

A one-way function is something that is very easy to do, or - put it this way - something that is much easier to do than to undo. For example breaking a window is very easy to do, but can you put it back together as easily? I think not. The sorts of one-way functions required for cryptography are that it is easy to undo if you have that little extra piece of information and close to impossible if you don't have it. There are many one-way functions in math and one involves prime numbers. Everyone learns prime numbers; they are basically numbers that can only be divided by 1 and themselves, such as 2, 3, 5, 7, 11. There are an infinite number of these and there is no known pattern to them except that they are prime. When you multiply two together you get a number that can be divided evenly by those two primes. Finding the primes of a number is known as "factoring." I think I'll now stop treating you all as babies and get on with it.

It's easy to multiply two primes, example 11,927 and 20,903 (which gives us 249,310,081) but it's very difficult to recover those two primes from the result. This is a perfect example of a one-way function, which is the most sophisticated encryption system known to us today. It may take weeks for even a supercomputer to factor a large number that was created by two primes. This is exactly the reason why an encryption system was based on factoring two different decoding keys; one to encrypt the message/file and one to decrypt it. With only one you only have half the capabilities, i.e., with only the key used for encryption you can only encrypt files/messages, theoretically. Decrypting requires a separate key, available only to the intended recipient of the message. This key is based on the product of the two prime numbers, where the decrypting key is based on the numbers themselves. A computer can randomly generate a new pair of unique keys in a moment because it is simple for a computer to make two primes

and multiply them. The encrypting key can then be made public without appreciable risk.

Now here's how it works, I want to send *2600* this article. My computer looks up *2600's* public key and uses it to encrypt this information. No one can read the message other than *2600,* because their public key doesn't have any information needed to decrypt the article. My computer then sends this newly encrypted file and *2600* decrypts it with a private key that corresponds to their public one. Now they want to answer and tell me what a great job I did! The computer looks up my public key, they encrypt their message with it and send what looks like random numbers and letters as an e-mail. I then take this, paste it into my homemade decrypter and tada!

Now you may be wondering how big these primes have to be to ensure a very elite and secure one-way function. The concept of public-key encryption was invented by a dood known as Whitfield Diffie and Martin Hellman in 1977. Another set of crypto-phreaks, who the public called scientists, Ron Rivest, Adi Shamir, and Leonard Adelman, soon came up with the notion of using prime factorization as part of what we now know as RSA encryption, after the initials of their surnames. Today it is estimated that it would take millions of years to factor a 130 digit number that was the product of two primes, regardless how much computing power was used. To prove this point they had a little "competition." They challenged the world to find the two factors in this 129 digit number, known to crypto-phreaks as RSA 129. It was, and is, as follows:

114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541

They were quite sure that this message they had encrypted using the number as the public key would be quite secure forever. But they hadn't expected computers to get so powerful, so quickly. And in 1993 a group of more than 600 academics and crypto-phreaks from around the world began an assault on the RSA 129, using the Internet to coordinate each individual's work. In less than a year they factored the number into two primes, one 64 and one 65 digits long. (This time I'm not wasting my time typing up these two primes!) They then decrypted the message that said, "The magic words are squeamish and ossifrage." So as you can see from this, a number 129 digits long isn't enough to encrypt data that is really important and sensitive. Mathematicians today believe that a number 250 digits long is more than enough to stop the whole population of Earth from uncovering the two primes. But who really knows? Computers are getting faster by the second so we might end up with an RSA 1,000,000.

One thing we don't have to worry about is running out of primes - there are said to be far more primes than atoms in this universe (yeah right). Key encryption allows more than just privacy; it can also ensure authentication of many things. This will, hopefully, bring new online benefits in the future (more on this later). Security can also be increased by including time stamps with the encrypted messages or digital IDs.

Society's Biggest Problem

None of the protection systems that most commercial and government computer systems use today are completely fail-safe. The best they can do is make it as hard as possible to try to get into them. Despite popular opinions to the contrary, computer security has a good record. Well at least that's what they tell the public. In fact it is estimated that at least 2000 computers are broken into in a week, in Australia and the U.S. alone. Computers are capable of protecting information in such a way that even the smartest hackers can't get at it readily unless someone entrusted with information makes a mistake, but not too many computer systems in

the world use this, or take full advantage, of these methods. The main reason computer systems are so easily breached and files so easily decrypted, is that people are stupid when it comes to passwords and setting up systems. People don't want to spend hours on end just to set up a network. They do it the easy way, with the default passwords.

Because most systems will soon use today's encryption techniques such as to order concert tickets and buy other products, a breakthrough in mathematics or computer science that defeats the cryptographic system could be a disaster to the people owning these systems and to the government in general. The obvious breakthrough would be to create a mathematical formula that gives us an easy way to factor extremely large prime numbers. Any person(s) possessing this power could do anything they wanted, electronically.

Every Cryto-Phreak's Nightmare

Many in the U.S. government are opposed to encryption capabilities because it reduces the stronghold they have over the people of the U.S. Though this, of course, isn't quite how they put it. They say that such encryption "...reduces their ability to gather information." But, thanks to many crypto-phreaks, this technology, and technology as a whole, can't be stopped. The NSA (National Security Agency) is a part of the U.S. government's defense and intelligence community that protects the U.S.'s secret communications and decrypts foreign communications to gather intelligence data. The NSA doesn't want software containing advanced encryption capabilities to be sent outside the United States. This doesn't bother me and many other crypto-phreaks at the moment, because we don't live in the U.S., but if the U.S. government manages to do this, many other governments may follow. However, this software is already available throughout the world, and any computer can run it. No political policy will be able to restore the U.S. government's tapping capabilities that it had in the past.

The U.S. government recently had a court case with one Philip Zimmermann, the programmer of PGP (Pretty Good Privacy), one of the best and most commonly used encryption programs. The case ended in Phil not being able to release PGP outside of the U.S. But (unofficially of course), Phil sent the scanned source of PGP 5.0 to his friends in Europe. They then scanned this and compiled it (though it was called PGP 5.0 international version). They also distributed it like crazy all over the globe, thanks to the Internet. As you can see from this, cryptography will never be stopped, just like hacking. They may catch a crypto-phreak or another Mitnick but they won't stop us all.

Now if commerce rests on any single concept, it must be identity. There can be no business without ownership. To regulate commerce there must be a legal system with accountability and that can't happen without precisely identified individuals. What the U.S. government is planning is to make sure everyone has an identity on the Internet, using the encryption methods previously mentioned. The U.S. and British governments both came up with ideas on how to manage all these keys but it seems that key escrows aren't to be, for now. Instead the U.S. government is planning to pass a bill that will ensure that there is a backdoor in each and every cryptographical program (in the U.S.) so that the NSA, FBI, CIA, and the many other unknown governmental groups will be able to access any bit of any person's encrypted bytes. Does this seem immoral? No, why would it be? According to many of Clinton's advisors, backdooring software and enabling the government agencies full access to key escrows are necessary to combat state-sponsored terrorism and prevent the undermining of the emerging Net economy. Does this sound like a load of bullshit to you too? The worst part is that the computer illiterate thinks it's all true. Help them to see the truth.

Hacking the Atcom Cyberbooth

by Fever
a_fever@juno.com

Recently I was sitting around in an airport, waiting for a flight, when I noticed something strange. In the middle of the room, there was a large gray obelisk with a sign saying, "Surf the Web! Send/Receive e-mail!" Naturally curious, I sat down. I discovered a bug that some of you may find useful, or at least entertaining. Since then I have done some research on these machines, and this is what I have learned:

A Cyberbooth is basically a Pentium 120 to 166 with an ISDN line. The top of the line model, the Cyberbooth Kiosk, is a four-sided unit featuring two computers and space for two optional pay phones. This is the obelisk I mentioned earlier. They cost about $15,000. The Wall Unit and the Low Profile Cyberbooth are basically the same machines, the only difference being in the shape. The wall unit looks like a prop from a bad Star Trek episode, while the Low Profile just looks... odd. The newer Payphone Cyberbooth and Desktop Cyberbooth have smaller screens and are slower. The Payphone only has a 33.6 modem. This is one of the few cases outside of Microsoft where a new product is considerably worse than the old ones. This may explain why Atcom won an MS RAD award. There are some interesting features on these machines, however. These two are the only ones with sound. The Payphone Cyberbooth mounts next to real pay phones. Download some sounds from the Net, and you have a conveniently placed red box. You could also play sound effects at passersby. This could be especially fun at an airport. The Desktop Cyberbooth, also called the "Hospitality Solution," is intended for hotel rooms, and this gives rise to two unique features. The first is that they don't require a credit card, they just charge your time directly to your room. The second is that it has a 3.5" floppy drive. I'm sure you could think of some rather... creative uses for that, but keep in mind that they know what room you're in, and what machine you have access to. If you're going to play with it, use an assumed name and pay cash.

The Cyberbooth offers several main features. You can access the web, e-mail, telnet, play games (just in case you can't wait to get home to play Mine Sweeper), or access online services like Compuserve and America Online. (Don't use America Online. You'll be much happier in the long run.) Unfortunately, all of these features require you to swipe your credit card!

Atcom gives you some options free, in the hope that you will give them your credit card later. You can look at the Atcom web site and send e-mail to their webmaster telling him about this article. You can also visit some other pages free. These will usually be on the right of the screen, but you may sometimes find free options on the top too.

At this point, you might be thinking that you can just go to the Atcom site and then go wherever you want from there. There are a few things they do to prevent this. The main problem is that as soon as you attempt to leave, you will get a message telling you that you are not allowed to access that page without paying, and you will remain on the free page.

"Oh no!" you cry, "I can't pay for this! How can I get on the web?" There is a *huge* hole in security that would allow any AOLuser to get on the web, assuming he could figure out how to use the web. Look at the top of the Cyberbooth screen. Click on the "Cyberbooth Marketplace" button. This will give you several graphics linked to advertisers' web pages. Click on one that looks interesting. This will take you to an advertiser's web page. From there, try to find a link out. For some reason, when you go through the Marketplace, it lets you out. I have not found any other ways to get free access from a Cyber-

Atcom continued on pg. 52

letters continued from pg. 39

get bad they will drop all of that stuff like a hot potato. That really concerns me - where are we all going to buy our banned books once B&N takes over the world? They are altering the way that publishing is done as well, making it harder for smaller-grossing books to be published at all. When you consider that many of the great works of western literature were miserable sellers for the first 50 or so years, you can see the problems this will cause. Food for thought - just remember who your friends are and that a leopard is a leopard even if he changes his spots.

Rachel
Co-Manager
Internationalist Books
Chapel Hill, NC

Well, at least we were able to help get these thoughts into every Barnes & Noble in the nation.

Between The Lines

Dear *2600*:

Not that I'm eager to see *2600* sink as low as the rest of American journalism, but I think most of the media have missed a very interesting part of the Starr report. Read the footnotes of the report, especially the ones where they are substantiating testimony of the events and timeline.

The footnotes refer to "White House Epass" and "WAVES" records, "movement logs," etc. If any *2600* staff or readers know more about these technologies, or how White House security is set up, it would make a great article.

Pete

If we get the info, we'll print it. Hopefully our White House contacts will come through again.

Help Needed

Dear *2600*:

I've been getting some slack from a group of "aol lamers" claiming to be elite programmers and in their words "er33t hax0rs." For one, they claim they hack using aol addons and program aol addons. I've told them time and time again that they 1) use aol, 2) can't do shit, and 3) they are fucking with *2600* when they fuck with me. In the past month or so, they have been telling me to tell y'all "that we in the aol warez scene can't be touched, and anytime they think they can take us to bring their fake asses on." I want to take all of their lame asses out but I need help. There are more of them and I don't have the time to fuck em all. So if you wanna help take action, respond and I'll give you their e-mail and sn's on aol.

morbus

Please keep us out of your little cyber gang wars. They aren't of interest to anyone with half a brain.

Dear *2600*:

I own a large apartment complex (100+ units) and in the past 3-4 months I have had reports and documentation of calls to 900 numbers (sex lines) from several residents' apartments. The calls are being billed on the customers' RBOC bill from third party billing agencies. The calls take place when they are not home and in one case the resident was out of state.

I can't believe that someone is getting into the apartment with a master key as they are tightly controlled and the events are all during daylight hours. We have lots of nosy neighbors and a service crew of four people who ask questions of anyone who is not a resident.

Each resident has a portable phone. Could someone be accessing their phone line through the portable phone? I was able to listen to the caller's voice as it was recorded by one of the billing companies . It was too clear to be coming from a portable phone. This leads me to believe that the hacker is getting into the E5 switch and fooling Ameritech's equipment as to the source of the call. Is this possible?

Please give us a clue as to how this may be happening. The residents who this is happening to are not wealthy people.

Col Pete

First off, you do not need to be a hacker to do this. Hackers will explain to you how it works unlike the phone company or the people who want to continue getting away with this. For some reason people think that because we understand how these things work, we're the ones responsible when things go wrong. Anyway, your problem is simple. And it's extremely common. To give you an idea, over the years we've had at least a dozen phone lines that don't belong to us pop up in the 2600 office on unused jacks. In fact, we have one right now. It happens to lots of people all the time and the phone company doesn't want you to know this because if word got out that your phone number actually appears in multiple locations, they would have a hell of a time convincing people that "if the call comes from your line, it must be coming from your house." There are numerous points where a line can be compromised - junction boxes, basements, even central offices. We know of cases where phone lines for an entire apartment complex were accessible in one tenant's closet. In your case, someone obviously has gained access to all of your lines and is simply clipping onto them at will. In all likelihood, the point of entry is somewhere on your property. Check your basement, garage, even individual apartments if all of the lines run through them. If each of your residents has the exact same type of portable phone, it's possible a weakness is being exploited there. Most modern cordless phones have protection against this type of thing. In either of the above scenarios, your culprit would have to be fairly close.

Hotmail Fun

Dear *2600*:

Well, you guys probably already know bout this one, but there's a very simple way to hack someone's Hotmail account. Let's say that I wanted access to my friend's account. I would call him voice and tell him to go check his e-mail, knowing that his account is here@hotmail.com. Now I hang up with him and log onto the net. As URL, I type the following: www.hotmail.com/cgi-bin/start/here and bingo, I'm in. This applies to anyone who knows a person's ID, and when they're checking their mail. All you

have to do is add the user ID after the "start" line. I hope this gives someone some fun - I know I've gotten a kick out of it.

Feng Laser

This method generally only works from the same IP. We did discover one notable exception. If you connect to hotmail using www.anonymizer.com and someone anywhere in the world does the above to your username at the same time, they will be logged on as you without being prompted for a password. (This is rather ironic since anyone connecting to hotmail via anonymizer is jumping through hoops to maintain their privacy.) We're certain that there are other ways of doing this as well. As a side note, hotmail accounts are also vulnerable through the "reminder questions" that users are encouraged to enter in case they ever forget their passwords. The idea is that only you will know the answer to your reminder question. But a lot of the questions users enter are fairly easy to answer, such as "how many cats do I own?" Once you guess the answer to the question, you're told the user's password without any further verification.

Non-Subscriber

Dear *2600:*

I was thinking about subscribing, but I won't because: 1) Why should I have to pay a premium to subscribe? (It's $4.50 an issue, which works out to $18 per year at the bookstore). 2) You get *all* of my money up front when I subscribe - you can never be sure that I will buy all four issues so that should be worth something to you in the form of a *discount.* 3) How *do* I know that you will be around for the next four issues? You can do better.

Sandy

You must be a real fun person to hang around with.

2600 To The Rescue

Dear *2600:*

It was a Monday morning and since I was void of sleep, I wasn't functioning all that well. My friend next to me in homeroom asked me if I did my English homework. All of a sudden I remembered we had to read an article from a periodical and bring it in, finding any words we didn't know and defining them. I froze, but remembered my *2600* in my locker! Due to the article on "How to Hack Your ISP" I got an A on my project! When I got it back, I saw a side comment that said, "Good Lord, what on earth do you read?" Thanks for keeping the mag great!

jeff

And who says we're leading the youth of America astray?

In Defense of Microsoft

Dear *2600:*

I'm a 16 year old computer security enthusiast. I also just got a job at Microsoft. In writing this I may alienate some of my friends and peers, but I think it has to be said. Microsoft really isn't that god-awful. Many of the people here are, or at one point were, hackers and phreakers. A couple have helped me with some issues, and in one instance, a co-worker and I spent the better part of a Friday night and two large pizzas discussing the injustice done to Kevin Mitnick. These people are really not the anti-Christs that some make them out to be. In taking this job, I've received ridicule and scorn from all of my hacking peers, claiming I've sold out and gone over to the Man's side. Well today, who the hell is the Man!? The only people I have met who still embody the hacker ethic and spirit that I have only read about reside at the big M.

Count Zero Int

We can assure you that there are still plenty of hackers outside Microsoft. We don't doubt that there are lots of nice and enlightened people within the MS compound. But that doesn't alter what Microsoft itself is and, to many people, it's something scary, huge, and potentially damaging to a lot that we stand for. If your hacker friends aren't kidding themselves about this, maybe it's good to have them on the inside. If they think Microsoft is different just because it's keeping them employed, that's very sad.

Clarifications

Dear *2600:*

In response to the article in 15:3 ("Screwing With Blockbuster Video"), at the Blockbuster in my hometown it is policy to ID when a movie is checked out. This became policy only recently so the article may have been right at the time it was written. Also, this may be unique to this store. I am not sure if it is a franchise or corporate situation.

Spoon

Dear *2600:*

Regarding the back cover of 15:3 in which Belgium is described as "easily the most mysterious and misunderstood of all the former Soviet Republics" I believe part of the "misunderstanding" could be that Belgium was never a Soviet Republic. In fact Belgium joined NATO in 1949 and the EEC in 1958. It has a long, well known, non-Soviet history.

StuntPope

Revisionism is such an ugly thing.

Dear *2600:*

In reference to page 50 of 15:3, look at: www.lucent-ade.com/scat/ This is what Lucent will tell you about SCAT-9, although I assume the -9 designation is an additional something Ameritech dreamed up. It seems odd to me that Ameritech and company would be as paranoid as darkrazor suggests, but who knows....

Dustin Decker

Dear *2600:*

It appears one of your articles was a tad off. It appears that in issue 15:3 there were errors in the article "Hack your Console" by m0tion. Error #1 was in the URL for Vivid Barrier (surf.to/vividbarrier), as they don't sell backup units, but rather, design a good front end for most emulators of console and computer systems. A better place to go for older console backup units would be www.stylex.com. Although it's an e-mail inquiry-only site

now, they do carry a lot of backup units. Another site is Video Game Deck at www.vgd.org. There, you can find info on backup units for every system that ever was and where you can get one (if they're still making it, that is). Secondly, as to the bit on it being legal to backup a Nintendo ROM image for your own personal use, it is technically illegal due to the fact that Nintendo Japan and Nintendo of America use proprietary technology in the manufacture of their cartridge games (such as the MBC chips). Duplication or emulation of their hardware is grounds for legal action. Although there is some truth to m0tion's statement, you can be cast into the hell of Nintendo's legal battles if you are dumb enough to get caught. Personally, I prefer working with the Nintendo Gameboy myself, as it has *tons* of potential, as well as lots of resources and SDK's for coding. You can get all the best GB hacking and coding utils from: home.hiwaay.net/~jfrohwei/gameboy/. Everything from GBcamera to PC conversion, Phreaking ROM's and Terminal software are available as well as other stuff. In conclusion, Console systems are the best, and even though m0tion was a little off on a thing or two, he's dead on when saying that they are a blast to hack! If you haven't seen what your game system is *truly* capable of, then you didn't get your full money's worth! So if you still haven't tried it yet, go out, locate the docs, and go nuts!!!

Rave669

Dear *2600:*

In response to the 15:3 letters section D-Recz makes some pretty bold statements. I hope that I am safe to make the assumption, judging from the response that *2600* had for him and that of the fellow hackers who I have been in touch with, that he is out beyond left field on this one? Now most of us would say, "Okay, he's entitled to his opinion," and leave it at that. Most people would... *except* those of us from the Chicago community. Now, I won't speak for the "Chicago Underground Community" or the "Chicago 2600" as I do not have that all powerful ruling ability to speak for the masses. I just have a question, in regards to D-Recz. In all the time that I was in Chicago, from all of us involved in the computer underground, not a one of us has ever met you. Why? With as many active h/p boards in the Chicagoland area and the fact that most of the sysops were working on bringing the H/P community back together again, you had plenty of chances of gathering with the local community. I guess I just wanted to know who voted you into office to speak for us?

Archive

We received several letters like yours. Here is the writer's response to our comments.

Dear *2600:*

Allow me to clarify my anger-causing response in the Fall 1998 issue. When I said "the Chicago-area *2600* meeting," I was mistaken. My intended phraseology was "several of us at the Chicago-area *2600* meeting."

D-recz

Dear *2600:*

In the 15:3 article "Back Orifice Tutorial," it was stated that the only way to get rid of the Back Orifice server is to delete it from the registry. Not true, there are two other ways that it can be either deleted or shut down. Number one: You can't simply delete BO from a machine because it is being used constantly so here is the way that I have found to stop and delete it. *You have to have physical access to the target machine,* you have to have the Back Orifice GUI client (I have yet to try the others), and then you view the network connections. Every time I have tried this it has given me an Illegal Operation Message and I was forced to shut down the server then delete it from the C:\windows\system directory as ".exe" or the file name it was assigned. Number two: In any of the clients, use the process list command and find the BO server " .exe" or the name you gave it, and get the Process ID. Then you can run the process kill command and input the ID. This will kill the BO server, shutting it down, but not deleting it. By the way, I have used BO to play some cool schooltime pranks with the message box command! Keep up the good work and *free Kevin!*

Cslide

Dear *2600:*

Yo, your picture of the "Belgium" telephone should have been "Belorussia." Not even close to Belgium, one of the low countries.

Frank
Seattle, WA

Leave us alone!

Dear *2600:*

I'm just writing to confirm and rebuke some of the things RepoMonster reported about in 15:3. Firstly, as you had suspected he did not overload the switch. What he did do was fill the girl's box. I know this by the experiences that I have had. Secondly, he probably did get a playback of a voice message (either the first or last message in the box). I had the same experience on a friend's voice mail when he was away on a trip, and again when my girlfriend was away. I thought nothing of it until I read the letter. Then I went about things more scientifically. I tried it again on my girlfriend's voice mail two times, on a business in the area, and on another friend at a school other then my girlfriend's. That makes four different systems with the same results on each. Lastly, I don't think there is a way to exploit this. The area that you call into seems effectively dead but it does not mess with other voice mail boxes on the same phone system. The only thing I can seem to find of use is to find out how many messages/how much time one box holds on any given system. It also sometimes makes their messages harder to retrieve.

Shaggy Dan

Dear *2600:*

In the 15:3 issue, the article "Expanding Caller ID Storage" dealt with a hack on CIDCO Caller ID units. I have a Model PA rev. D, contrary to the authors E and J revisions. On this unit you must solder a jumper to replace the Jumper C you are to disconnect. If the D jumper or none are soldered, the unit will remain at 25 calls. If the B jumper is soldered, the unit moves to 99 calls. The A jumper will provide a full 100 call capacity. Mixing the jumpers seems to leave the unit at either 25 or 99 calls. This is the only unit I have tried, but I am sure other revs, probably those under D, will need to have a jumper sol-

dered as well. I would bet that they redesigned to default back to 99 calls to save on having to waste time and pay to solder in the extra jumper. I bet that makes for a few more unemployed Malays.

Frogman

An Offer

Dear *2600:*

I am 15 and I live in the suburbs. I have been interested in the telephone system since I was seven. My grandfather worked for New York Telephone, along with my dad (he now works for Bell Atlantic). When my grandfather died we went to clean out his house. What I found changed me: an old rotary lineman's phone, a NY Telephone hard hat, and a tone generator. Ever since then I have been reading phreaking philes and other such things. So I am moving in January and am getting an Ethernet line from Bell Atlantic run to my *house!* The line has access to all of the Bell Atlantic servers! If you would like to trade me a username on your system for one on Bell Atlantic, let me know.

st

Regretfully, we only trade accounts with .mil users.

Military Madness

Dear *2600:*

Excellent magazine. Very useful for a network administrator. The candid information provided in your magazine has been very useful in closing network security gaps.

The military puts out some pretty good standards for Network Security. Too bad the military never reads them. As a system user inside the Washington Beltway, I was sickened by the lax system security enforcement. The military should look at itself before crying to the government for help. The simple act of choosing a halfway intelligent password seems beyond the average military user.

A brute force hack is a pretty simple quest. The military is the only place where you wear your resume on your clothing. It is *really* stupid to use something from your uniform for a password. Unfortunately, vanity wins out with the "leaders" I knew. I was very disappointed to see passwords like Airborne, SEAL, Ranger, Pathfinder, Recon. What was even more depressing was the use of "slang ranks" (JesusChrist, God, Headmen, TopKick, Grunt) as passwords.

The sad part of this is that Military clearly states how to properly construct a good password. Perhaps the "leadership" should read some of the policies they spew.

Dippy
Virginia

Dear *2600:*

I thought I would let the rest of the hacker community know about a web site where you can get a free CD sent to you about every 4-6 months. The CD is called *The Defense Acquisition Deskbook.* I haven't had much time to experiment with the CD, but it is full of DoD documents. Everything from how food is rationed on aircraft carriers to the way the government is run. I have found some information about computers and hacker prevention. I haven't had much time to look around the CD. Everything on it is unclassified but it's still pretty cool. The web site is www.deskbook.osd.mil - just go to that site and fill out an app. Within like a month or two you will receive the latest version of the deskbook. It's compatible with Winblows 3.x and 95, 98 as well as the Mac OS.

Virtual Vandal
Detroit

You'll only get it for free if you manage to convince them that you're part of a governmental agency. Otherwise you can get it for $30.

Thoughts and Reflections

Dear *2600:*

My compliments to *2600* and the principles it upholds. Your informative journalism with specific regards to the Kevin Mitnick case and your "freedom policy" with regards to the distribution of information in general are not only worthy accomplishments in themselves, but more importantly, have accomplished the vital task of motivating individuals to take action.

Not to sound like I'm giving an awards speech, but seeing people take serious action towards controlling the forces in their own lives ("Progress," 15:3) gives one reason to hope. On the other hand, reading the often misinformed and unrealistic remarks in the *2600* letters section gives one reason to doubt.

It is bad enough to live in a country where the media have left the average person so uninformed that they have become incapable of making rational decisions on an issue, and instead are easily swayed by "public opinion" and the dictates of their own ego.

Eric B. AKA Flyable George's letter (15:2) was a ludicrous (not to mention illogical) farce, which seemed dedicated to blaming the tribulations of hackers and the faults of society in general on *2600!* This is not a personal attack towards the writer and this letter is not intended to be a rebuttal. The point is that we are living in the misinformation age (what is being done to Kevin Mitnick exemplifies that) and the purpose of the hacker community must be to negate that, or there are only going to be more Mitnicks.

Ironically, being a hacker (unlike what the media would have us believe) is one of the most responsible positions a person can take in our society. This theme must be the motivating force of the hacker movement if it is to be of any merit for humanity in the long run. And while hacking is fun, reality is sobering. If hackers are going to be this moving force for the future, the petty "lamer newbie" bullshit has got to end. We all have come together so brilliantly in the defense of Mitnick, but if we are going to fight amongst ourselves then we have already lost.

Eric B., like anyone else who writes a letter to *2600,* represents a cross-section of society, but in particular, hacker society. The same letters section also contained a letter from The Informant, in which he accused the hacker community of racism. While this may or may not be true, *2600* editors rightly questioned this weighty accusation because he presented no evidence - if obtaining information is

the hacker's goal, why is a hacker writing an uninformative letter about a potentially very serious topic?

Then to top it off was the epitaph of DramaDame, which, I'm sure left others, like myself, in tears from laughter - my God. What role-playing game did you crawl out of? It serves more as a warning than anything else.

These are really just a few examples from one issue. Having been a *2600* reader for several years, the feelings of frustration after reading the letters section are not new, but finally grew to the proportion where I had to express them. It may be my imagination, but is what seems to be a more acerbic slant to the *2600* letters editorial arising from the same feelings?

Hackers, please look past the emotional quality of my rant, and realize that we don't need a hacker's constitution, just the love of information and truth that we claim we already have.

All information for all people.

BurningWorld
New York, USA

Dear *2600:*

I really admired the cover of issue 15:3. It sends the message that the immigrants who came to America received when they entered the country via Ellis Island. That Liberty has turned her back on them, as she is doing to Kevin, and may, sooner than we think, do to us. Keep spreading the word that history may soon repeat itself.

fl00dland

Dear *2600:*

I am a professional technologist working in public-sector computer networking. I came across your magazine while on a trip to the big city (I would never have seen your publication in a small town like mine). It looked interesting and I was curious. Several days later, I had time to read the 15:2 issue I had bought and it impressed me very much. Not the least of which was the underlying "honor among thieves" theme of most of your pieces. The issue left me with the sense that most hackers remain non-malicious in their activities. I learned that true hackers pursue their craft simply to enjoy its inherent intellectual challenges, to serve as watchguards for complacency in system security, and to advocate against undue and restrictive uses of technology by the corporate and military culture.

Please accept my encouragement to all of your readers, especially the younger ones, to continue the non-malicious pursuit of hacking, and to discourage malicious hacking by ostracizing those individuals from your community. Based on the single issue I've read, hacking seems to develop keen analytical and technical skills, as well as requiring one to consider what they believe to be right and wrong.

And I hope none of you mind if an old guy like me continues to enjoy (and learn from) your publication.

WG
Friday Harbor, WA

It's good to have you with us.

Atcom continued from pg. 47

booth, but feel free to experiment. Tell me if you find anything interesting.

Need more details? Here is the easy five step process:

1. Sit/stand in front of the Cyberbooth.
2. Click on "Cyberbooth Marketplace."
3. Click on "WinterNet." If Winternet isn't there anymore when you read this, improvise.
4. It seems WinterNet won a Microsoft "Best of the Net" award! Click on it.
5. Congratulations! You're off the free site, but who wants to spend time with Microsoft? Click on "Search."

You have reached Microsoft's Search Engine page. You can go pretty much anywhere from here. There are still some limits on what you can do. The biggest problem after this is that it won't allow you to type a URL. This shouldn't be a problem if you can get to a search engine, or maybe www.anonymizer.com. You will also be stuck with only a partial screen and what there is will be the Atcom Atbrowser. You might have some problems due to the Cyber Patrol software installed on the machine. It blocked Alta Vista searches on everything from *2600* to Disney, but it seemed to get along with Yahoo. It will block any page with "hack" in the title. It also blocks many "legitimate" pages. This program is nothing but trouble on this system.

Why is this bug here? They know it exists, yet they refuse to fix it. I can only speculate as to their motives. Perhaps the advertisers don't want their links limited. Much more likely is that someone at Atcom is lazy and doesn't want to get off his fat ass to fix it. If you're going to try this hack, try it soon, as they will probably fix it very fast now that it is public knowledge.

If you would like to find out more about the Atcom Cyberbooth, you can check out their web site at www.atcominfo.com or send e-mail to help@atcominfo.com. To find a Cyberbooth near you, go to:

www.atcominfo.com/cl-main.htm

le firewall

by Black Ice

Firewalls can stand between you and your destination. This doesn't mean that they always stop you from getting there, but they are watching you. I don't know many people who like to be watched, so here is some information about Checkpoint's Firewall-1 3.0b product, running on Solaris 2.5.1 with the latest patches. This is not a comprehensive article on Checkpoint, just some information you may enjoy.

My ISP uses a firewall between it and the Internet. This isn't revolutionary, except that is makes my 42K connection as slow as 28.8! This is because it is checking every packet that goes in and out of the ISP. You would figure that they would at least put the news feed somewhere else!

Checkpoint's FW-1 does what is called "Stateful Inspection." FW-1 checks every packet against a rule-set that the FW admin creates. The firewall can then accept, reject, encrypt, authenticate, or drop the packets according to the rule-set. The rules are based on, Source Address, Destination Address, Service (ie: http, icmp, dns, nntp, etc), Action (Reject, Drop, Accept), Logging Level (None, Short, Long, Alert, Mail, etc), and Time. The FW admin creates these rules to pertain to the level of security that is required. For example, if they only allow http traffic from the "external network" to an internal host, host A, then the rule-set would look something like figure 1.

This allows only http traffic to host A from the external network. FW-1 will drop any other packets from the external network, causing a timeout. All rules are based on IP addresses. These addresses have a slew of associated properties, one being a name for easier readability.

FW-1 also does Network Address Translation (NAT). With NATs you can hide the internal structure of your network from the outside world. This is very handy for corporations that have everyone surfing the web for "business purposes." Each user's IP address could be seen and a decent network map detailed from this information. With NATs the actual IP address behind the firewall is translated to another via rules. This is then the address that is propagated across the Internet. Now if someone sees this address and tries to attach to the network from the outside, the firewall will just drop the packet because the ARP request for that machine's MAC address will not exist.

Not all firewalls are created equal, and they all have their own bugs and problems. FW-1 does come with some proxies, such as telnetd and httpd, but it is not known as a proxy firewall.

So what's the magic cookie to get around these firewalls? It's the same as most everything else, human error. Here's a quick list of things you want to look at.

1. Easily hacked services such as sendmail, finger, etc., may still be left on the firewall. If you can break into the firewall machineÖ jackpot. Rules are held in /etc/fw/conf by default.

2. People do maintenance of the firewall that may leave the internal network susceptible for periods of time.

3. It is very easy to create non-secure rulesets that don't do what the creator wanted.

4. There's sometimes a backdoor. They may have the Internet locked tight, but the company's dial-in modems are open season.

5. Current patches aren't applied and lame attacks such as LAND will work.

6. The external router isn't protected.

7. Java/ActiveX attacks - as most firewalls pass this through and don't check.

8. Yada yada yada.

Most good firewall rules have a rule, which states that the firewall will drop and log all packets sent specifically to it. This is good because there should be no attempt to send pack-

Source	Destination	Service	Action	Log	Time
External Network	10.10.1.1	httpd	accept	long	any
ANY	ANY	ANY	drop	long	any

Figure 1 - Sample rule Set

ets directly to the firewall. This is a good indication that a box is a firewall if you know it exists. There are two ways to do this. Drop and Reject. Drop will just drop the packet and you will have to wait for your client to timeout. Whereas a reject may send a rejected packet back, depending on the protocol.

So you think to yourself all I have to do is find an open service and execute an Overlapping Fragment attack. The people who design firewalls are smart. I'll exit with this reasoning and implementation from FW-1.

Routers are often vulnerable to the Overlapping Fragments attack. In normal operation, the router passes the first fragment of a packet because it is allowed by the ACL (access control list). The router then passes the second fragment, as it routinely passes all non-first fragments. However, in an Overlapping Fragments attack, an intrusive fragment overwrites the end of the first fragment, resulting in the acceptance of a packet that should have been rejected by the ACL.

FireWall-1 prevents such attacks through a process we call "virtual defragmentation." In this case, the firewall only passes a fragment after it has internally reconstructed the full original packet. The FW-1 Inspection Engine only sees the full packet data - the same data that would be seen if the packet weren't fragmented. Using this scheme, no overlapping of fragments is permitted by the FW-1.

PHREAKING IN THE MIDWEST

by deth6 of the Bullz On Parade

I have read countless articles on phreaking and have found that many are outdated and/or apply to specific areas of the country like the east and west coasts and the north and southwest. However, I have failed to find much information on phreaking in the midwest, where there are definitely *tons* of phreakers or wanna-be's. So here is a tutorial on phreaking in that area, specifically Illinois. All the techniques described hereforth also apply to most parts of Missouri, Iowa, Ohio, Wisconsin, and Indiana, and I assume Michigan as well, although I'm not sure.

Unlike the boxes in the east which are opened with 7/16" allen wrenches, Illinois simply uses a 7/16" bolt to close its boxes. These boxes abound everywhere, especially in areas with underground lines like new subdivisions or isolated farm roads. They are pale green and come in assorted sizes, usually about three feet tall. They will usually say either "Illinois Bell" or "Ameritech" or something like that on them, and almost always have one of those "Call Julie Before You Dig" signs. There are two types of boxes, the green ones described above, and the huge five foot silver ones.

Once you have the damn thing open, you can see all the phone lines of the area lined up for you in myriads of screws, many of which are just unused lines that show up on caller ID as "Illinois Bell Telecom" and can be used to get free phone calls with a beige box. Don't bother stripping wires, just hook up directly to the screws.

Now go ahead, hook up whatever boxes you may have and go at it! A great example is the beige box, as you can listen in on other people's conversations and gain great knowledge for social engineering or learn great secrets about people. Another favorite trick of mine is to get an FM transmitter kit and hook it up with alligator clips to a line in the box. Then, close up the box and wait down the street in the safety of your car and tune in your radio to the frequency of the transmitter. These transmitters can be acquired from electronics companies like Marlin P. Jones and Associates through mail order. Call 800-652-6733 for a catalog.

Don't forget to watch out for cops and other assorted pork products as well as phone company linemen and trucks. These are *not* good for your health.

How To Hide From Netscape

by J.P.
trmbone@hotmail.com

Do you ever access sites that you don't want anyone to know about? In this article I will help you keep your privacy while you are looking at pages that might be of concern.

One day I was on the computer when I realized that I was on a questionable page (which is a nice term for a hacking page or something of the sort), and that in order to clear my tracks I would have to delete my history URLs on netscape, then clear that pop down list, plus I would have to clear the temporary Internet files, and that would do a good job of preventing people from seeing where I had been. To do this it would have taken me like 10 minutes, which is too long when your parents or boss or whoever want to see where you've been. So what I did was made a simple batch file to do all the dirty work.

Netscape stores its history file (netscape.hst) and preference files (prefs.js) in your user directory (in my case c:\program files\netscape\users\rusty\). In order to get a "clean copy" of netscape.hst I went into netscape and clicked Edit|Preferences then Clear history. Now to clear that damn drop down history list you have to edit the prefs.js file. Open it with Wordpad and delete the lines that look something like:

```
user_pref("browser.url_history.URL_1",
"www.2600.com");
user_pref("browser.url_history.URL_2",
"www.hacking.com");
```

Only delete those lines, or else you have screwed up your preferences for Netscape, and it is a pain to fix. Then after both files are clean, you can hide any suspicions by going to sites like www.pbs.com so no one will think you're up to anything.

Now that these two files are modified to your liking, make a copy of each one (netscape.hst and netscape2.hst).

Now you are ready to program your batch file. First of all you want to replace your old copies of your files with the cleaned up ones.

```
cd \progra~1\netscape\users\rusty\
del prefs.js
copy prefs2.js prefs.js
del netscape.hst
copy netscape2.hst netscape.hst
```

Now you need to clean your temporary Internet files.

```
cd \progra~1\netscape\users\rusty\cache\
del *.gif
del *.jpg
del *.htm
del *.txt
del *.wav
```

Note: The reason I didn't just do `del *.*` is because the fat.db is a very important file for netscape and can't be screwed up.

Be smart. Know that these examples don't always cover your ass. Basically this will keep your privacy on your home computer, and that's about it. Don't try this on your school's network which has programs on it to track your whereabouts on the Internet.

For Sale

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.

ORDER MY BOOK: *Y2K & YOU.* There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welsh, 11875 Pigeon Pass Rd., Ste. D-1-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

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.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. How to build a switchblade from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, newsletters and videos for only $1 (S&H). Our products cover information on hacking, phreaking, cracking, electronics, virii, anarchy and the Internet. Legit and recognized world-wide. Send your $1 US to: SotMESC, Box 573, Long Beach, MS 39560.

MS OFFICE '97 PRO ED (Standalone Install). New, unopened, authentic, registerable. No manuals included. On 1 CD-ROM $75. Undetectable virii (6) for DOS & MS Win 3.1. On 6 Disks, $6. Collections of choice, royalty-free art & photos. Ready to run as screensavers and/or wallpapers. On ZIP disks $15 each. E-mail or snail mail for catalog of collections. Cash, MO and checks accepted. The Omega Man, 8102 Furness Cove, Austin, TX 78753-5819. omegaman4@juno.com

PAOLO'S ONLINE: http://www.paolos.com. Not just the same old cheap pick sets and maybe a pick gun. We have access to the bleeding-edge locksmithing tools, from code books to safe penetration to '99 model auto entry! We specialize in special orders. Stop getting gouged/ripped off by lamer spy shops, and let us equip you with the latest and greatest in the trade. Also, switchblades, exotic weaponry, non-lethal self-defense, and more. Free password to our file archives with every order. Your BEST PRICE beat, and YOUR SATISFACTION GUARANTEED. Serving professionals since 1996.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCK PICKING, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd. #267, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 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 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

Help Wanted

HELP TO FIND VOICE MAILBOX PASSWORD. Password for voice mailbox lost. A new replacement

will erase all existing data including the voice mail box greeting. Will pay $75 to first person who can recover all digit (numerical) password. For details, e-mail: help-discover@usa.net

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

Wanted

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

Services

NO PRETEXTS! 100% LEGAL! Free non-pub/unlisted numbers. Free employment locates. Free recorded message - 24 hours. 1-800-555-5125 Ext. 92600.

THE FAMILY, a close knitted social group, has formed for all unappreciated, misunderstood hackers, phreakers, and computer nerds. We welcome you to join, with your kind, in furtherance of mutual love, peace, and prosperity. Master the possibilities of collective thought. Contact: Purcell Bronson, Drawer K, Dallas, PA 18612. (Attention: Michael Harris - lost your address. Please write again.)

INFORMATION ARCHIVES. Source codes, text files, DoD manuals, information for all! Catalog: $2 + one 32 cent stamp. NEW: INFO ARCHIVES will BUILD you a CUSTOM COMPUTER SYSTEM! From low-end systems to servers that use more power than Vegas, we can build it for you! Also: let us design and code your web page. For either of these services, please send us a letter describing the computer you would like built or the web page you would like constructed for a FREE cost estimate. Information Archives, J. Olsommer, PO Box 222, Lakeville, PA 18438.

SUSPECTED OR ACCUSED OF A CYBERCRIME? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (415) 560-6973 or omar@alumni.stanford.org. Free in-person consultation (to ensure confidentiality) for 2600 readers in the San Francisco Bay Area.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cybercrime@dmorrow.com. Extensive computer and legal background.

Personal

IN DESPERATE NEED OF FRIENDS AND MENTORS. I've been in prison going on 10 years and facing several more. I'm locked in a single man cell for 23 hours a day with no access to getting a better education except through free world help. Any and all correspondence will be greatly appreciated. Feel free to post this anywhere you deem appropriate. Ian D. Fields #524714, Hughes Unit, Rt. 2, Box 4400, Gatesville, TX 76597.

MY STARVING BRAIN IS STILL TRAPPED in a big Federal prison with 1,300 bums and nuts so I am asking you to help me escape (boredom and insanity) by mailing me any computer-related material you can spare. Sending me stuff (or even a short shout to say hi) is guaranteed to bring you good luck and a copy of my informative paper, "Proctor Prophecy," chock-full of humor, observations, and gleanings. Special request: I am seeking H/P correspondents in Richmond, VA and Palm Beach, FL. Tom Proctor, FCI 28204-004, Petersburg, VA 23804 (after 1/25/99 c/o 200 West Marshall Street, Richmond, VA 23220).

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: http://members.aol.com/BrazilByct

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

MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS

UNITED STATES

Alabama

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

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

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: EspressoNet on Regents Road (Vons Shopping Mall).

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

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 & Copans Rd.) in the food court.

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

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

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

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

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Aiea (Oahu): Internet Cafe, 559 Kapahulu Ave.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: La Piazza Cafe at 3845 North Broadway.

Indiana

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

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: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

Maine

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

Massachusetts

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

Northampton: JavaNet Cafe at 241 Main Street.

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.

Missouri

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

Nebraska

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

Nevada

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: Eastern Hills Mall (Clarence) by lockers near 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: Trivium Cafe on N. Main St.

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

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

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

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

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

Pennsylvania

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

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

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

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell & Pulteney Streets.

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

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

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

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

British Columbia

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

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

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

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) downstairs near the BT touchpoint terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

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

INDIA

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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

MEXICO

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

POLAND

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

RUSSIA

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

SCOTLAND

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

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.

It's safe to subscribe to 2600. We know a lot of you were afraid that we would disappear and take your money with us. Since we announced our financial problems last year, many of you haven't renewed your subscriptions and have instead gone to the newsstands. Since our problems are now behind us, even the most paranoid people no longer have anything to worry about. Of course, there's the possibility of your name being tracked by all kinds of monitoring agencies. But did you ever think of the risks of not subscribing? You could get hit by a bus crossing the street on the way to the bookstore or get involved in one of the many fights to the death that occur over the last issue on the stands. And those same monitoring agencies will find out what you bought anyway. So play it safe. Have 2600 delivered to the relative safety of your home or office at the same price we've had since 1991!

Name: _____ Amt. Enclosed: _____

Address: _____ Apt. #: _____

City: _____ State: _____ Zip: _____

Individual Subscription

O 1 Year - $21 O 2 Years - $38 O 3 Years - $54

Corporate Subscription

O 1 Year - $50 O 2 Years - $90 O 3 Years - $125

Overseas Subscription

O 1 Year, Individual - $30 O 1 Year, Corporate - $65

Lifetime Subscription

O $260

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

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

Historic Foreign Payphones

Found in Valparaiso, this Chilean phone could have been used by dictator Pinochet to call the CIA collect for instructions.

Photo by Vladimir Sanchez

This phone was seen in Phnom Penh, Cambodia and is rumored to have been used by Pol Pot himself for anonymous prank calls.

Photo by Celia Johnson

Nuwara Eliyah, Sri Lanka. Said to be the very phone where Arthur C. Clarke calls the Defcon voice bridge from.

Photo by Celia Johnson

From Izmir, Turkey - the ancient city of Smyrna. Supposedly used by Selim I in the heyday of the Ottoman Empire. (not verified)

Photo by Tom Mele

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