2600

"People who go to places of worship, people who go to libraries, people who are in chat rooms, are going to have 'Big Brother' listening in even though there's no evidence that they are involved in anything illegal whatsoever." - Laura Murphy, spokeswoman for the American Civil Liberties Union on the new surveillance powers given to the FBI

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
Dragorn, Porkchop

Cover Design
Mike Essl

Office Manager
Tampruf

Writers: Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, mlc, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmaster: Dominick LaTrappe

Web Assistance: Juintz, Kerry

Network Operations: CSS

Broadcast Coordinators: Juintz, Pete, daRonin, Digital Mercenary, Monarch, w3rd, Gehenna

IRC Admins: Antipent, Autojack, DaRonin, Digital Mercenary, Porkchop, Roadie

Inspirational Music: Doe Maar, Psychic TV, The Saints, Alice in Chains, Yoko Ono, Chumbawamba

Shout Outs: rms, Hope Cordes, Kyoske, Patrick, Christopher Bollman, Mark Hosler, Uzi Nissan, Rustu Recber

RIP: Jack Biello

Take Our Words

Fair Use and Abuse

We've reached a critical stage on so many different fronts that it's hard to imagine they're not all somehow intertwined. We shouldn't doubt our ability to influence change in whatever forum the battle we choose is being waged. This is the time to speak up.

Recent changes in the way our government works seem to no longer be about terrorism - if they ever were in the first place. As freedoms disappear and power becomes more centralized, a greater number of people are beginning to realize that we're moving into some very dangerous ground.

The "reorganization" of the FBI on May 29 was enough to shock a lot of us into paying attention. Now, all of a sudden, we no longer have an agency whose sole purpose is to investigate crimes. Their new reason for being is to prevent the crimes in the first place. Splendid, you might say. Anything that helps to stop crime has got to be a good thing, right? This is precisely what you're supposed to say. However, if you take an extra few minutes and think it through, you may come to the conclusion that this solution may indeed be a worse crime itself.

Let's look at what we're now facing. For the moment we'll confine it to the online world and the hacker culture. The FBI now no longer has to have any evidence of a crime being committed or even planned. They can wander onto IRC or an AOL chatroom and simply capture everything and then, at their leisure, look for things they don't like. The users responsible will then face a full investigation - all on the basis of words spoken in a public forum. The potential for targeting of certain individuals or even groups for prosecution is now in the stratosphere. People attending *2600* meetings will be subject to the same kind of scrutiny. Agents may now attempt to infiltrate organizations even when there is no sign of any criminal activity - just to keep an eye on things. If this doesn't make alarm bells go off in your head, there's probably not much we can say to make you see the distinct threat we're now all facing.

How much does this really have to do with hackers? Isn't this all about capturing terrorists and stopping really bad people from doing really bad things? That's what it was supposed to be. But clearly these goals have been subverted. According to a Fox News report on May 30, 2002:

"The FBI's top new marching orders will focus on terrorists, spies, and hackers, in that order." Granted, this is Fox News and they're liable to interpret anything from credit card fraud to online pornography as a derivation of computer hacking. The feds themselves refer to their new focus as "counterterrorism, counterintelligence, and cyber investigations." But the latter category in particular is so nebulous that literally anything that someone involved in computers might be doing would be open to scrutiny. And therein comes the proverbial chilling effect.

Not convinced yet? The FBI now can check various commercial databases and see what videos you've been renting, what books or magazines you're reading, what's popping up on your credit card bills, where you're traveling to, etc. Even your medical records won't be safe from their prying eyes. And all without any evidence that you've done anything wrong! In fact, approval from FBI headquarters is no longer even needed. Your local field office can do this on their own if they feel like it. And those who doubt that federal agents would abuse the power they hold need only look back at the Bernie S. case of the mid 90's.

In other countries government agents routinely infiltrate law-abiding groups of people who disagree with government policy. They then succeed in disrupting and dividing the group, at times even pushing them into illegal situations that never would have happened otherwise. And that gives the authorities carte blanche to move in. (In the United States we saw this occur decades ago with the FBI's counterintelligence program - dubbed COINTELPRO. Innocent people involved in the civil rights, antiwar, and countercultural movements were spied upon and harassed by these agents until such conduct was outlawed in the 70's.) Now this KGB style of dealing with dissidents, misfits, and individual thinkers has come back home wrapped in a flag. We can only wonder how many innocent people will be caught up in its wake.

It's an awfully odd coincidence that word of the FBI's apparent bungling of an investigation that might have detected the September 11 plot came literally days before the largest such reorganization in our nation's history. That story managed to convince a number of people that

change was needed. But the subsequent events managed to also slap a few faces out of their deep sleep of apathy and blind acceptance.

The fear now of course is that any resistance will be too little too late. But it doesn't have to be that way.

When we were sued two years ago by the motion picture industry, it caught a lot of us by surprise. The Digital Millennium Copyright Act was already law. What chance did we have to fight its existence? Was it not also too little too late?

We don't think it was. Nor do the thousands of people who supported us through the entire ordeal. And as we look around today, we realize that we have become so much stronger and more unified *as a result* of the action taken against us. We lost the case. And we lost the appeal. And, after considerable consultation, soul searching, and debate, we believe it's time to change the focus of this fight.

We wanted to take this all the way to the Supreme Court. But, as legal experts who know considerably more about the system than we do emphasized, there was an infinitesimal chance that they would even agree to hear the case and even less of a likelihood that we would win if they did. Both rejections ran the risk of setting the clock back as far as legal precedent went and this, quite frankly, is not the time to lose even more ground.

But, painful as this decision was to reach, we've come out of it learning something important. We've won. Maybe we weren't victorious in court but that doesn't exactly tell the whole story. Look around you. People have become aware of the evils of the DMCA. When this first started years ago, so few people knew anything about it - that's how it became law in the first place. But now it seems to be on everyone's minds as it becomes every bit as pervasive as we knew it would.

The industries that embrace the DMCA have fallen into disrepute with the general public as their true motives of sheer greed become more and more obvious. The recent attempt to charge fees for Internet broadcasting in the name of the DMCA outraged a whole new crowd of people. The efforts by the recording and motion picture industries to control and eventually bury any aspect of fair use by consumers has backfired horribly. People are realizing that such new (and mandatory) innovations as digital television will give them *less* freedom and flexibility if they don't challenge these laws. Attempts to control copying of CDs have ranged from the absurd to the criminal. It was recently discovered that simply using a magic marker to write over a certain section of a "copy-protected" CD was enough to defeat the entire system leading many to wonder if magic markers were now illegal access devices under the DMCA. And Macintosh users were horrified to discover that inserting one of these CDs into their machines would often cause actual damage to the machine! In fact, Philips, the company that *invented* the CD, says that these things don't even meet the definition of a CD and should not be sold as such. We encourage people who find these products in the CD section of a store to separate them to avoid confusion and false advertising, not to mention possible costly repairs for people who unknowingly try to play these things in their computers.

We'd like to say that our early battle with the DMCA was what started to wake people up. But it wouldn't be fair to those people who *really* did that job - the MPAA, the RIAA, and all of the other corporate and government colluders who joined forces to establish a stranglehold on the technology and dupe the public. Once their true colors became known, it was a foregone conclusion that they would begin to self-destruct in an expanding cloud of greed.

With the ominous changes in federal agencies, we are looked upon by many as little better than terrorists. Warped though that perception may be, we have to face the fact that this will overshadow the actual merits of our case. After all, when the MPAA started this whole thing, they *chose* us as the people they wanted to sue even though there were hundreds of others they could have gone after. Their reasoning was that as hackers, we would be summarily dismissed in the courts. Unfortunately, that proved to be true. But they most certainly didn't count on the massive rallying of support that came our way. It took courage and it took intelligence for individuals to stand up against what they knew was wrong. And now, unlike in 2000, the DMCA is being challenged on many fronts, not just ours.

So, while the stage may be shifting, the fight will intensify and see many more participants. We will not shy away from any of this nor lose sight of the ultimate objective, which is to repeal this horrible law once and for all and restore the right of fair use and free speech to the public.

It just got a lot harder with all the domestic spying, branding of hackers as terrorists, etc. But intensified pressure often in turn makes a battle all the more intense. While more seems to be at stake than ever before, we've never felt so far from defeat as we do now.

The Comprehensive Guide to
802.11b
Wireless Networks

by Dragorn

Wireless networking has been around for decades (fixed microwave links, laser links, ham packet radio), but Wireless Ethernet, aka WiFi (short for "wireless fidelity"), aka 802.11b has recently exploded in popularity for home and office use. As is too often the case with any new, widely adopted technology, the average consumer has little understanding of the impact of the little box with antennas that they just hooked up to their cable modem or that their office manager just told them to install on the network.

802.11b Background and Basics

802.11b is part of the 802.11 wireless family (which includes 802.11a and 802.11g, however neither are as widely used as 802.11b). Operating in the 2.4ghz unlicensed radio band, 802.11b is designed to offer up to 11mbit (closer to 6mbit usable) over short distances (typically less than 1500 feet) but with custom antennas and a clear line of sight, links of several miles are possible. Because it operates in the unlicensed band, no single corporation controls the airwaves. But unfortunately, this means there is also a lot of garbage floating in the 2.4ghz range of the spectrum along with the wireless data. Many cordless phones operate in the same frequency and household microwaves leak significant noise into the 2.4ghz range. Some wireless camera equipment (X10) uses the 2.4ghz range as well. WLANs also recently faced the threat of severely restricted transmission power due to a petition by Sirius satellite radio, however the complaint was recently withdrawn by the company.

802.11b operates in two modes - infrastructure, where dedicated access points (APs) act as the central points for a large number of clients and ad-hoc, where each client talks directly to other clients. In infrastructure mode, each client needs only to be able to see the AP (or another AP in the same distribution system) - two clients need not see each other directly because the AP will relay traffic. In ad-hoc, every client must be in range of every other client. In either operational mode, it is, by definition, a shared media network - everyone can see all the traffic in the air or, at least, all the traffic in the air that they are in range of.

Each 802.11b network is given a Service Set Identifier, or SSID. This is the name of the network, which all clients use to identify which network they are communicating with. Networks operate on one of 12 (in the US) or 14 (international) channels. Most wireless setups will automatically select the best signal out of all the network points sharing the same SSID.

802.11b has link-layer encryption called Wired Equivalence Protection, or WEP. WEP uses RC4 in 40, 64, 128, or on some recent cards, 256 bit encryption. While never designed to provide a tremendous amount of security (wired equivalence implying "as secure as a shared media wired network," which, as anyone running a sniffer on a wired shared media network can tell you, isn't very secure), additional flaws have been found in WEP which allow key attacks against data encrypted by many manufacturers. More on this later.

```
dragorn@gir.lan.nerv-un.net:/home/dragorn                      o o o
Networks--(Autofit)------------------------------------   ┌─Info──┐
   Name                      T W Ch Packets Flags Data Weak   ||        |
   kogo                      A Y 11    353          3    0  || Ntwrks |
   SpeedStream               A N 11    194          0    0  ||   448  |
   SYSTEM                    A Y 06     28          0    0  || Pckets |
   flakat                    A Y 01   3305        273    0  || 118708 |
   AirPort Network 22bad7    A N 01    279          2    0  || Cryptd |
  | flakat                   A Y 06    131          2    0  ||   1777 |
  | Paul4A                   A Y 06    315          1    0  ||  Weak  |
  | Ipt4692eB                A Y 06    362          0    0  ||     0  |
  | Tcholakian               A Y 06    374        129    0  || Noise  |
    Airport Base B461 (Toy Fr A N 01   99  A2     68    0  ||  2035  |
    Fisher                   A Y 01     34          0    0  || Discrd |
    KCA Network              A N 01     96          1    0  ||  2434  |
    Airport Base  C811 (Fashi A N 01   15  A3     10    0  || Pkts/s |
    Tcholakian               P N --      1          0    0  ||    28  |
    Home                     A Y 07      1          0    0  || Elapsd |
 Lat 40.750 Lon -73.994 Alt 32.3f Spd 7.940m/h Fix NONE---  └013227─┘
┌─Status─────────────────────────────────────────────────────────────┐
| Found new network "Home" bssid 00:50:18:07:74:9A WEP Y Ch 7 @ 11.00 mbit |
| Found new network "Tcholakian" bssid 00:30:65:1B:B1:5C WEP N Ch 0 @ 0.00 mbi |
| Found IP range for "Airport Base  C811 (Fashion)" via ARP 143.55.179.0 |
| Found new network "Airport Base  C811 (Fashion)" bssid 00:02:2D:1F:6B:61 WEP |
└Battery: 17% 0h39m0s──────────────────────────────────────────────────┘
```

802.11b Packet Types

The most common types of 802.11b packets are:

1. Beacon packets. Typically, access points continually transmit beacon packets containing their SSID, maximum transfer rate, and MAC address of the access point. Most APs send between six and ten beacon packets a second continually.

2. Probe packets. When a client tries to join a network it sends a probe request packet containing the SSID of the network it wishes to join. If an access point allows the client to associate with the network, it responds with a probe response, also containing the SSID.

3. Data packets. Typically, these are just

TCP/IP encapsulated in the 802.11 frames.

4. Ad-hoc packets. These are no different than data packets except they are sent card to card instead of through an access point.

Detecting 802.11b Networks

There are two primary methods for detecting wireless networks, utilized by different programs.

1. Active detection, where the client transmits probe requests and looks for networks that respond to them.

Positive: Sometimes able to detect cloaked networks, does not require a card or driver capable of RF Monitor support.

Negative: Requires the client to be within transmit range of the access point for it to be detected, generates traffic on the target network which can be traced, and lies on questionable legal ground so far as actively joining a network is concerned.

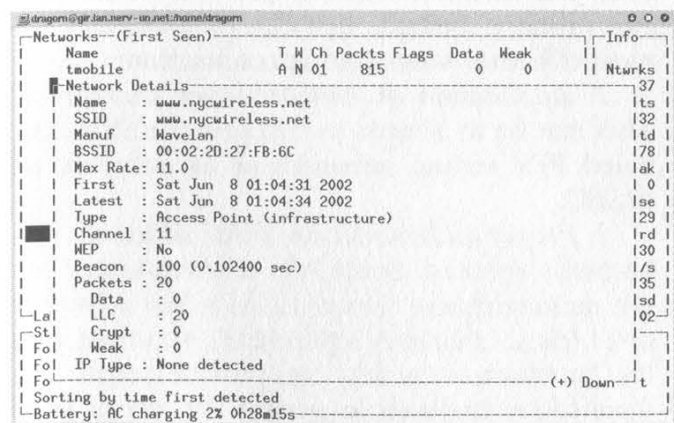*Used by:* NetStumbler (www.netstumbler.com, Windows).

2. Passive detection, where the client listens to all wireless traffic in the air and extracts information from the packets found.

Positive: Client needs only to be within receive range to detect a network, no traffic is generated which can be observed. Passive sniffers are also capable of recording data packets for additional dissection.

Negative: Requires a card and driver capable of RF Monitor support, which enables raw packet detection. Cannot detect a non-beaconing network with no data traffic.

Used by: Kismet (www.kismetwireless.net, Linux/BSD), Wellenreiter (www.remote-exploit.org, Linux), Airsnort (airsnort.shmoo.com, Linux), and others.

Using passive sniffing it is essentially impossible to detect someone monitoring your network. No traffic is generated by the sniffer and, even in "secure" environments, a handheld such as the Ipaq or Zaurus are more than capable of capturing traffic and can easily be kept in a jacket pocket or bag.

```
dragorn@girian.nerv-un.net:/home/dragorn                  o o o
┌Networks──(First Seen)──────────────────────────────┬Info─┐
│    Name                T W Ch Packts Flags Data Weak │ │     │
│    tmobile             A N 01    815         0    0  │ │ Ntwrks │
│  ┌Network Details──────────────────────────────────────37 │
│  │ Name    : www.nycwireless.net                        │ts │
│  │ SSID    : www.nycwireless.net                        │32 │
│  │ Manuf   : Wavelan                                    │td │
│  │ BSSID   : 00:02:2D:27:FB:6C                          │78 │
│  │ Max Rate: 11.0                                       │ak │
│  │ First   : Sat Jun  8 01:04:31 2002                   │0  │
│  │ Latest  : Sat Jun  8 01:04:34 2002                   │se │
│  │ Type    : Access Point (infrastructure)              │29 │
│  │ Channel : 11                                         │rd │
│  │ WEP     : No                                         │30 │
│  │ Beacon  : 100 (0.102400 sec)                         │/s │
│  │ Packets : 20                                         │35 │
│  │  Data   : 0                                          │sd │
│ └Lal LLC   : 20                                        │02─┘
┌St│ Crypt   : 0                                          │
│ Fo│ Weak    : 0                                          │
│ Fo│ IP Type : None detected                              │
│ Fo└────────────────────────────────────(+) Down──┘t
│ Sorting by time first detected
└Battery: AC charging 2% 0h28m15s────────────────────────
```

Passive monitoring of wireless data opens many advantages for tracking and analyzing networks. The level of monitoring possible varies depending on the type of card used. Cisco cards use a very fast hardware channel hopping method, which allows them to scan all of the channels transparently. Prism2 cards must do channel hopping to detect all the 802.11b channels, spending a small amount of time on each channel - most wireless sniffers include this capability either internally or as a helper application (Kismet uses "prism2_hopper" to hop three channels per second).

The most simplistic information is in the 802.11b headers - the MAC of the source, destination, and access point systems, the direction of communication, the channel, SSID, WEP, and supported transfer rates. Cisco access points even include an extra status field that often contains information about the function of the equipment, and sometimes even the location of the wireless access point.

Far more information can be gathered by dissecting the data packets of unencrypted networks - FTP, telnet, HTTP, POP, and IMAP traffic are all as vulnerable to observation as they would be in an unswitched ethernet network. ARP, UDP, and especially DHCP can be used to detect the IP ranges used by the network.

Basic sniffing can be done with almost any wireless card, but some are better than others. Most consumer wireless cards are underpowered, only capable of detecting strong signals, and don't support external antennas. Orinoco cards are more powerful than most, and support antennas, however it is not always possible to do full RFMon mode, which is required for passive monitoring (there are patches to the Linux Orinoco drivers but they only work on some firmware versions). While not perfect, one of the best cards for general sniffing is the Cisco AIR-LMC350 which has dual antenna jacks, 100mW transmit, and -95dBM sensitivity (compared to 20-30mW transmit for most prism2 cards and -80dBM sensitivity). As mentioned before, the Cisco chipset uses a very fast internal channel hopping scheme, which can sometimes result in missed packets if a single channel is saturated, but overall the performance of the card is excellent. It can be obtained through online retailers for approximately $110 US.

Equally important is a proper antenna - remember that a car is just a big metal box, and metal boxes are not good for radio signals. A car-mounted antenna, while not absolutely necessary, will often triple the amount of data received. 5db gain magnetic-mount antennas can usually be found for $60 US.

The Myth (and truth) of WEP, SSID Cloaking, and Non-Beaconing

WEP is alternately touted as the only protection you'll ever need, and so weak it's not worth enabling. The truth lies, as always, somewhere in the middle - all, or nearly all, modern chipsets include workarounds for the flaws in WEP key generation, however all it takes is a single older system on your network (access point *or* client) to expose the key.

```
 dragorn@gir.lan.nerv-un.net:/home/dragorn                        o o o
,-Networks--(Autofit)----------------------------------,-Info-,
I  Name                    T W Ch Packts Flags  Data Weak  II      I
I  I fl,-Statistics--------------------------------------,twrks I
I    Ail  Start   : Sat Jun  8 01:02:35 2002          I  202 I
I    <nl  Networks: 202                                Ickets I
I    lil  Encrypted: 61 (30%)                          I33660 I
I    del  Default  : 32 (15%)                          Iryptd I
I    Zol  Max. Packet Rate: 82 packets/sec             I  621 I
I    Zol  Channel Usage:                               I Weak I
I    hol  -----------------------------------------     I   0 I
I    HOI        X                   01: 31 (15%) I 02:   0 (00%) INoise I
I    ATI        X                   03:  6 (02%) I 04:   3 (01%) I  722 I
I    lil        X                   05:  4 (01%) I 06:  99 (49%) Iiscrd I
I    pal        X                   07:  2 (00%) I 08:   1 (00%) I  841 I
I    del        X                   09:  4 (01%) I 10:   5 (02%) Ikts/s I
I    0al  X     X         X         11: 37 (18%) I 12:   0 (00%) I   21 I
I    .10I  X     X         X         13:  0 (00%) I 14:   0 (00%) Ilapsd I
L-Lat 40I  -----------------------------------------     I03302-'
,-Statusl  1 2 3 4 5 6 7 8 9 1 1 1 1 1                  I         I
I Found I              0 1 2 3 4                        I         I
I Found L----------------------------------------------Ibit   I
I Found                                                Imbit   I
I Saving data files.                                   I         I
L-Battery: AC charging 6% 0h28m15s----------------------'
```

WEP only encrypts data packets - link layer packets such as joining, beaconing, probes, etc. are left unencrypted. Actually cracking the WEP key depends on the key length, the number of flawed systems generating traffic, and the traffic levels on the network - if there are no systems generating data traffic, you will never have the opportunity to capture weak keys. The most important factor is time - typically only one or two in thousands of packets contains a weak key, and current key attacks require thousands of weak keys to extract the full key.

Various dictionary-based brute force attacks are under development, but will of course have the same weakness of any brute force attack - beyond the expected range of likely keys it becomes time consuming number crunching.

WEP has the additional flaw of being a shared private-key encryption method. Once your key is cracked (or otherwise compromised by system being cracked, insecure means of giving the key to personnel or other network users, an employee leaving, or even an employee losing a wireless-enabled handheld), all systems must be updated with a new WEP key, which has the same weaknesses and vulnerabilities as the previous one.

Coupled with additional security (as discussed later), WEP can be a useful deterrent, however it is by no means sufficient as the only line of defense - while it may foil the casual sniffer, a determined attacker with the rights tools stands a good chance of breaching your network.

In a further attempt to make consumer hardware more secure, or to at least appear more secure, many manufacturers include SSID "cloaking," where the SSID is blanked from the beacon packets. Unless a client knows the correct SSID, it cannot join the network. Unfortunately, this "protection" is completely transparent - once a client joins the network, the SSID is sent by the client and the AP in cleartext (even if WEP is enabled - remember, WEP only encrypts data packets, not link packets). Kismet automatically detects this exchange and fills in the network SSID. If you have users on your network, your SSID will be exposed.

Several physical attacks (of varying legality) are possible to force a cloaked network to disclose the SSID - when a card gets a weak signal or loses the signal, it attempts to rejoin the network, disclosing the SSID. Any 2.4ghz RF interference strong enough to disrupt the network and cause systems to rejoin will, in addition to being against all FCC regulations, happily cause a disclosure of the SSID.

The second common trick favored by manufacturers to try to protect AP's is to disable beaconing entirely. While not completely in accordance with the 802.11b specifications, this doesn't cause major problems for normal operation. However this, like SSID cloaking, does not provide any significant protection. Any data traveling over the network can still be seen, and the SSID is disclosed in the same fashion as the cloaked SSID by users joining the network.

```
 dragorn@gir.lan.nerv-un.net:/home/dragorn                        o o o
,-Networks--(Autofit)----------------------------------,-Info-,
I   Name                     T W Ch Packts Flags  Data Weak  II Ntwrks I
I   <no ssid>                A Y 11    30          8    0    II     06 I
I  ,-Data Strings Dump--------------------------------------,      Its I
I  I FHEPFCELEHFCEPFFFACACACACACACABM                       I     I63 I
I  I EGENEHFPDADJDJDADIDJDICACACACACA                       I     Itd I
I  I EGENEHCACACACACACACACACACACACABN                       I     I88 I
I  I \MAILSLOT\BROWSE                                       I     Iak I
I  I FMG_0990898                                            I      0 I
I  I FastEthernet0/22                                       I     Ise I
I  I Cisco Internetwork Operating System Software           I     Ird I
I  I IOS (tm) C2900XL Software (C2900XL-C3H2S-M). Version 12.0(5)XU, RE I 133 I
I  I Copyright (c) 1986-2000 by cisco Systems, Inc.          I     I/s I
I  I Compiled Mon 03-Apr-00 16:37 by swati                   I    I12 I
I  I cisco WS-C2924-XL                                       I    Isd I
I  I EGENEHFPDADJDJDJDJCACACACACACACA                        I   I40-'
L-Lal  I EGENEHCACACACACACACACACACACACABN                    I---
,-Stl  I \MAILSLOT\BROWSE                                     I
I Fol  I FMG_09999                                            Ibi I
I Fol  I W"CeP                                                Iit I
I Sal  I `kw7e+
I Found new network "<no ssid>" bssid 00:40:96:31:92:73 WEP N Ch 9 @ 2.00 mbit I
L-Battery: AC charging 2% 0h28m15s----------------------------'
```
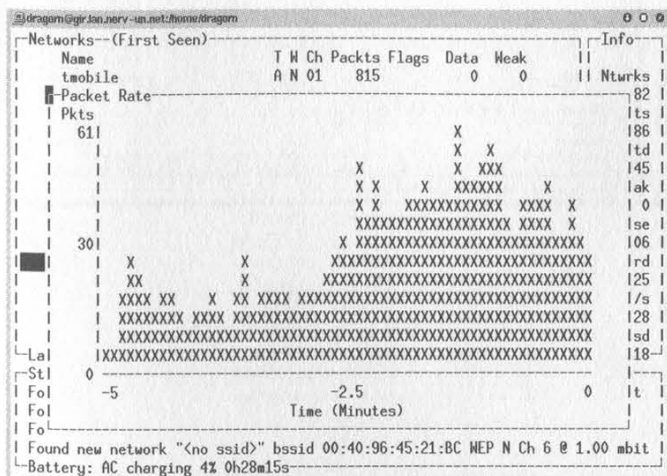
Securing Wireless Networks

After all of the above doom and gloom, how does one secure a wireless network? There are two primary methods that can be used, and are most effective when used in conjunction:

1. Application or network-layer encryption. This can be as simple as SSH (or an SSH-tunneled PPP virtual network) or as complex as IPSEC.
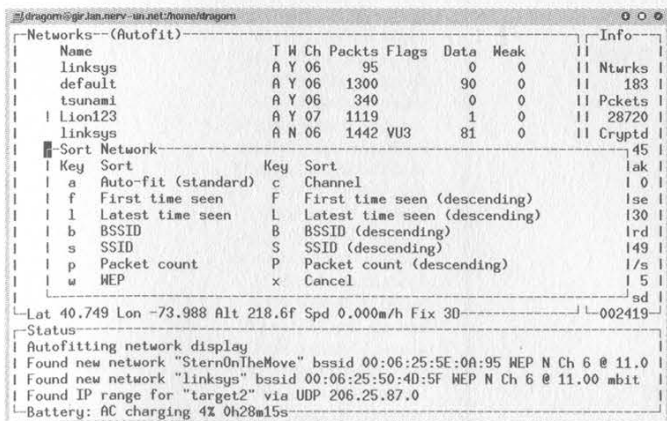
2. Proper authentication. MAC addresses can be easily spoofed. Some APs offer enhanced login authentication (Cisco LEAP). For APs that don't (most consumer equipment), solutions like NoCat (www.nocat.net) can provide secure authentication methods to protect the rest of your network from the wireless segment.

3. *Properly tuned equipment.* Don't assume stronger is better! Always use the minimum power possible for your network and select your antennas appropriately. Not only is it good for security, this will help reduce the congestion in the 2.4ghz band.

```
dragorn@girlan.nerv-un.net:/home/dragorn                    0 0 0
┌Networks──(First Seen)────────────────────────────┐┌─Info─┐
│   Name                 T W Ch Packts Flags Data  Weak ││      │
│   tmobile              A N 01   815          0     0  ││ Ntwrks│
│ ┌Packet Rate──────────────────────────────────────┐  │82  │
│ │ Pkts                                             │  │ts  │
│ │  61│                          X                  │  │86  │
│ │    │                          X  X               │  │td  │
│ │    │            X          X XXX                 │  │45  │
│ │    │           XX X    X  XXXXXX       X         │  │ak  │
│ │    │           XX X  XXXXXXXXXXX  XXXX X         │  │0   │
│ │    │           XXXXXXXXXXXXXXXXXX XXXX X         │  │se  │
│ │  30│           X XXXXXXXXXXXXXXXXXXXXXXXXXX       │  │06  │
│█│    │ X       X  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX    │  │rd  │
│ │    │ XX      X  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX    │  │25  │
│ │    │ XXXX XX  X XX XXXX XXXXXXXXXXXXXXXXXXXXXXXX  │  │/s  │
│ │    │ XXXXXXX XXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  │  │28  │
│ │    │ XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX │  │sd  │
│└La│  │XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX│  │18─│
│┌St│  0 ─────────────────────────────────────────  │──│───│
│ Fo│  -5               -2.5                    0    ││t   │
│ Fo│                Time (Minutes)                  ││    │
│ Fo└───────────────────────────────────────────────┘│    │
│ Found new network "<no ssid>" bssid 00:40:96:45:21:BC WEP N Ch 6 @ 1.00 mbit │
└Battery: AC charging 4% 0h28m15s──────────────────────────────┘
```

Community Wireless Networks

Wireless networks provide a phenomenal level of networking possibilities. Most urban areas have at least one wireless users' group aimed at building a free, community wireless network. Often called a wireless mesh or a parasitic grid, community networks aim at blanketing a city (or parts of a city) with free broadband access. Groups such as NYCWireless (www.nycwireless.net, New York City, NY), BAWIA (www.bawia.net, Boston, MA) and Personal-Telco (www.personaltelco.net) have already made significant inroads into providing wireless public networks.

```
dragorn@girlan.nerv-un.net:/home/dragorn                    0 0 0
┌Networks──(Autofit)───────────────────────────────┐┌─Info─┐
│   Name                 T W Ch Packts Flags Data Weak ││      │
│   linksys              A Y 06   95           0    0  ││ Ntwrks│
│   default              A Y 06  1300         90    0  ││  183 │
│   tsunami              A Y 06   340          0    0  ││ Pckets│
│ │ Lion123              A Y 07  1119          1    0  ││ 28720│
│   linksys              A N 06  1442 VU3     81    0  ││ Cryptd│
│ ┌Sort Network──────────────────────────────────────┐ │45  │
│ │ Key  Sort              Key  Sort                 │ │ak  │
│ │  a   Auto-fit (standard)  c   Channel            │ │0   │
│ │  f   First time seen   F    First time seen (descending) │se │
│ │  l   Latest time seen  L    Latest time seen (descending)│30 │
│ │  b   BSSID             B    BSSID (descending)   │ │rd  │
│ │  s   SSID              S    SSID (descending)    │ │49  │
│ │  p   Packet count      P    Packet count (descending)│/s │
│ │  w   WEP               x    Cancel               │ │5   │
│ │                                                  │ │sd  │
│ └Lat 40.749 Lon -73.988 Alt 218.6f Spd 0.000m/h Fix 3D─┘ └─002419─│
│┌Status──────────────────────────────────────────────────────┐
│ Autofitting network display                                  │
│ Found new network "SternOnTheMove" bssid 00:06:25:5E:0A:95 WEP N Ch 6 @ 11.0 │
│ Found new network "linksys" bssid 00:06:25:50:4D:5F WEP N Ch 6 @ 11.00 mbit │
│ Found IP range for "target2" via UDP 206.25.87.0                            │
│└Battery: AC charging 4% 0h28m15s───────────────────────────────┘
```

Community wireless networks offer an alternative to "big business" broadband and can often get broadband to areas unreachable by conventional means, and can provide a completely independent means of transport for free information without relying on any corporate services or resources. After September 11, the NYCWireless group was involved in bringing back connectivity to areas left without links that the large providers had not been able to restore.

While uncommon, sometimes companies (knowingly) share their wireless networks. Akamai in Boston allows public use of their wireless network equipment, which covers most of Cambridge, with minimal filtering of outgoing traffic (SSH and HTTP both work fine).

In most cases, donating a node to a community network is as simple as putting an access point on a broadband connection (cable, DSL, or other) with a public SSID and registering it with the group of your choice. The web site for a wireless group in your area should contain all the information you need to join.

Threats to 802.11b

802.11b in general and community networks specifically face several hurdles in the near future. Broadband companies are beginning to crack down on the sharing of access and on users who utilize the full bandwidth allocated to them. Connection sharing is already against the acceptable use agreements of most broadband providers, and not far away for most others, and should providers begin charging per megabyte over an arbitrary quota (as Time Warner/Road-Runner is considering), free public broadband could quickly become a thing of the past.

Also, in many urban areas (and even less urban areas) the airspace available for wireless networks is becoming saturated. Just like collisions in shared-media ethernet, as more wireless networks with overlapping signals are in an area, less bandwidth is available for each. Non-802.11b devices like phones, microwaves, cameras, and even a planned microwave-based lighting system all leak noise into the air that further degrades 802.11b signals.

Finally, while the current 802.11b equipment is well understood and supported with open source drivers, manufacturers are aggressively discouraging community-developed drivers for 802.11a hardware, and in fact as of the time of this writing it is completely unsupported in Linux.

Practical Examples

To gather the data for the cover we used a Cisco card, magmount antenna on the roof, a Garmin GPS, and Kismet. In an hour and a half, we found 448 networks. In the center of Manhattan, an area which arguably should be more security aware than anywhere else, only 26 percent of the networks had encryption enabled. At least 75 of the access points were factory configurations, with all the default access granted.

Plaintext data included searches on outpost.com, an individual with 129 email messages (every single one of them porn spam), books purchased at Barnes and Noble, IRC sessions, instant messenger conversations, browsing at the Fry's website, Windows Network Neigh-

borhood file transfers, data from globix.net, uPNP services looking for drivers, and more.

Vulnerable networks ranged from personal systems in apartments, law firms, book stores, and news companies. At the very least they exposed all of the data handled by the company, and at the worst presented an easy entrance into the corporate network. Wireless demo units are often plugged in behind the corporate firewalls of retail stores (Office Depot for months ran a default Linksys demo unit plugged into the corporate network behind the firewall).

```
dragorn@gir.lan.nerv-un.net:/home/dragorn                      o o o
Networks--(Autofit)------------------------------------  -Info-
  Name                T W Ch Packts Flags Data Weak   ||
 ko█ -Statistics----                                     -twrks-
 Ri| Start    : Sat Jun 8 01:02:35 2002                  | 448 |
 Sp| Networks: 448                                       |ckets|
 fl| Encrypted: 120 (26%)                                |18237|
 Ai| Default  : 75 (16%)                                 |ryptd|
 fl| Max. Packet Rate: 402 packets/sec                   | 1775|
 Pa| Channel Usage:                                      | Weak|
 Ip| ------------------                                  |   0 |
 Tc|        X              01: 91 (20%) | 02:   0 (00%)  |Noise|
 Ai|        X              03: 13 (02%) | 04:   3 (00%)  | 2024|
 Fi|        X              05:  6 (01%) | 06: 236 (52%)  |iscrd|
 KC|        X              07:  6 (01%) | 08:   1 (00%)  | 2423|
 Ai|        X              09:  5 (01%) | 10:  12 (02%)  |kts/s|
 Tc| X      X              11: 51 (11%) | 12:   0 (00%)  |  27 |
 Ho| X      X       X      13:  0 (00%) | 14:   0 (00%)  |lapsd|
Lat 401                                                  |13210|
-Status-    1 2 3 4 5 6 7 8 9 1 1 1 1 1                  -
 Found |                    0 1 2 3 4                    |t
 Found |                                                 |0 mbi
 Found |
 Found new network "Airport Base  C811 (Fashion)" bssid 00:02:2D:1F:6B:61 WEP
Battery: AC charging 16% 0h28m15s
```

Books processed at Barnes and Nobles during the June 7 2600 meeting:

Good Old Coney Island, Ingram Book Company, $19.95
Times Square Roulette, MIT Press, $59.95
Art of the State: New York, Abrams, Harry H. Inc, $12.95
AIA Architectural Guide, $14.95
New York Design Index, Norton Publishing, $59.95
New York's Architects, $12.95
Stone and Steel : Paintings & Writings Celebrating the Bridges of New York City, Baker & Taylor, $30.00
NY Yankees Collection, Ingram Book Company, $24.95
When the Tripods Came, Simon and Schuster, $4.99
Pool of Fire, Simon and Schuster, $4.99
City of Gold and Lead, Simon and Schuster, $4.99
White Mountains, Simon and Schuster, $4.99
Rainbow Jordan, Harper Collins, $4.99
Extreme Teen Bible Just A Future With A Promise, Thomas Nelson Inc, $19.99
Rise of New York, Yale University Press, $30.00
Long Island Country, Norton Publishing, $85.00
The Rockefeller Family, Abbeville Press Inc, $49.95
Truth or Dairy, Harper Collins, $6.95
Wurst Case Scenario, Harper Collins, $6.95
My so-called Life, Random House, $4.99
Chernowitz!, Penguin/Putnam Paper, $5.99
Where the Lilies Bloom, Harper Collins, $5.95
Children of the River, Random House Inc, $5.99
Athletic Shorts: Six, Random House Inc, $4.99
Drifter, Simon and Schuster, $3.99
Stotan!, Random House Inc, $4.99
Ironman, Random House Inc, $4.99
Crazy Horse Electric, Random House Inc, $4.99
Old Magic, Simon and Schuster, $4.99
Watsons Go To Bermin, Random House Inc, $5.99
Neon Genesis Evangelion, Publishers Group West, $15.95
Star Wars: Dark Empires, LPC Group, $17.95
Gift of Magic, Random House Inc, $4.99

Wireless networks found in Midtown Manhattan:

tmobile, 00:40:96:31:B7:B2
411Base, 00:30:65:14:C0:52
yogaunion, 00:60:1D:F0:87:C2
alpina-networks, 00:05:5D:DA:0A:96
425pas, 00:02:2D:08:8D:9E
WLAN, 00:01:24:F0:7E:C3
WLAN, 00:04:E2:0E:BE:8D
WLAN GMG, 00:01:24:F0:1A:9C
86904AGROUP, 00:02:2D:0D:36:22
<no ssid>, 00:02:2D:03:55:4C
www.nycwireless.net, 00:02:2D:27:FB:6C
MLNET, 00:04:5A:0E:32:EF
WLAN, 00:04:E2:0E:60:C3
104, 00:03:47:15:BF:75
chazroot, 00:10:2B:01:19:32
chazroot, 00:03:2F:01:32:DE
linksys, 00:04:5A:D2:39:C1
tsunami, 00:40:96:28:65:07
training, 00:04:5A:CF:92:75
linksys, 00:04:5A:0E:83:9E
linksys, 00:06:25:5D:7B:A3
linksys, 00:04:5A:FC:EE:7F
linksys, 00:04:5A:CF:DE:7B
linksys, 00:06:25:60:B6:B7
linksys, 00:04:5A:FC:FF:67
<no ssid>, 00:40:96:42:B1:5D
<no ssid>, 00:40:96:38:0F:BB
linksys, 00:06:25:53:26:2C
default, 00:40:05:DF:0C:17
linksys, 00:04:5A:2F:D5:27
DavisCam, 00:D0:D8:60:02:29

tsunami, 00:40:96:54:A2:AC
SSI, 00:60:1D:22:9E:F7
linksys, 00:04:5A:2E:30:B1
linksys, 00:04:5A:2F:E8:F1
Cesar-Buckner, 00:06:25:60:2A:5B
Theater, 00:50:DA:93:7C:8A
EF5535, 00:60:1D:1E:69:E7
Apple Network 300c52, 00:02:2D:30:0C:52
101, 00:50:DA:00:6D:CC
OptecInc, 00:30:AB:09:A5:F1
kogo, 00:60:1D:21:96:EF
lfap, 00:06:25:60:33:1F
linksys, 00:04:5A:F1:5F:14
connect.02, 00:40:96:49:11:9C
linksys, 00:04:5A:DA:3E:6F
default, 00:01:24:F0:21:9B
rlmpr, 00:04:5A:26:68:0B
<no ssid>, 00:40:96:41:C5:55
linksys, 00:06:25:5F:D4:7B
default, 00:05:5D:F1:E6:74
bryny2, 00:40:96:2A:95:FE
linksys, 00:04:5A:DD:59:83
linksys, 00:04:5A:0E:32:3A
celerity, 00:04:5A:26:D3:6D
linksys, 00:04:5A:0E:19:70
3Com, 00:04:76:A5:C4:E1
<no ssid>, 00:40:96:29:B8:49
mystic, 00:50:DA:01:FA:8C
SpeedStream, 00:01:24:F0:C8:6F
RiskVal, 00:40:05:DF:52:F5
interact, 00:01:24:F0:1E:6E
WLAN, 00:90:D1:01:2B:2E
<no ssid>, 00:E0:63:50:AD:90
Airport Base B461 (Toy Window), 00:02:2D:1B:7D:17
101, 00:01:03:78:DB:04
SYSTEM, 00:04:5A:DD:3A:81
flakat, 00:04:75:61:47:DD
AirPort Network 22bad7, 00:60:1D:22:BA:D7
default, 00:90:4B:08:4A:44
flakat, 00:04:75:61:79:6A
Paul4A, 00:30:65:1D:11:78
Ipt4692eB, 00:40:96:43:CB:22
linksysupiker, 00:04:5A:2D:D2:57
<no ssid>, 00:40:96:32:D6:17
Tcholakian, 00:30:65:14:B6:6A
WLAN, 00:30:F1:26:FD:93
WLAN, 00:30:F1:10:1E:2F
WLAN, 00:01:24:F0:77:7B
bay9, 00:40:96:34:89:19
<no ssid>, 00:40:96:33:30:25
<no ssid>, 00:40:96:2A:8B:1F
CSR-Airport1, 00:60:1D:22:C1:34
NYCSR022 Imac, 00:30:65:08:45:16
tsunami, 00:40:96:41:33:90
contino, 00:50:18:06:68:C0
Lion123, 00:04:5A:0E:59:92
linksys, 00:06:25:60:8C:BD
linksys, 00:06:25:54:1E:07
default, 00:90:4B:08:38:2B
linksys, 00:04:5A:0E:8A:03
hudson, 00:05:5D:DA:30:EE
linksys, 00:06:25:53:0D:68
DSR-Airport1, 00:02:2D:0C:E4:84
<no ssid>, 00:40:96:29:75:F4
101, 00:01:03:7C:02:4B
bay6, 00:40:96:34:78:80
bay7, 00:40:96:34:E2:23
bay2, 00:40:96:34:B9:71
WLAN, 00:30:F1:27:01:BB
cpqcorpnet, 00:50:8B:D0:06:4C
<no ssid>, 00:02:2D:46:DE:85
8500A6GROUP, 00:02:2D:00:BC:84
<no ssid>, 00:40:96:31:92:73

kurz4768, 00:04:5A:F9:92:F2
<no ssid>, 00:02:2D:27:FB:5B
voyager, 00:40:96:34:4E:45
<no ssid>, 00:40:96:57:6C:39
spica, 00:40:96:37:D5:5B
Black Ink Airport, 00:60:1D:21:87:5E
voyager, 00:40:96:34:66:57
<no ssid>, 00:40:96:33:4C:DE
changes, 00:04:E2:0E:B9:3D
bay3, 00:40:96:34:87:40
bay9, 00:40:96:34:E4:87
bay17, 00:40:96:34:56:31
bay14, 00:40:96:34:34:0F
<no ssid>, 00:E0:63:82:CB:D4
<no ssid>, 00:20:E0:8B:DA:DB
Zimmlaw, 00:90:D1:00:FB:23
<no ssid>, 00:E0:63:50:2B:AA
WaveLAN Network, 00:02:2D:2F:11:7C
bay2, 00:40:96:31:A5:BF
default, 00:05:5D:ED:37:48
default, 00:04:05:DE:D5:3C
XcelerateWLAN, 00:01:24:F0:2F:88
OST-WAP, 00:06:25:53:19:CB
AI-mobile&wireless, 00:40:96:37:71:6A
bay11, 00:40:96:31:C4:E3
<no ssid>, 00:E0:63:50:AE:CE
bay1, 00:40:96:34:B8:85
<no ssid>, 00:02:2D:34:7D:25
Apple Network 3ca3eb, 00:02:2D:3C:A3:EB
<no ssid>, 00:40:96:31:B2:3F
<no ssid>, 00:20:E0:8B:0C:99
linksys, 00:04:5A:FD:B0:13
iml, 00:05:5D:EA:B8:36
LEON, 00:50:18:08:3C:62
J5_WIRELESS, 00:04:5A:FA:61:C5
Wireless, 00:30:AB:0B:9F:01
default, 00:50:18:05:83:D8
linksys, 00:04:5A:0E:7A:6A
tsunami, 00:40:96:40:D6:41
default, 00:90:4B:08:57:E6
<no ssid>, 00:40:96:33:B1:74
RedWire, 00:06:25:5B:21:1D
<no ssid>, 00:40:96:30:0B:D2
bay8, 00:40:96:34:13:76
bay19, 00:40:96:33:06:30
<no ssid>, 00:40:96:31:AE:34
<no ssid>, 00:40:96:45:AA:BF
PBNY, 00:50:DA:01:7C:11
tmobile, 00:40:96:31:10:F1
<no ssid>, 00:40:96:57:66:05
tsunami, 00:40:96:33:54:56
<no ssid>, 00:40:96:58:03:47
NYC, 00:50:8B:99:2B:7B
MobileStar, 00:40:96:31:10:26
<no ssid>, 00:E0:63:81:CD:79
101, 00:50:DA:94:78:5D
wireless, 00:30:AB:11:AB:0D
default, 00:50:18:09:BA:56
linksys, 00:04:5A:FF:D9:67
linksys, 00:04:5A:F6:31:92
<no ssid>, 00:40:96:32:C4:49
linksys, 00:04:5A:EE:0F:65
fumei, 00:04:5A:CF:F9:4B
Wireless, 00:30:AB:14:6B:BA
octavalent, 00:04:5A:D2:4F:E1
linksys, 00:04:5A:EE:94:A1
DavisCam, 00:D0:D8:60:02:40
tsunami, 00:40:96:29:26:85
<no ssid>, 00:40:96:48:F9:0E
handcraft, 00:06:25:53:1A:24
tahari, 00:40:96:5A:B0:DC
NY101, 00:30:65:00:5C:11
linksys, 00:04:5A:0E:F8:C9

linksys, 00:04:5A:F5:21:61
hpinvent, 00:04:5A:E4:FB:81
<no ssid>, 00:40:96:45:21:BC
target2, 00:40:96:25:9F:98
linksys, 00:06:25:50:4D:5F
SternOnTheMove, 00:06:25:5E:0A:95
linksys, 00:06:25:5F:F8:B9
linksys, 00:06:25:59:BD:1C
SGNET, 00:02:2D:1F:60:72
Fisher, 00:02:2D:1F:5F:70
KCA Network, 00:02:2D:31:B7:47
Airport Base B461 (Toy Front), 00:02:2D:1B:7C:D8
linksys, 00:04:5A:2E:3B:01
Zoom0334c9, 00:40:36:01:92:13
Zoom0334c9, 00:40:36:01:92:15
honeybear, 00:02:2D:05:FA:22
Andre-Bergmann, 00:30:65:04:15:B4
dunx, 00:50:18:06:5C:34
HONGlinksys, 00:04:5A:EE:84:B9
ATC!, 00:40:96:55:BD:DA
linksys, 00:06:25:51:72:09
painter, 00:06:25:61:28:C4
default, 00:05:5D:EC:98:3C
0a3857, 08:00:46:0A:38:57
101, 00:01:03:79:6C:84
Studio Base Station, 00:60:1D:F1:31:66
w_ap_34, 00:20:D8:02:5C:BF
airbubble, 00:60:1D:F0:2A:D3
mkda, 00:40:96:35:0B:FB
Apple Network 03edc7, 00:02:2D:03:ED:C7
Apple Network f1e092, 00:60:1D:F1:E0:92
default, 00:50:18:07:32:16
default, 00:05:5D:D9:C1:5A
tsunami, 00:40:96:29:94:44
default, 00:04:E2:1A:EA:D4
tsunami, 00:40:96:28:A0:08
LiquidSite, 00:40:05:DE:30:4A
juan_alday, 00:04:5A:F1:51:FE
mkda, 00:40:96:32:F1:B1
Wayne, 00:01:24:F0:3D:4C
linksys, 00:06:25:5A:E1:D1
<no ssid>, 00:40:96:33:20:C8
Wireless, 00:01:24:F0:C9:8D
mkda, 00:40:96:33:C4:5A
mkda, 00:40:96:34:14:76
1206COSENTINI, 00:40:96:59:B4:27
linksys, 00:04:5A:0E:89:01
galeb, 00:04:5A:DD:7F:83
mkda, 00:40:96:34:2D:3C
mkda, 00:40:96:34:6A:95
mkda, 00:40:96:33:07:DA
WAP1, 00:04:5A:0F:20:45
350 WEST 50TH (EAST SIDE), 00:02:2D:0C:CF:39
mkda, 00:40:96:35:0E:EF
<no ssid>, 00:40:96:38:E2:0A
mkda, 00:40:96:38:BD:2C
vcwlan, 00:40:96:54:64:CA
linksys, 00:04:5A:DD:38:CB
joltage, 00:02:2D:2A:3F:04
<no ssid>, 00:40:96:33:07:62
mkda, 00:40:96:33:FC:0A
<no ssid>, 00:40:96:29:47:F2
linksys, 00:04:5A:FD:D2:AB
vcwlan, 00:40:96:47:72:57
msi, 00:06:25:60:2C:1B
Heimdall, 00:02:2D:1F:55:5A
linksys, 00:06:25:59:66:22
default, 00:01:24:F0:3C:7E
l758wn, 00:04:5A:0E:8B:FD
linksys, 00:06:25:5D:A9:53
350 WEST 50TH (EAST SIDE), 00:02:2D:01:17:2D
MSFTWLAN, 00:40:96:40:C7:92
linksys, 00:04:5A:DB:BA:31
linksys, 00:04:5A:FD:C0:E7
dopinmo, 00:04:5A:0E:46:08
linksys, 00:06:25:59:88:96
linksys, 00:04:5A:F5:2F:55
linksys, 00:04:5A:0F:26:92
WLAN, 00:90:D1:00:D1:9C
WLAN, 00:90:D1:00:E8:E5
<no ssid>, 00:02:2D:2A:ED:9F
ANY, 00:30:65:18:0D:A5
VNWLAN, 00:04:E2:1B:82:31
linksys, 00:04:5A:FA:77:01
linksysny, 00:06:25:54:0A:7D
<no ssid>, 00:40:96:57:D8:4A
linksys, 00:04:5A:CF:90:D9
default, 00:90:4B:0B:0E:14
<no ssid>, 00:40:96:57:DB:1E
skywire, 00:01:F4:ED:6C:47
ipblue, 00:40:96:32:B1:7E

linksys, 00:04:5A:0F:1F:06
dsl, 00:04:5A:EE:85:69
xxxxxx AirPort Network xxxxxx, 00:40:05:DF:33:3C
dlink, 00:40:05:DE:E4:6A
default, 00:01:24:F1:50:0F
linksys, 00:06:25:5D:D4:C9
tsunami, 00:40:96:5B:0B:50
GLNYC, 00:40:96:40:93:37
whytiger, 00:01:24:F0:54:FE
linksys, 00:06:25:59:B0:DC
tsunami, 00:40:96:29:44:3D
linksys, 00:06:25:5A:E1:63
link37sys, 00:06:25:59:7D:3A
<no ssid>, 00:40:96:57:DA:C5
tsunami, 00:40:96:45:CF:87
Wireless, 00:30:AB:07:B6:EF
scm461, 00:06:25:51:7B:F8
tsunami, 00:40:96:58:29:D6
linksys, 00:11:22:33:44:55
tsunami, 00:40:96:5B:0C:26
116, 00:04:5A:D1:AB:37
cfe001, 00:40:96:58:14:19
p32002ny, 00:04:5A:F1:48:48
dragonballz, 00:40:96:41:90:0C
linksys, 00:04:5A:D2:50:7D
3ca724, 00:02:2D:3C:A7:24
AirPort Network f08516, 00:60:1D:F0:85:16
tmobile, 00:40:96:31:BE:1D
Apple Network 1cb1e1, 00:30:65:1C:B1:E1
home, 00:30:65:03:F0:4D
Apartment Airport, 00:60:1D:22:B5:B6
SternOntheMove, 00:09:43:74:53:B2
DC, 00:60:1D:1E:EA:7C
Boycott The W, Lemon, Chango, 00:02:2D:21:03:32
ZeL9gIv3xA8, 00:40:96:45:73:25
Cahners, 00:40:96:40:88:BC
linksys, 00:06:25:5B:17:63
linksys, 00:06:25:59:8B:5A
ghio, 00:04:5A:26:FA:BB
linksys, 00:04:5A:EE:2A:F3
daPlace, 00:50:18:05:B6:FC
default, 00:40:05:DE:2C:9B
tsunami, 00:40:96:32:DF:99
tsunami, 00:40:96:5B:20:77
Apple Network 041ffc, 00:30:65:04:1F:FC
2eee6d, 00:02:2D:2E:EE:6D
cfe001, 00:40:96:57:9E:2D
Cantaloupe Dogs, 00:02:2D:1F:6A:96
naprw, 00:A0:F8:39:44:D9
SpeedStream, 00:01:24:F0:B6:C4
<no ssid>, 00:40:96:57:DD:AD
linksys, 00:04:5A:D2:1B:75
default, 00:01:24:F1:A2:FA
default, 00:01:24:F1:4F:64
<no ssid>, 00:40:96:58:30:24
101, 00:50:DA:01:A6:3C
UNTETHERED1, 00:50:DA:00:5B:44
Wayport_Access, 00:40:96:25:A4:98
micky, 00:04:5A:ED:DD:89
101, 00:01:03:7B:FD:26
ssmb, 00:06:25:01:42:1A
tmobile, 00:40:96:32:C3:83
Apple Network 02562b, 00:30:65:02:56:2B
MSD Wireles Network, 00:02:2D:0F:C9:F6
linksys, 00:06:25:04:70:09
SuiteLLC2, 00:02:2D:1D:EA:BD
linksys, 00:04:5A:FF:D6:83
vcwlan, 00:40:96:55:C6:AD
default, 00:40:05:DF:82:D0
linksys, 00:04:5A:FA:4E:7D
101, 00:02:B3:04:E6:58
jimmyvanm, 00:02:2D:04:92:21
TVI Wireless, 00:02:2D:2A:C3:FA
Wireless, 00:04:5A:0F:36:48
Big Foot Digital, 00:02:2D:2B:82:C8
Apple Network 1e1b51, 00:30:65:1E:1B:51
ward, 00:06:25:5B:08:FF
101, 00:02:B3:05:6E:79
<no ssid>, 00:02:2D:2F:84:64
<no ssid>, 00:60:1D:F1:6F:10
Lacombe AirPort, 00:30:65:1E:B1:F5
Apple Network 03372d, 00:30:65:03:37:2D
350 WEST 50TH (EAST SIDE), 00:02:2D:0C:B5:7E
101, 00:02:B3:05:3D:7C
TuPuppi Network, 00:02:2D:1D:E5:C7
350 WEST 50TH (EAST SIDE), 00:02:2D:01:31:2D
nycwireless.net, 00:30:AB:0A:85:00
<no ssid>, 00:40:96:5B:61:24
Office, 00:30:65:1C:6E:4D
voyager, 00:40:96:34:34:2D
<no ssid>, 00:40:96:33:8C:8F

tmobile, 00:40:96:32:C2:6D
Sterling New York, 00:30:65:15:78:71
Ira's Network, 00:02:2D:07:92:76
vcwlan, 00:40:96:41:E5:FD
linksys, 00:06:25:5D:A3:8D
NY101, 00:06:25:51:44:8E
AWireless1, 00:04:5A:D1:F0:05
jec, 00:04:5A:2F:E8:B9
101, 00:50:DA:90:90:59
cpadwap, 00:01:24:F0:20:E9
linksys, 00:04:5A:0F:33:2A
Cahners, 00:40:96:5A:A5:7F
<no ssid>, 00:07:50:CA:50:40
Cahners, 00:40:96:59:A4:BD
linksys, 00:06:25:59:78:C4
linksys, 00:06:25:50:3A:42
schmelkin, 00:05:5D:EA:EA:36
bay8, 00:40:96:31:44:BD
linksys, 00:06:25:59:A0:40
linksys, 00:04:5A:FD:AE:23
linksys, 00:04:5A:0C:5C:FC
Moss/Mack, 00:06:25:5D:8F:1F
tsunami, 00:40:96:29:49:3A
711, 00:02:B3:86:C8:74
linksys, 00:04:5A:EF:33:7B
<no ssid>, 00:40:96:31:A7:52
cvsretail, 00:A0:F8:3A:28:93
WLAN, 00:01:24:F0:72:6D
<no ssid>, 00:06:25:A6:08:D7
dorsay, 00:30:65:1E:10:11
Apple Network 0b9e1f, 00:02:2D:0B:9E:1F
0d7131, 00:02:2D:0D:71:31
ANY, 00:60:1D:1E:95:FB
Apple Network 1f3f06, 00:30:65:1F:3F:06
76mad, 00:02:2D:2F:9D:E9
bay7, 00:40:96:31:45:45
bay2, 00:40:96:34:EA:1B
branto-linksys, 00:06:25:59:79:D6
mphasisny, 00:04:5A:DD:73:9D
braonkompanije, 00:50:18:05:3B:E8
WaveLAN Network, 00:02:2D:0C:D0:44
Cahners, 00:40:96:59:A6:4E
chd, 00:06:25:51:A8:66
voyager, 00:40:96:52:05:A6
Wireless, 00:30:AB:13:B1:28
riddlenet, 00:06:25:53:0A:BB
<no ssid>, 00:40:96:57:74:0A
linksys, 00:04:5A:2E:0F:75
linksys, 00:04:5A:0E:35:65
NTC-NYC-1, 00:06:25:50:B4:AD
AirPortNetwork, 00:02:2D:31:51:7C
Apple Network 1e5c12, 00:30:65:1E:5C:12
Apple Network 0791b9, 00:02:2D:07:91:B9
bay8, 00:40:96:34:99:FB
NexLand, 00:A0:65:B5:3A:04
linksys, 00:04:5A:2E:4F:D3
2df9cb, 00:02:2D:2D:F9:CB
WLAN, 00:01:24:F0:71:8B
Silverstein, 00:60:1D:23:1A:69
0b5034, 00:02:2D:0B:50:34
Apple Network 0b7d63, 00:02:2D:0B:7D:63
NY Airport, 00:02:2D:0F:6F:17
linksys, 00:04:5A:26:D5:9D
vokesnet, 00:06:25:5D:4A:21
6floor, 00:04:5A:DA:87:23
linksys, 00:06:25:50:2B:88
training, 00:04:5A:2E:21:6D
<no ssid>, 00:02:2D:37:04:32
interfaith wireless, 00:04:5A:0C:06:28
<no ssid>, 00:06:25:A8:3F:7E
fsviclnk, 00:04:5A:F9:C9:32
REDIVI, 00:04:5A:2E:04:3D
01WLAN, 00:90:4B:08:58:C5
linksys, 00:04:5A:0F:27:E8
homenet, 00:04:5A:0C:09:2A
Airport RoadRunner, 00:02:2D:1D:E6:03
Apple Network 025373, 00:30:65:02:53:73
LeRoy, 00:30:65:1E:0C:C3
Apple Network 29c76e, 00:02:2D:29:C7:6E
<no ssid>, 00:05:5D:EE:B3:31
tmobile, 00:40:96:31:B8:72
f076edAirPort Network f076ed, 00:60:1D:F0:76:ED
Airport network, 00:02:2D:2C:0C:F3
tsunami, 00:40:96:40:DB:D6
default, 00:05:5D:EE:FF:A6
linksys, 00:04:5A:0E:14:48
Airport Base C811 (Fashion), 00:02:2D:1F:6B:61
Tcholakian, 00:30:65:1B:B1:5C
Home, 00:50:18:07:74:9A

How to Break Through a Proxy or FIREWALL

by unformed

There are different reasons for breaking through firewalls/proxies. 1) Get completely unfiltered access to the Internet; 2) Get unmonitored, or secure, access to the Internet; 3) Access services normally disallowed by the firewall.

This article will demonstrate various ways to get by most implementations of firewalls/proxies. In absolutely no way am I responsible if you do anything you're not supposed to (or even supposed to) be doing. If you get caught and fired, tough shit. If you access illegal information, tough shit. If you open up a hole and somebody breaks into your computer, tough shit. I'm not responsible. (This is for the lawsuit-happy bastards out there.)

Anyways, lets begin.

For all methods, it is expected that you have access to a machine on the other side of the firewall and that it has access to whatever you need. Your machine will be the client and the machine on the other side of the firewall will be the tunnel. The accessed machine will be the server.

Furthermore, this article also assumes you have a basic knowledge of your browser's configuration, installing software on your client and tunnel machines, and logging in via ssh.

A Linux/Unix box is preferable for the tunnel, but not required by any means. The software is freely available for any system.

HTTP Tunneling Through SSH

Often only some ports will be firewalled (80, 21, etc.) for caching, filtering, and monitoring purposes. However, they leave direct access available for other ports (25, 23, etc.).

If your browser must use a proxy to access the web, but you don't require a proxy to get mail, this is probably the implementation.

If you have direct access to non-popular ports, you can access almost any service as long as you change the port. Generally, the main purpose of bypassing this firewall is to have unfiltered and/or unmonitored web access. The method can of course be modified to meet your needs.

Install a proxy server (i.e., tinyproxy) on the tunnel machine. For security purposes, set the listening port to an odd port (i.e., 8999, REMOTE_PROXY_PORT) or set access rights to only localhost. Install an ssh (i.e., sshd) server on the tunnel. For security purposes, set the listening port to an odd port. Do *not* set access rights to only localhost because you'll access the proxy through ssh.
Install an ssh client on the client machine. Select a random port (LOCAL_PORT) and then set the browser's proxy to localhost: LOCAL_PORT.
Run ssh with LOCAL_PORT forwarded to REMOTE_HOST: REMOTE_PROXY_PORT. (CLI ssh: ssh -L LOCAL_PORT:REMOTE_HOST:REMOTE_PROXY_HOST -l USERNAME REMOTE_HOST)

Once connected and logged in, if the proxy and the tunnel are working correctly, you've got completely unfiltered web access.

(Using a SOCKS5 compliant proxy would offer an almost completely unfiltered and unmonitored connection, as long as the application supported SOCKS proxies.)

SSH Tunneling Through HTTP

Some implementations allow only HTTP access while blocking all other ports. Check out Corkscrew at http://www.agroman.net/cork-screw/

Corkscrew is a tool to allow full SSH access through a strict HTTPS session. Then through the ssh access, you can create another tunnel to allow access to all other programs.

Conclusion

Hopefully this allows some of the people out there to worry a little less about getting caught doing things they're not supposed to. The reason for using ssh in both cases is because it's encrypted. In the event you are caught, at least you're only caught for breaking the rules. There's nothing additionally incriminating.

SSH can also be used for a lot more interesting things. Using Windows, you can instal Cygwin, ssh into a *Nix box and tunnel over X connections, and end up working as if you were actually at the machine.

Anyways, that's my story, and I'm sticking to it.

A Nasty NT Bug

by HJH

First off, I owe a major thanks to Zappadoodle.com. Most of what follows is just an easier to parse summary of what they've already discovered.

Despite being quite bullish on Linux, I've still considered the Windows NT line to be a worthy competitor, especially Windows 2000. From what I'd read, and the little experience I'd had, it seemed like a solid, dependable, if somewhat bloated OS.

Then I read Zappadoodle.com.

That site described an odd little bug that allowed anybody to bring that OS to its knees. The entire demo consists of a measly three lines of C code:

```
void main() {
  for (;;)
        printf("Hungup\t\b\b\b\b\b\b\b");
}
```

That loop prints a string to the console, which means it passes through some code in CSRSS.EXE. The output routine that happens to parse it has a nasty flaw; it doesn't properly handle several backspace characters after a tab. Specifically, it backs up one character too many, and doesn't make sure the cursor position is still within the console buffer. By repeatedly doing this, the cursor position will eventually move outside the memory area set aside for CSRSS.EXE. By also writing normal characters, CSRSS.EXE

will attempt to write there.

It won't succeed. The processor will refuse CSRSS.EXE's attempts because it doesn't have access to that bit of memory. NT will follow up by killing off CSRSS.EXE. So far, this is nothing more than poor bounds checking and standard OS procedure.

Now things get interesting. See, CSRSS.EXE is apparently a vital part of the NT operating system. If the kernel notices CSRSS.EXE isn't around, a kernel panic ensues and everything halts; no buffers are flushed, no more network requests are handled, and so on. Don't ask me why Microsoft considers console access so critical.

Depending on the version of NT, the machine may immediately reset or hang on a blue screen. That's right, this bug affects more than one version of NT. It's known to be in Windows XP, 2000, and NT 4. It may be in NT 3.5 and 3.1 as well. Basically, if you run NT, you have this bug.

I know what you're thinking; bounds checking isn't that hard to fix, and we already know where to find the relevant code, so Microsoft probably has a patch out already. Guess what? The bug has been public knowledge since late October of 2001 and as of now, no patch is available. Microsoft hasn't even admitted this bug exists.

Even worse, Microsoft is due to stop supporting NT 4 in a year or two and has already abandoned NT 3.5 and 3.1. It's unlikely those three will ever see a patch.

OK, if Microsoft isn't going to be any help, an administrator will have to fill in. Force anyone other than trusted admins into a guest account. Prevent them from uploading and executing their own programs. From now on, only a small set of programs are permitted. That should take care of it, right?

Nope.

Despite its importance to NT, CSRSS.EXE handles all console output by any user. Administrative privileges are irrelevant.

And I said *all* console output. This means Visual Basic programs can still down NT. As can a Perl script. Or Python, TCL, QBASIC, and even a few Java programs. The only exceptions are programs that do more than just spit data at the console. For instance, EDIT is safe, but TYPE isn't.

In case you missed that, let me make it clear: you can crash NT merely by printing out a text file to a console. It sounds impossible, but I've confirmed it on a WinXP box with a 16MB text file.

While I could use this nasty bug to bash Microsoft and sell Linux, I'm more concerned about all those vulnerable NT machines. Maybe if we spread this info around enough, we can get Microsoft to pay attention and release a fix. It sure beats waiting for a worm to exploit it, anyway.
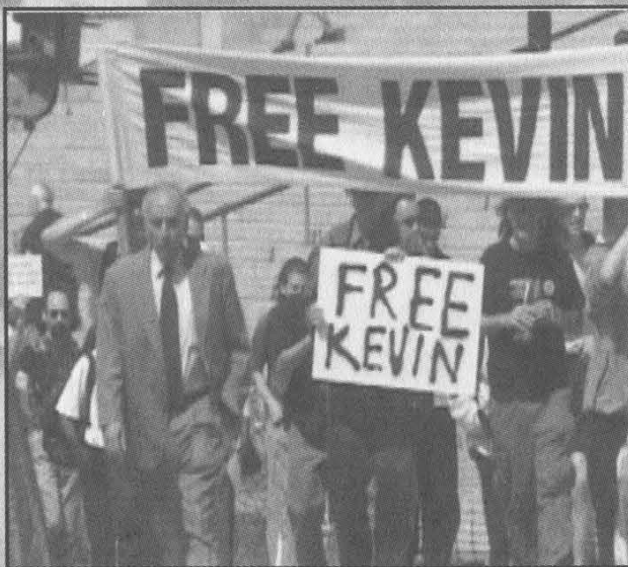
by dufu

As I read *2600,* I realize just how old I am - or maybe just how young all the new experts and pseudo-experts are. After all, my first computers were a TRS-80 Model I and a Commodore 64. Boy... programming was never so easy as back then.

Every time I get a hold of the newest *2600,* I swear that I'm going to write in and comment on how everyone seems to have gotten so much smarter than me. After all, browsing MCIMail with someone else's account was a big thing back when I was a kid. Getting other's credit card numbers has actually become easier although back then, you could find a list of a hundred or more on any given BBS. 64k? Wow. That would have taken a few months of programming - even in basic - to fill up. Who would ever need more than that?!? Real time chatting? Some folks did it. But it was more like IRC - and I could read at 300 baud so it was easier. Networking? Hmm. Isn't that what they used mainframes for? After all, the 286's weren't even out yet. Color monitors came only in amber or green for the most part unless you had a lot of money.

I remember picking up two 12 meg hard drives at a local computer flea market for free. The largest hard drives on the market at the time were five megs and I thought we had hit the jackpot. Until I found out I couldn't get them to work on my C64.... Boy. Tossing those 40 pound monsters into the trash must have made the garbage men happy....

Then came my first IBM - a real IBM. Weight was twice as much as any clone. So was the electric bill for using it if I remember correctly. Man. It had multiple megabytes of drive space, semi-color output - although not as good as the sprite driven C64! It could go to the same BBS systems I used to visit and fit more on the screen! Wow. Too bad I couldn't read at 1200 baud. Hacking SuperWilbr - some school's remote word processing system or something. Any old-timers actually know what it was?

Someone came out with 2400 baud. Next computer flea market netted me a few 4800/9600 modems. Too bad they were nowhere near compatible with anything I used or owned. Their big blue boxes looked just like the magnetic bone healers the guy was selling in the booth next to mine. Oh, did I mention I started getting a seller's booth at the shows to make dropping off my find easier? Yeah, I started selling junk from the last year's shows too. Helped finance my life.

Doom, Doom II, Quake, and Heretic were all played on a 386 with no sound card. And beat. I either got lucky a lot, saved a lot, or used the cheat codes a lot. Regardless, I won.

Then came phone phreaking. I never really took part, but I played enough to build my own advanced Rock Box (see 19:1, page 19) without the aid of others. Loved to blast the random telemarketer who called. Seems they call much more now. I remember that 1-800-424-9096 and 9098 were the White House Press Line and the Department of Defense hotline. One still works. You play to figure out which. I memorized the touch tones so that I could tell you what number or numbers you dialed. That always freaked people out.

I'm drifting from the real purpose of this article. Let me jump back to the present time. I now work for a large accounting firm that has recently been taken down by the DOJ because of the actions of a few dozen people. Their leader has plead guilty to the charges pressed against the firm that fired him for the exact transgressions that got both of them into trouble. We've lost more people and more money than Enron even though they get most of the press. I work with technology all day, every day. Lucent digital phone systems that can be crashed by playing too much. Networks that are full of great information - all of which is now useless. Drones - aka employees running around with either W95 or W2K but nothing in-between. I even remember my first week when I performed a basic defrag on a PC and almost got fired for "hacking" because they "caught" me doing it. They have since become some of my best friends and beloved coworkers. They come to me for technical advice and guidance in many cases. I push the limits of our in-house technical support folks' knowledge base regularly enough that they have given me the direct number to their dedicated MicroScoff advanced support center - along with the access code. It's even more fun to stump those guys....

I could go on and on about how Lotus Notes and eFax don't mix, W2K and our network keep me from accessing sites, etc. However, it was simply therapeutic to write this. What is the bottom line, you ask? In a few years, you'll be just like me - wondering where all the newbies learned their tricks and how they can possibly have enough free time to use them all.

Keep hacking. Keep it moral. Teach others. Become a leader of the ignorant, not their enemy.

grab that Cache

by David Nicol

After reading all about "right-click protection" and how it is supposed to work, I thought I'd share the method I use to locate an image I have seen recently on a web page when I want to share it with someone.

Since all images are kept in Netscape's cache, it is possible to create HTML pages that refer to the images in the cache, and then work with the images you want. I do this with a small perl program something like:

```
#!/usr/local/bin/perl

open FILELIST, "find ~/.netscape/cache -type f
|";
mkdir "pages$$",0777
 or die "could not make directory to put the
HTML pages in";
$Page = 'aa';
while (<FILELIST>){
```

```
        chomp;
        print " adding $_ to
page$$/$Page.html\n";
        open PAGE,
">>pages$$/$Page.html" or die $!;
        print PAGE "<img src=file:$_
height=40 width=40>\n";
        $. % 10 or print PAGE "<br>\n\n";
        $. % 100 or $Page++;
};

__END__
```

This gives you a bunch of HTML pages each with a hundred files from Netscape's cache on it as images. When you find the image you want, clean up with something like:

```
rm -rf pages17*
```

Below is a window-grab of the result of running the above program on my Netscape cache.
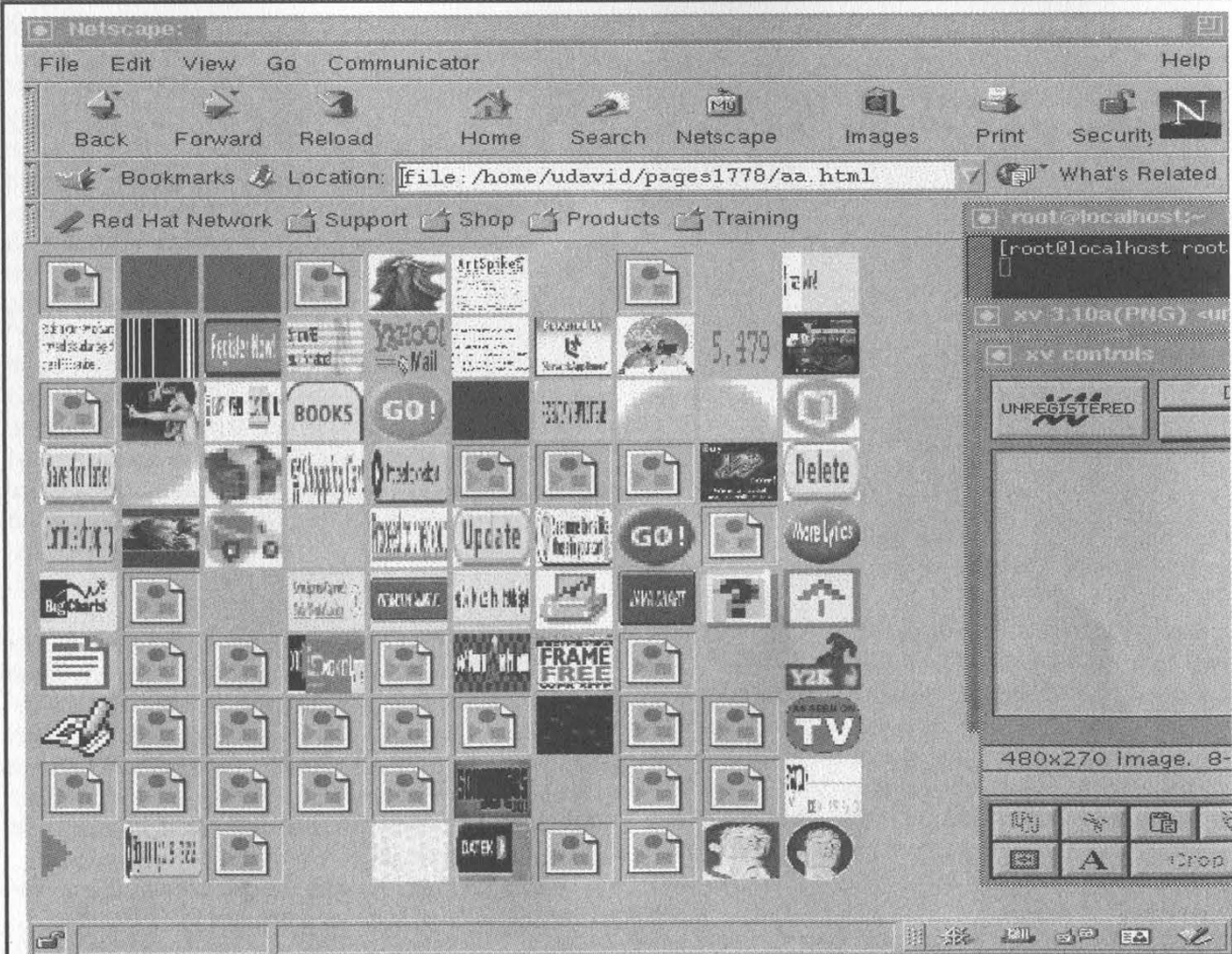
THE END OF AN ERA

by Lucky225
lucky225@2600.com

In the beginning, Ma Bell created the operator center and the payphone. The first payphones were the old three-slot ones. When you placed a long distance call from these phones, an operator would ask for whatever the rate was for the call and when you deposited the coins you would hear bells or gongs, one bell for a nickel, two for a dime, and a gong for a quarter. This was an ineffective way of verifying how many coins were being deposited and one could easily deposit coins on a payphone next to them or ring a little bell - the earliest form of redboxing. When Ma Bell introduced the one-slot payphone it used a single frequency for identifying coins that were deposited: 2200hz. One 66ms beep was a nickel, two 66ms beeps (66ms off) was a dime, and five 33ms beeps (33ms off) was a quarter. This was a good idea, but because it only used a single frequency, a system like ACTS could not be widespread as talk-off problems would register human voice and sound as valid coin deposits. In the late 1970s Automated Coin Toll Service (ACTS) was introduced requiring new payphones that used DTMF coin deposit signaling, with the famous DTMF (Dual Tone Multi Frequency) 2200+1700hz deposit tone (same timing as the single frequency 2200hz). ACTS was supposed to be the latest and greatest thing back then requiring less operators for payphone customers and automating payphone long distance calls. But it was a major step backwards for AT&T. By the early 80's phone phreaks with blue boxes that no longer worked found another way to call long distance by fooling the phone company with tones.

It's amazing that a service so susceptible to fraud has survived this long, but it is now coming to an end. On May 21, 2001 AT&T filed an application (NSD File No. W-P-D-497) with the FCC to discontinue interstate sent-paid coin service (ACTS). On October 15, 2001 by public notice (DA-01-2375) the FCC granted AT&T's request. The application reports that its earnings from the service are small and rapidly declining, and that only a small amount of calls are placed from phones where the service is provided. Furthermore, they say that it costs millions of dollars to provide the service each year, an amount far greater than the revenues generated. Also, the rates are ridiculous compared to what one would pay if he or she was using a calling card or other
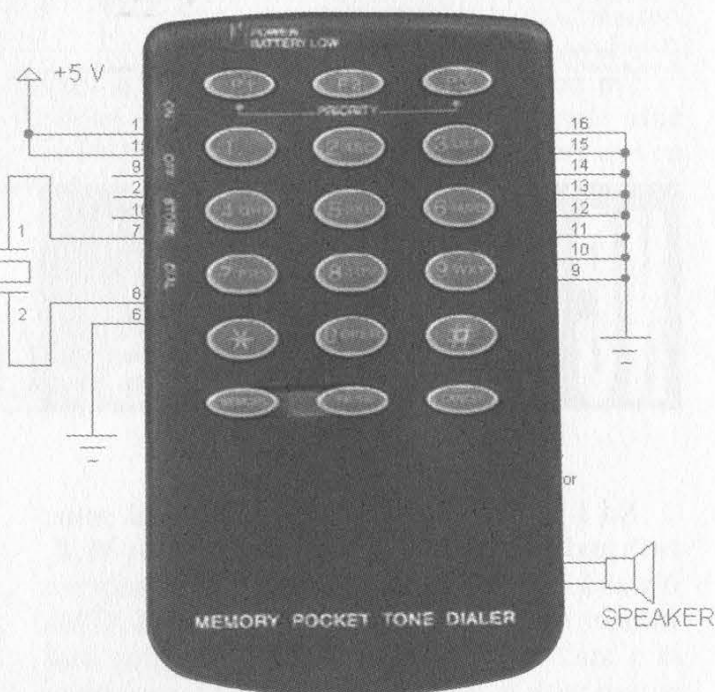
form of payment - a minimum of $4.65 of interstate long distance calls (a $1.95 coin surcharge fee plus $2.70 for each 3 minutes). The $1.95 is a one-time fee. However, the $2.70 is the minimum you will be paying for each additional three minutes. That's 90 cents a minute, rates that were possibly driven up by red box fraud.

When you place a long distance call from ACTS payphones, you will now get the following recording: "Your call will now be completed. Please note, effective soon, this phone will no longer accept coins for AT&T long distance calls. You may wish to begin using a prepaid calling card or other payment methods as a substitute." You can hear this recording at http://amatus.austin2600.org/~lucky225/redboxatt.wav.

Once AT&T discontinues the service, that will be the end of redboxing. AT&T is the only carrier that offers sent-paid coin service. If you try to use any 101XXXX carrier, for example MCI's 10-10-222+1+NUMBER, you will still be routed to AT&T's automated system. I contacted Carmell Weathers of the FCC's Common Carrier Bureau about this to try to find out if any other carriers had offered to continue providing sent-paid coin service, and here's what he had to say:

I'm not sure what he meant by this as they have already granted AT&T's request by public notice. Perhaps it's still in transition and AT&T is going to be forced to continue providing the service. Doubtful though. Red boxing will soon become history though. Even with AT&T's discontinuation the local phone company does provide ACTS for intraLATA calls, but I'm sure the payphones will start being replaced with Nortel Millenniums and COCOTs in the near future. So keep your eye out and if you haven't done any experimenting with ACTS payphones, now's probably your last chance. Note however that Canada still uses single frequency 2200hz payphones, but those are slowly being phased out too.

NCR ATMs - Aurum Ex Machina

by Acidus
Acidus@resnet.gatech.edu

So I was out at a mall and I needed some cash and I walked up to an ATM at Lenox Mall. It was a PNC Bank ATM, and I couldn't help but wonder why a bank from Pittsburgh had ATMs in a mall in Georgia. Anyway, something was wrong with it, and it appeared that a repairman must have been working on it because the screen showed some kind of configuration program. It looked a lot like the BIOS config screen on any PC.

The screen had something like eight options, things like change system time, change system data, change drive settings, print config, and reboot. These options were printed along the sides of the screen next to the buttons. I pushed the button next to "print config" (or something like that), and instead of taking me to a screen to configure the thermal printer, the ATM hummed for a second, and out of the receipt printer came a printout of the current configuration of the machine. Here is the printout word for word:

```
       PNC BANK

***** 01/01/07 12:19:19 *****

SETUP

DATE (YY/MM/DD)   07/01/01
TIME (HH:MM:SS)   12:19:20
FLEX DRIVE A      1.44MB
FLEX DRIVE B      NONE
DRIVE 1 TYPE      127
DRIVE 2 TYPE      NONE
TOTAL MEMORY (KB) 16000
COPROCESSOR       YES
```

Other than the "Flex" thing, this looked just like the specs of a simple computer. I didn't want to change the date or anything, and I couldn't do much at this screen. I knew I didn't have much time, and the "reboot" option looked really good. So I hit it and the machine went blank. And nothing happened. Then it whirled to life, and in the top left counter I saw numbers: 4096, 8192, all the way up to 16000. Hello *post!* Then what should my wondrous eyes see but "Phoenix BIOS Ver 4.something or other." The machine then did some kind of check on its Flex drives and then a big IBM logo came up. In the bottom on the screen it said "IBM OS/2 Version 3. Government" There was something after "Government," but the screen was smeared with something so god awful, I sure as hell wasn't going to touch it. The screen cleared and then the words "Load 40" came up, at which point the screen went to 40 columns. At this point I started attracting serious attention and decided I should go. As I left I saw the machine default into the setup program again.

I had always thought ATMs had specialized hardware and crazy stuff like that, not a PC running OS/2 of all things. The more I researched the weirder it was. ATMs are quite a complex blend of software and hardware, and a comprehensive study of them is beyond the scope of this article. However, information on ATMs and their specifics is (for obvious reasons) very hard to come by. This should clear some of the mystery up.

Hardware

The standard computer equipment available on an NCR ATM is: a Pentium processor (speeds from 100 to 166), RAM (16MB to 32MB), a 1.2 gig IDE hard drive, one 1.44MB flex drive (it's just a floppy), a 10 inch VGA

color or monochrome monitor (notice VGA, not SVGA, so it's only doing 320x200x256), and RS-232 port. Optional parts include a sound card (to play digitized speech), an IDE CDROM to store the speech (speeds range from 6x to 24x), a second Flex drive, and other banking specific hardware (a better thermal printer for receipts, currency cassettes, etc.).

I found the RS-232 interface a great thing to hack. It is there to allow remote video card systems to be controlled by the ATM. However, this is a rarely used option. RS-232 is extremely well documented but sadly slow. On the other hand, ATMs have really weird connectivity. The NCR ATMs I researched (Personas and 5xxx series) didn't support TCP/IP. They had weird protocols like NCR/ISO Async, IBM 3275 Bisync, and a lot of other very obscure stuff. RS-232 is the only guaranteed way to move lots of data on and off the system.

There is a lot of banking specific hardware in these things. I don't want to fill this article with specs of currency cassettes or mag card canisters. If you are interested, check my references. The only thing of interest is a DES Hardware encryption system.

Software

The operating system running on the ATMs is OS/2 Version 3. (I have since seen versions of OS/2 Warp for sale for ATMs as well.) I know next to nothing about OS/2, so study on your own if you want. I do know however that OS/2 is used for its multitasking abilities.

The main NCR programming running is something called the Self Service System Software (S4). This keeps a log on the hard drive of "all significant customer and supervisor activity." It also manages all the applications such as the communications software and the graphical display. S4 has an API programmers can use called ADI. ADI handles things like memory allocation and access to the file system. However, programmers can call OS/2's API directly. These machines use FAT as their file system and, since it's IBM, it is most likely still FAT16. Other software running on these ATMs is NCR Direct Connect, which seems to be the interface to the communications. (It handles the protocols, and can convert between them or emulate other ATMs.)

The software running on the ATMs could be pretty old. I mean, the diagnostics asked it I had a coprocessor to enable. Math coprocessors have been standard inside processors since 386DXs and 486DXs. Also, NCR offers a book for Pascal programmers to develop applications for the ATM.

ATM software is developed on standard PCs, and since they use Intel x86 Pentium class processors with a standard DOS based operating system, anything that doesn't use Windows API calls should work. In fact, a lot of Windows 3.x programs work in OS/2. A good rule of thumb: if it works in DOS, it will work in OS/2.

Communication

Communication in the ATM is conducted through leased lines, though some ATMs in less high traffic areas may still use dial-up. By Federal law all information traveling on these lines must be encrypted. The NCR ATMs uses DES.

Alarms

Alarms on the ATM mainly protect against a physical attack. These are the mechanical and thermal alarms, and they make sure you don't take a crowbar or a blowtorch to the money door. However, NCR does have an enhanced alarm system which protects the Flex disk drive door. This enhanced version also has seismic sensors. However, unplugging the ATM or rebooting it a lot shouldn't mess anything up.

Conclusions

There is a lot more info about ATMs and you can check my references. I have no desire to try and steal money from them so I never really looked at the data lines or ways to intercept key presses inside the machine. However, my research shows that the computer part of the ATM, since it uses standard PC parts, is vulnerable. I rebooted it for god's sake. I wish I knew the OS/2 equivalent of [F5] which would have let me interrupt the boot and get to a command prompt. The machines most hackable are in malls and other public places. These have much less armor plating and other countermeasures and instead rely on their exposure to protect them. If you look like you know what you are doing, no one will question you.. Who would like to put anti-virus software on an ATM? With a little research about OS/2 and how it loads, you could easily drop out of the boot-up and get to a command prompt. Using the floppy and the RS-232 port (or better yet a CDROM if it's there), you could install your own software. How cool would it be to have an ATM running Doom?

References

NCR PersonaS 88 ATM System Description - Got the bulk of my info from this. Found it after a ton of searching on a cached Google page of NCR's Russian web site. I don't think they wanted this out in the public, but I got it and moved it to my site: http://www.prism.gatech.edu/~gte344p/NCR-ATM.pdf

The Bankers Exchange - They sell ATM parts and accessories. Used them to check on parts: http://www.bankersx.com/home.html

The idiots at Lenox - for leaving the ATM in diagnostic mode.

The *Afghan* Phone System

by Iconoclast
phosgene@setec.org

If you are a curious phreak like me, the telecommunications infrastructure of Afghanistan immediately comes to mind as something that deserves exploration and understanding. Alas, the lack of said infrastructure leads me to say that it is quite possibly the worst place to try to make a phone call from on the entire planet.

We take our precious lovely dialtone for granted, but there you will be hard-pressed to even find a working telephone. To begin with, let's take a look at the numbering formats for the country. Country codes are assigned by the International Telecommunications Union (ITU) (www.itu.int). The International Country Code (ICC) for Afghanistan is 93. The "9" signifies it is in geographical region 9 of the world. The United States has an ICC of 1.

From within Afghanistan, to place an international call you would dial the International Direct Dial (IDD) code which is 00. To place a call within the country you would prefix it with the National Direct Dial (NDD) code which is simply 0. There are no city codes or area codes in the country on the old electromechanical exchanges. Numbers within the various cities are five digits long. An excellent directory of people to call in Afghanistan was listed by the Afghan Wireless Communications Company (AWCC) but was recently removed. Hopefully, they will restore this information (www.afghanwireless.com/search.cfm).

Telephone usage is actually dropping, since in 1996 there were 29,000 lines available and in 1998 there were only 21,000 lines. Of course, Taliban bans on Internet use didn't exactly spur telecom growth. My sources in the CIA have stated that "in 1997, telecommunications links were established between Mazar-e Sharif, Herat, Kandahar, Jalalabad, and Kabul through satellite and microwave systems" (www.cia.gov/cia/publications/factbook/index.html).

Two telecommunications companies from China, Zhongxing Telecom and Huawei Technologies, were attempting to install a switching network in the capital city of Kabul which could handle 130,000 lines. The status of this project is unknown at the current time.

Most of the existing exchanges are based on electromechanical switches that are 40 years old. These old exchanges are using Siemens Strowger switches. Completing calls on these exchanges is very difficult. New equipment using digital switches is being installed. In order to place calls to the older switches, one must have the operator service in Kabul complete the call for you. You can reach the operator service by dialing +93-2-290090. Then give them a five digit phone number and the call may have a slight chance of being completed.

Parts of the country have digital exchanges which can be dialed directly without the operator. The various city codes are: 02 Kabul, 03 Kandahar, 04 Herat, 05 Mazar-i-Sherif, 06 Kunduz, 07 Jalalabad, and 08 AWCC Mobile Telephone Network.

Regarding international telecommunications links, this is primarily done through satellite communications. A company called Telephone Systems International S.A. (www.telsysint.com) provides international connectivity. According to Afghan Wireless, there are satellite earth stations - one Intelsat (Indian Ocean) linked only to Iran and one Intersputnik (Atlantic Ocean region), as well as a commercial satellite telephone center in Ghazni.

This New York City based company unveiled a brand new GSM phone network in Afghanistan in May, 2002. Chairman Hamid Karzai was the first person to place a telephone call over it. This has actually been the fastest GSM installation in a developing country.

There are two different kinds of phone cards planned for sale. One is called a "Fixed Line Phone Card," the other is a "Mobile Top Up." To use the Fixed Line Phone Card, one would dial 81 from within the country, listen to the instructions, and then enter the PIN as printed on the back of the card. The destination party number is then dialed. If a mistake in dialing is made or one wants to make an additional call, then "##" is entered followed by the number. The Mobile Top Up card adds funds to a GSM account. The number 171 is dialed from within the country, the PIN is entered as printed on the back of the card, and the account is automatically credited.

Of course, by now you probably just want to "reach out and touch someone" over there in Afghanistan. Why not give Osama a call? He uses an INMARSAT satellite phone, although lately has not been picking up when I call him for some reason (I wonder why?!). To call Osama Bin Laden just dial +873-682-505-331. Have phun!

Yet Another Way to Defeat URL Filters

by ThermoFish (JW)

In 17:3, the article entitled "Another Way to Defeat URL Filters" by ASM_dood put it up to readers to come up with a script to turn IP addresses into their decimal equivalent. At the end of the article a script by CSS was put in which did just that. While that script works great, most people know the hostname (URL) of the site they want to go to. Who wants to have to go get the IP address of the hostname they want to go to? Instead of the two step process of getting the IP address of the hostname and then turning that IP into a decimal, I would rather just type in a hostname and get its decimal equivalent in one step. Therefore, I wrote some code to accomplish that.

This code was written in VC++ and you need to include the WSOCK32.LIB library in the workspace for it to link properly. I left the IP to Decimal function separate to show how that is done more clearly. The retrieval of the IP from the hostname is done with the HOSTENT structure and GETHOSTBYNAME() function.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <iostream>
#include <winsock.h>
#include <conio.h>

int IPtoDec (char *ip);

int main()
{
  using namespace std;
  WSAData wData;

  if (WSAStartup(MAKEWORD(2,2), &wData) == SOCKET_ERROR)
  {
   cout << "Winsock init error\n";
   cout << "\n\nPress any key to exit.\n";
   getch();
   return 1;
  }

  hostent *h = NULL;
  char hostname[80];

  cout << "\n\n"
        << "########################################\n"
        << "# Host Name to Decimal Equivalent v1.0 #\n"
        << "#              by: ThermoFish (JW) #\n"
        << "########################################\n\n";
  cout << "Enter hostname: ";
  cin  >> hostname;
  h = gethostbyname(hostname);

  if (h == NULL)
  {
   cout << "Could not resolve " << hostname << endl;
   cout << "\n\nPress any key to exit.\n";
   getch();
   return 1;
  }

  char *ip = inet_ntoa(*(reinterpret_cast<in_addr*>(h->h_addr)));
  cout << "\nIP address    : " << ip << endl;

  IPtoDec(ip);

  cout << "\n\nPress any key to exit.\n";
```

```
 getch();

 return 0;
}

//Function to convert from IP to Decimal
int IPtoDec (char *ip)
{

        {
                using namespace std;
                char *cptr = strtok (ip, ".");
                int shift = 24;
                unsigned long acc = 0L;

                while (cptr != NULL)
                {
                        acc += atol(cptr) << shift;
                        shift -= 8;
                        cptr = strtok (NULL, ".");
                }

                cout << "\nIP as Decimal : " << acc << endl;

        }
        return (0);
}
```

Getting into Cisco Routers

by Grandmaster Plague

Cisco routers are some of the most fascinating machines on the Internet. It is almost assured that if you send a packet to a random machine on the Internet, your packet will pass through a Cisco router. The prevalence of these beauties on the net is mind boggling. But how do you break in? Well, this requires a little explaining first.

Standard Disclaimer: The information in this article is meant for educational purposes only. I do not advocate doing anything mentioned in this article. I also take no responsibility if you do anything mentioned in this article.

Some Background Info First

Cisco routers are great at passing packets from network to network. However, they are shitty at directly receiving packets sent at them. If they could receive packets as well as they could route them, then Cisco would sell an all-in-one super-duper Internet server-router gee-whiz-it-does-everything machine. Keep this in mind for the attack that will come later. Now, if you try to telnet to a properly configured Cisco router you will get one of two things. The first is that your connection will be denied (or will time out) based on a firewall ruleset, or because tcp/ip access is not allowed to the router (serial only). Either way, bypassing this first case is beyond the scope of this article. (Hint: combine the info to be learned in this article with my spoofing article in 18:3 for your answer.) The second possible thing is you get a password prompt. If you get this (just a password prompt) you're most likely at a router, and it's on to the rest of the article.

Conceptualizing The Attack

The attack boils down to this. First, you flood the router from one host, causing it to default to a sort of "safe mode" wherein only the barest of routing functions are executed. Ciscos have been made to keep on routing until they can't possibly route anymore. This is why critical system access goes before routing functionality goes. Now, Cisco builds in a little safety net for admins who this happens to by letting them still get access to their system to shut down a router-gone-haywire. So, if the system is overloaded, you can telnet in and enter the default password to get complete enable (root!) access to the router. You then will transmit the router's password file to your machine and crack it. Now you have full enable access and can do whatever you please with the router.

The Attack Itself

The first thing you'll need for this attack is at least one valid socks (or wingate) proxy or a shell on some system - anything to make your access come from another host. I would recommend at least two such hosts to do this. First, you want to initiate a DoS attack that will flood the router,

such as a huge password in the password field, or an icmp flood. For the purposes of this article, we will use a huge ping command (as root on a linux/BSD box):

ping -s 65535 -f -c 1000000 cisco.host.whatever.net

Get that started and wait for a bit. Then, after a minute or so, you telnet to cisco.host.whatever.net from a different IP address (another NIC with its own IP address, not one behind the same NAT router, or through a wingate). Now, you get a nice prompt and type the default password in (usually enable or admin... otherwise check www.mksecure.com/defpw/). Now you're logged in with full enable access. We want to keep access and not be noticed, so we find either the encrypted or (if lucky) the unencrypted password. This is usually simple. Start logging your terminal session and type in "sh conf". When you see a line that starts with "enable secret" or "enable password" grab that line. If you only see three arguments to either of these commands, the third argument is the password. Still, if you get the "enable password" line, then be happy, because even if it's encrypted, it's a Cisco Type 7 password (whose encryption has been broken hundreds of times). See http://hackersplayground.org/papers/crack-cisco-passwords.txt for code and explanation on how to break Type 7 passwords. If you're not so lucky, you'll see something like "enable secret md5 +949a8(%0xCV8". That's an md5 encrypted password. You can dump it into john the ripper (after some formatting). Let it run for a little while and you'll get a nice password to use to get access to the router. Congratulations, you should have full enable access at this point. Disconnect from the router and stop your ping flood.

What Do I Do Now?

Well, I'd be surprised if people reading this article didn't have ideas of things they can do once they get full enable access on a Cisco router. But, for those of you who don't, I'll give you some ideas. Modify the route tables to go through another machine which can sniff data. TunnelX is the best project I've seen to do this. It was featured in *Phrack 56* (http://www.phrack.org/phrack/56/)in the article "Things To Do In Cisco Land When You're Dead" by gauis. That article covers installation of tunnelx. If you realize that a significant bit of traffic goes through routers, you'll realize that you need to set up a script to check the packets you sniff for key terms and discard as they come in, so you don't waste ten gigs of disk space in two minutes. Another fun thing about routers is that they're often connected directly (through serial) to mainframes at NOC's. These machines are super fun to play with and are often otherwise inaccessible to the outside. Ciscos that are the primary router for a network are almost always trusted machines on that internal network. You can get to machines that are not visible to the Internet. DoS is also really easy. Just change the route table of the router to send all packets received to 127.0.0.1. The possibilities are endless.

Conclusion

Cisco routers are some of the most prevalent machines on the Internet. The security of these machines is crucial to the survival of the Internet and corporate networks around the globe. It is often unbelievably easy to get full enable access on a Cisco router with very little work. There are many ways to secure your system. (See *Hardening Cisco Routers* by Thomas Akin, O'Reilly Books, ISBN 0-596-00166-5 or http://secinf.net/info/fw/cisco/add.html#routing or a host of other sites.) But Cisco has a lot of problems that they need to fix before your router will be secure out of the box. Hopefully this article has moved that along a bit.

Hi again Mary (Nary).

A New Era of Telecommunications Surveillance

by The Prophet

As the satellite republics of the Soviet Union fell at the end of the 20th century, the Western world was shocked at the surveillance societies erected by their authoritarian governments. From a population of 17 million in East Germany, the dreaded Stasi secret police employed 34,000 officers, including 2100 agents reading mail and 6000 operatives listening to private telephone conversations. Additionally, over 150,000 active informers and up to two million part-time informers were on the payroll. Files were maintained by the Stasi on more than one out of three East Germans, comprising over a billion pages of information.

While centralized domestic surveillance in the United States has probably not yet reached the levels seen in East Germany, the picture is

very different when government databases are linked - and especially when government databases are linked with commercial ones. To help it fight the insane "war on [some] drugs," the federal government has already connected the databases of the Customs Service, the Drug Enforcement Agency, the IRS, the Federal Reserve, and the State Department. These are accessible via FinCEN and other law enforcement networks (and probably via classified intelligence networks as well - but sorry, that's classified). Additionally, the United States has relatively few data protection laws (particularly concerning the collection of data for commercial purposes), meaning the extensive use of computer matching has led to a "virtual" national data bank. With only a few computer searches, and without obtaining a search warrant, law enforcement can gather a comprehensive file on virtually any US citizen in a matter of minutes.

Telecommunications, unlike paper and electronic records, enjoyed much stronger privacy protections - until September 11th. Americans have the egregious wiretapping abuses of J. Edgar Hoover's FBI to thank for this. However, long before September 11th, the FBI was laying the groundwork to turn the US telecommunications system into a surveillance infrastructure. This began in 1994 when, at the strong urging of former FBI Director Louis Freeh, Congress passed the Communications Assistance for Law Enforcement Act (CALEA, pronounced "Kuh-LEE-uh" for short).

The legal reasoning behind CALEA is fairly recent and, to fully understand it, it should be considered in light of the failed Clipper Chip key escrow initiatives of the early 1990s. During the consideration of key escrow legislation (which ultimately failed) and CALEA (which was ultimately successful), the FBI nearly convinced Congress that Americans have no legal or moral right to keep any secrets from the government. Fortunately, Congress was not fooled - they decided that while Americans should be subject to surveillance of all of their communications, citizens could still keep secrets from the government. How magnanimous of them! The stated purpose of CALEA is to preserve, despite advances in technology, the surveillance capabilities law enforcement agencies possessed in 1994. The actual implementation of CALEA, predictably, has been much more broad than Congress originally contemplated.

Technically, the FCC is tasked with determining the surveillance capabilities telecommunications carriers are required to provide. Because surveillance is not the core competency of the FCC, they have deferred to the

FBI's expertise, and serve as a "rubber stamp" for the technical requirements the FBI requests. Privacy groups have widely criticized the resultant 11-point "punch list," with which telecommunications carriers must comply, as a dramatic expansion of the capabilities originally contemplated by CALEA. For example, mobile telephones containing GPS locators have recently appeared on the market. Touted as a safety feature, GPS is also a surveillance feature mandated by CALEA. If you carry such a phone, the FBI knows exactly where you are at all times. (Of course, J. Edgar Hoover's FBI will only use that capability against criminals and terrorists, right?)
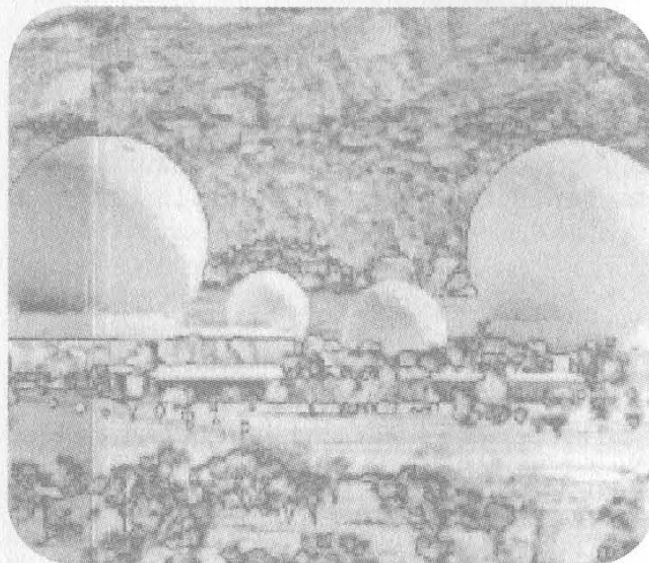
Other technical requirements on the "punch list" include the capability to intercept all packet-switched communications, which includes Internet traffic. The FBI presents this in seemingly reasonable terms - they just want to tap Voice Over IP (VoIP) and other packet-mode voice communications like any other telephone call. Of course, to those familiar with TCP/IP, this is very frightening indeed; the only way to intercept the "bad guy's" data is to look at everyone's data. On the Internet, this is accomplished with DCS1000 (formerly Carnivore) and other proprietary surveillance devices. The FBI really likes to keep secrets, so they won't reveal a complete list of the surveillance devices they use, won't reveal the manufacturers, and won't release a full list of surveillance capabilities. In the face of intense Congressional pressure, the FBI reluctantly allowed one "independent technical review" of the nearly obsolete Carnivore system. However, this was conducted on such restrictive terms that MIT, Purdue, Dartmouth, and UCSD refused to participate on the grounds the study was rigged. Jeffery Schiller, when explaining MIT's refusal to CNN, said, "In essence, the Justice Department is looking to borrow our reputation, and we're

not for sale that way."

Eventually a research team at the obscure Illinois Institute of Technology Research Institute was selected to perform the study. While the FBI intended to keep the identities of the "independent researchers" a secret, they accidentally leaked the researchers' names on an incorrectly formatted Adobe PDF document. So much for secrets. As it turned out, three of the supposedly "independent" team members possessed active security clearances (including top secret NSA and IRS clearance - go figure), and two others had close ties to the White House. With the deck so carefully stacked in the FBI's favor, it is surprising (and telling) the IITRI study warned Carnivore "does not provide protections, especially audit functions, commensurate with the level of the risks," and was vulnerable to "physical attacks, software bugs or power failures." The ACLU offered to perform its own review of Carnivore, but the FBI not-so-politely declined. In the interim, the next release of Carnivore, called DCS1000, is now in operation. As with Carnivore, the capabilities of DCS1000 are not fully disclosed. Mysteriously, many Internet Service Providers (ISPs), including Comcast and Sprint, have implemented so-called "transparent proxy" servers, possessing extensive logging capabilities. Comcast, in a widely-publicized incident which even drew the ire of US Representative (and hacker foe) Ed Markey, was caught associating the web browsing habits of its customers with their IP addresses. While Comcast claims they no longer collect this information, it is likely that other ISPs have implemented similar technology - and equally likely that Comcast could resume logging at the FBI's request.

While telecommunications providers are wary of providing the FBI with direct access to their infrastructure, most do not object out of privacy considerations. Instead, they are primarily concerned that the FBI's activities do not cause disruptions in service. Telecommunications carriers are particularly indignant at court rulings requiring they provide the FBI with direct access to telephone switches, and grant them the ability to install their own software upon the switches. Lucent implemented this capability on the 5ESS switch in the 5E14 software revision, which nearly every 5ESS in the country now runs. Surveillance capabilities have also been present for some time on the Nortel DMS100 platform. While the capabilities of the FBI's switch software are, like DCS1000, presently unknown, the 5E14 software revision incorporates a number of useful surveillance features on its own. For example, when a surveillance target makes a phone call, the switch can silently conference in a pre-programmed telephone number. Because the FBI also keeps secrets from telecommunications providers, even refusing to share basic architectural information, providers are skeptical of the FBI's assurances that no potential for disruption exists. Additionally, because most surveillance capabilities are provided by the FBI's own software, telecommunications providers cannot audit court-ordered wiretaps. (Of course, J. Edgar Hoover's FBI is trustworthy, so checks and balances are not necessary.)

The cost of implementing surveillance capabilities is also of major concern to telecommunications providers. In exchange for retrofitting the nation's telecommunications infrastructure with a surveillance architecture of which Stalin could only dream (at one point in the CALEA legislative process, the FBI proposed implementing the capability to simultaneously intercept and record one out of every 100 telephone conversations taking place in each central office), the federal government promised $500 million to telecommunications carriers. However, implementing all of the requirements on the CALEA "punch card" is estimated to cost the cash-strapped telecommunications industry as much as $607 million. With the additional "roving wiretap" capabilities granted to the FBI after September 11th in the obliquely named USA Patriot Act, the cost of implementation is likely to soar even higher.

Americans face a new, and potentially dangerous, era of surveillance. History has proven through the nuclear arms race, the Nixon administration, and other similar craziness that things which are possible are not necessarily a good idea. Surveillance societies have appeared in the not so recent past, and they were frightening indeed. Stalin's Russia. Ceausescu's Romania. Hoenecker's East Germany. Perhaps the United States can avoid the mistakes made by the surveillance societies of the 20th century. And perhaps J. Edgar Hoover's FBI is also completely honest, professional, and incorruptible - just like Robert Hanssen.

Web Server Discovery Tool

By Boris Loza

This project started when I decided to find all the web servers on my network. One can do this by running nmap to identify all open HTTP/S related ports: 80, 8000, 8080, or 443. But nmap is known for crashing servers (just a couple of misbehaves to mention: killing syslogd on Solaris, Cisco's DOS, etc.). Therefore it is not allowed in some organizations. Moreover, even if the ports in question are open, nmap doesn't give you the type and the version of the web server listening to it. Nmap can also trigger the IDS and page the information security group! Using commercial tools like ISS Network Scanner or CyberCop to find all web servers on the network is cumbersome, time consuming, and IDS detectable.

Taking all this into consideration I decided to write my own tool for discovering all web servers on the network. I wanted this tool to be easy to run, not to use "crafted" TCP packets, be efficient, quick, and provide as much information about discovered web servers as possible. We intended to run this tool periodically, like a war dialer, and to do this even during business hours (before users shut down their workstations to go home). I wanted to create a tool as efficient as possible with minimum network and server impact. In this article you'll see what I eventually came up with.

The Tool

First, let's understand a little bit about how a web server and a browser communicate. The browser or client generates request headers and sends them to the web server. The server receives the request headers, translates them, and generates the response headers. These response headers have to include information specific for the web server that will allow both the browser and the server to communicate. I decided to use this information to create the tool.

In the heart of the tool is the following Perl code:

```
1.    use HTTP::Response;                                       #Encapsulate HTTP responses
2.    use LWP::UserAgent;                                       #Dispatch WWW requests
3.    my $ua = new LWP::UserAgent;                              #User agent object created
4.    $ua->agent('Mozilla/5.0');                               #Using Mozilla/5.0 as agent's name
5.    my $req = new HTTP::Request(GET, "http://$ARGV[0]");      #Encapsulate a request using GET method
6.    print $headers = $ua->request($req)->headers_as_string;  #Read response from the web server
```

I use Perl's libwww-perl library for WWW access (rows 1 and 2). This library will provide the API for writing my own WWW clients.

First I need to create a request header (rows 3 and 4) by specifying the name of the web browser the request comes from. Now I can send the request to the server using the GET method (row 5). Strictly speaking, I can use any agent's name here, for example agent('Foo'). This doesn't matter, since I need just one response from the server and I am not going to continue the session. Now I can print everything that comes from the server (row 6). After naming this little script as ws.pl and running it against one known web server I've got the following output:

```
C:\>ws.pl 192.168.0.40
Date: Thu, 04 Apr 2002 15:27:06 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/4.0
Content-Length: 56
Content-Location: http://192.168.0.40/Default.htm
Content-Type: text/html
ETag: "f82f8972cf9ac01:5ee8"
Last-Modified: Mon, 19 Feb 2001 23:55:33 GMT
Client-Date: Thu, 04 Apr 2002 15:28:43 GMT
Client-Peer: 192.168.0.40:80
X-Meta-Postinfo: /scripts/postinfo.asp
```

As I expected, the web server strikes back by sending all necessary information that will be needed for the session. If no HTTP web server is listening on port 80 the output will be:

```
C:\>ws.pl 10.56.53.27
Client-Date: Thu, 04 Apr 2002 18:38:39 GMT
```

In this article I am not going to explain all response headers from the output. For anybody who is interested, please refer to RFC 2616. For the purpose of the script, I am interested only in one: Server: Microsoft-IIS/4.0. This is a name of the web server I connected to. So I can modify line 6 of the script to display only this response header:

```
print $headers = $ua->request($req)->header('Server'):
```

```
C:\>ws.pl 192.168.0.40
192.168.0.40    Microsoft-IIS/4.0
```

After understanding the concept, I started working on something more useful. Below is a listing of the complete tool. This tool will discover a single web server or all web servers on a given subnet. The default port to scan is 80, but you can specify any port you wish:

```
#Web Server Discovery Tool. Boris Loza, 2002
use HTTP::Response;
use LWP::UserAgent;
use Getopt::Std;

$usage="Use:\tws.pl [-v] [-p port] hostname
\tws.pl [-p port] -C IPadress
\tws.pl ñh {To print this}

Discover Web Servers.
Hostname can be specified by an IP address or a DNS name.

Options:
        -v          : verbose
        -p          : specify a port (default 80)
        -C          : scan class C subnet

Example: ws.pl -v 192.168.10.3          {OR}
         ws.pl myhost.com               {OR}
         ws.pl -p 8000 myhost.com       {OR}
         ws.pl -C 192.168.0             {OR}
         ws.pl -p 8000 -C 192.168.0";

getopts('C:hp:v') || die "$usage";

print "$usage" if $opt_h;

my $port=80;             #Default port to scan
if ($opt_p) {$port = $opt_p;}
my $host = $ARGV[0];

#Create Request headers
my $ua = new LWP::UserAgent;
$ua->agent('Foo');

#Send Request headers
my $req = new HTTP::Request(GET, "http://$host:$port");
my $response = $ua->request($req);

#Use verbose mode. For single host only!
if ($opt_v) {
```

```perl
            print $response->headers_as_string;
            exit;
        }
}

#Scan Class C Network
$count = 1;
if ($opt_C) {
        (my $subnet, my $node) = ($opt_C =~ /(\d+\.\d+\.\d+)\.(\d+)/);
        if ($node) {print $usage; exit;}
        while ($count <=254) {
        my $host = "$opt_C.$count";

            #Skip unreachable hosts for speed (for Windows users only). Comment out for UNIX!
            if (`ping $host`=~ m/(timed out)/) {$count++;next}

            my $ua = new LWP::UserAgent;
            $ua->agent('Foo');
            my $req = new HTTP::Request(GET, "http://$host:$port");
            my $response = $ua->request($req);

            if ($response->header('Server')) {
                    print $host,"\t",$response->header('Server'),"\n";
            } elsif ($response->header('Proxy-Agent')) {
                    print $host,"\t",$response->header('Proxy-Agent'),"\n";
            } elsif ($response->header('Title')) {
                    print $host,"\t",$response->header('Title'),"\n";
            } elsif ($response->header('Client-Peer')) {
                    print $host,"\t","Web Server not found, but port $port is open\n";
            }
            $count++;
            }
exit;
}

if ($response->header('Server')) {
        print $ARGV[0],"\t",$response->header('Server');
} elsif ($response->header('Proxy-Agent')) {
        print $ARGV[0],"\t",$response->header('Proxy-Agent');
} elsif ($response->header('Title')) {
        print $ARGV[0],"\t",$response->header('Title');
} elsif ($response->header('Client-Peer')) {
        print $ARGV[0],"\t","Web Server not found, but port $port is open\n";
}
```

To run the ws.pl against a single host type:

```
C:\>ws.pl 192.168.0.2
Microsoft-IIS/4.0
```

Or specify a different port (port 80 is a default):

```
C:\>ws -p8000 192.168.0.58
192.168.0.58    HP-Web-Server-3.00.1696
```

You can use both an IP address and a DNS name here. For the verbose mode use the ñv option. The following command will print all response headers for the host 192.168.0.2:

```
C:\>ws.pl -v 192.168.0.2
Date: Fri, 05 Apr 2002 15:49:09 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/4.0
```

```
Content-Length: 56
Content-Location: http://192.168.0.40/Default.htm
Content-Type: text/html
ETag: "f82f8972cf9ac01:5ee8"
Last-Modified: Mon, 19 Feb 2001 23:55:33 GMT
Client-Date: Fri, 05 Apr 2002 15:50:45 GMT
Client-Peer: 192.168.0.40:80
X-Meta-Postinfo: /scripts/postinfo.asp
```

To scan the whole class C network use the ñC option. For example, to discover all web servers running on port 80 on the subnet 192.168.0, type:

```
C:\>ws.pl -C 192.168.0
192.168.0.10        Microsoft-IIS/5.0
192.168.0.21        HTTP/1.0
192.168.0.33        IBM_HTTP_Server/1.3.6.4 Apache/1.3.7-dev (Unix)
192.168.0.34        IBM_HTTP_Server/1.3.12 Apache/1.3.12 (Unix)
192.168.0.40        Microsoft-IIS/4.0
192.168.0.45        Netscape-Enterprise/4.1
192.168.0.82        ApsyServer 1.0
Oracle HTTP Server Powered by Apache/1.3.12 (Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a
mod_perl/1.24
Citrix Web PN Server
Web Server not found, but port 80 is open
```

HTTP/1.0 on the host 192.168.0.21 is a web interface for HP printer.

To scan the same subnet looking for web servers listening on port 8000, type:

```
C:\>ws.pl ñp 8000 -C 192.168.0
................
```

For help, print ws.pl ñh:

```
C:\>ws.pl -h
Use:    ws.pl [-v] [-p port] hostname
        ws.pl [-p port] -C IPadress
```

Discover Web Servers
Hostname can be specified by an IP address or a DNS name.

Options:
    -v   : verbose
    -p   : specify a port (default 80)
    -C   : scan class C subnet

```
Example: ws.pl -v 192.168.10.3            {OR}
         ws.pl myhost.com                 {OR}
         ws.pl -p 8000 myhost.com         {OR}
         ws.pl -C 192.168.0           {OR}
         ws.pl -p 8000 -C 192.168.0";
```

Conclusion

   After running this tool for the first time I found three times more web servers than I had on my list of the "official" web servers. The ws.pl has proved to be very efficient. Now I run it periodically to discover rogue web servers without any network or server impact. What else is important, I know what every line of this script is doing and can customize the script for my needs.
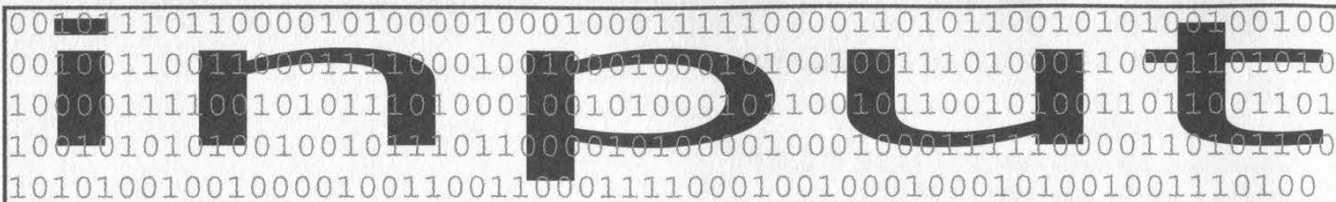
Darwin Awards

Dear *2600:*

I tried to log on to my school's network and my account was disabled. I visited the assistant net admin (who I happen to know and like) and he said they found suspicious stuff in my folder. Shortly after, my parents got a letter in the mail saying that I hacked the school network and that I would be punished accordingly. The net admin requested a meeting with my parents. Then I read the letter. I had WinZip, iTools, and my own PWL in my folder. The nerve of that guy! This goes to show just how much they train people. My parents wound up cutting off all access to the outside world - telephones, the Internet, my DSL - *for a whole month!* For having WinZip! I should tell the guys at WinZip.

CrashPlastic

They would definitely get a kick out of it.

Dear *2600:*

I am a new reader to your magazine. First I would just like to say that while I don't quite get most of the technical stuff, everything is quite interesting. So anyway, when I was in junior high school, I was caught with the *Anarchists' Cookbook.* I freely distributed articles that anybody wished to have, but strongly encouraged that destructive devices be used only when necessary. Of course, some spineless ass turned me in and I was called to the principal's office. To make a long story short, she wouldn't acknowledge the fact that nowhere in the school rules does it prohibit such material. She called my parents, then the sheriff. The sheriff! I couldn't believe it. I was suspended for a week and learned only that ignorance flows way too thick among those in authority. Keep up the good work and good luck on your lawsuits.

JohnnyD

Dear *2600:*

I just got to say, network administrators in the UK in schools and colleges without fail prove themselves to be ignorant beyond belief. The only qualifications required are no qualifications! All you need to do is say you want to learn to be an "IT Professional" and they "train you up" so to speak, but they don't even do that right. I found this out just last week when a close friend of mine applied for a job at my school. He was amazed at how easy it was. The course doesn't even entail learning the basics of networking, just how to turn off the event log and change people's passwords! You pay to go through a two month course, and in the end you don't even know what a protocol is, yet you're branded with the name "network admin." The system truly sucks.

Carter

Dear *2600:*

I recently created a website mostly to refresh my memory on HTML. I posted several scanned images of my weird drawings - nothing obscene or pornographic - just surrealistic, weird stuff. After about a week I was disconnected from AOL. I got a message that my password was wrong whenever I tried to log on. Eventually I found out why. They basically said that I was corrupting little kids' minds, all because I had put a MIDI of the *Sesame Street* theme song in the background just because I thought it would be funny. I know, I'm stupid for even using AOL, but that's not the point. I never even used AOL's Instant Messaging or one of its chats to tell anyone about the site. I used Yahoo's Messenger and told people in Yahoo's art chatrooms about the site. Is Yahoo owned by AOL? If not, then why would the site matter? If it is, then I don't see why they didn't just stop hosting the site.

John Fannin

At press time Yahoo! wasn't owned by AOL. But all it takes is one simpleton reporting you for being "suspicious" and companies like AOL will come down hard on you. To echo a popular refrain, get a real ISP that will back you up instead of shut you down.

Dear *2600:*

This article is about what waht kinda peoplw the hackers often are!! Im just ordaniray guy surfing suddeny get a nice little present one of your hackers which you gladly call freedom fighters. Whoops suddenly his present destroy all my music files and pictures!! What a nice guy true liberator! hm and he informs me that in colombia the goverment is cruel hm! Nice kinda fought of him and kinda thought who good theyre cruel to him! i kinda start to like CIA FBI and the colombian for treating the bottom scum succing aude eater of this planet some what productive fair way! MY feeling aBOUT YOU HACKERS IS THAT YOUR BUNCH OF IMATURE BASTARDS TALKING ABOUT RIGHTS WHILE VIOLITING OTHERS RIGHTS ! yOU ARE THE TRUE OPPRESSERES AND ERODING FORCE OF THIS PLANET!! yOUKNOW WHAT I WOLUD FOR cia CAMPAIGN FIND HACKERS PROCECUTE THEM FUCKEM FOR LIFE!"!

sINCERLY THE COMMON SENCE!!

Well you certainly told us.

Dear *2600:*

Your site is blocked on my school's network. My school happens to use a filter program called X-stop. The program is the masterpiece of a company called 8e6 technologies (www.8e6technologies.com). I went to their site and requested that your site be unblocked. The following is what was sent back to me:

"The site is currently blocked in our Criminal Skills library and does meet our criteria for blocking."

I think this is total BS. You guys aren't criminals

and your website is nothing more than a news/information site. Keep fighting and good luck on the DeCSS case.

Nick Fury, agent of S.H.I.E.L.D

We'd appreciate it if everyone involved in making software purchases sends people like these a periodic note saying "Your software has been blocked from our purchasing department because you meet the criteria of Close Minded Morons."

Dear 2600:

This is the last day of my two day suspension that I received for causing a message to come up on some 4000 computers in the district (using winpopup). During 5th period, I sent a message which I intended to send to one friend. However, to my dismay, Workgroup was selected instead of User. My little message said a mere "Hello."

About an hour later, the network administrator and the assistant principal came into the room and dragged me down to the office. After much arguing and reviewing of the technicalities of the network rules, I still received a suspension. I can understand a suspension if I would have said something like "F*** you" or something, but "Hello?" Please. Surprisingly, I still have network access, however I did fail a test as a result of this.

After it all happened, I spoke with the network admin personally. He told me that the security system (Foolproof, what a joke) doesn't do much, that I can even run commands like regedit, msconfig, edit, and fdisk.

It truly sickens me that our school can be run by people who don't understand most of the rules themselves.

Fisqual

Dear 2600:

This is regarding Anthony D. Bower's letter and your response in 19:1. I hope you've calmed a bit! I just think you shouldn't be too severe in dealing with the "dimwit" flight attendant. There was obviously much paranoia and caution during the still shaky early months following September 11, especially in American airports. If you even try for a moment to think of the entire situation from her possible point of view (likely seeing the "Passport" vulnerability article, plus all those pictures of actual passports), I can sympathize with her. So do you really feel she could ignore her apparent perception, not even check it out (which is where it ended, thankfully), and feel secure in doing so? And is being so (perhaps) "over" cautious always such a crime?

RW

Hysteria of that sort should not be tolerated, especially from someone who is supposed to be able to remain levelheaded in times of stress. What happens when she decides that anyone of a certain nationality is suspicious? Do you sympathize with her then? For someone to be taken off a flight because a flight attendant doesn't understand their reading material is simply unforgivable and a symptom of some very serious problems that we'd better start confronting.

Questions

Dear 2600:

I've been reading your issues since 1995. I'm from Brazil. I just want to know if I can translate your magazine for my language? That would be better for me and other Brazilians who read it!

Ricardo

We have no problems with people translating or otherwise spreading our stuff around. But we would draw the line at selling it if it was just a translation. If you want to start your own magazine and occasionally use articles from 2600, that to us is a far preferable way to go about this. Every part of the world has its own unique outlook and to just copy what we say wouldn't be fair to your potential readers. Plus we would like for such publications to return the favor and supply 2600 readers with information from their perspective.

Dear 2600:

I want to have a 2600 barbecue on my roof this summer. How can I advertise?

marblehead

And just what in hell is a "2600 barbecue?" If you're trying to set up a meeting, just look at our guidelines at www.2600.com/meetings. It's unlikely having meetings on your roof would qualify though as our meetings are in public areas and usually don't involve fire.

Dear 2600:

I want to send an anonymous fax to several offices explaining why a fellow employee was fired. With Caller ID and such, is there a safe way to do this without risking termination myself? I've thought of going to a Kinko's or such and sending it, but I don't think they'd keep it anonymous too long if lawyers got involved.

MW

*Assuming there isn't a crime being committed here, you're probably best off doing this from your own home or that of a friend since it's impossible to know how much some retail outlet is going to protect your privacy. You should be certain you block Caller ID by dialing *67 before your call and don't call a toll-free number since ANI is much harder to block. Above all, make sure the fax machine you use doesn't have the name and number of the owner emblazoned on every fax that's sent. Getting a machine out of the box that hasn't been programmed at all may be the safest method.*

Dear 2600:

Is it possible to make an Italian edition of your documentary *Freedom Downtime.*

gomma

When we get the DVD out, we hope to have as many language subtitles as we can get translators for. If you're a translator, contact us!

Dear 2600:

I operate a high volume video rental business. I would like to purchase several copies of *Freedom Downtime* and offer them as free rentals to interested customers. Are there any legal hurdles I must clear be-

fore doing this?

fallout

As long as you're doing it for free, it remains uncomplicated. Let us know how it goes.

Dear *2600:*

How can there be an organized meeting in North Dakota, but no meetings whatsoever in New Jersey?

psi

Probably because New Jersey is close to two major cities (New York and Philadelphia) where meetings already take place and also because there isn't one major city that stands out in New Jersey as the logical place to have a meeting. It's important to realize that the official monthly meetings aren't meant to occur in everyone's hometown. They're a somewhat special event where you go to meet new people from other places. This is why large cities tend to work better. But for those who absolutely can't travel (and to save ourselves from having to print the name of every town in the country), we can say that unofficially meetings can take place in any mall food court on the first Friday of the month starting at around 5 pm. And if that doesn't cause mass panic, nothing will.

Dear *2600:*

Who exactly is Network Solutions and who gave them the right to monopolize the domain naming "industry?" What is involved in acquiring a domain name and why can't we just do it ourselves without having to shell money out to some company?

Mark12085

A better question is who exactly is ICANN and what gives them the power to control virtually all aspects of domain name management? The scandal of top level domains alone could fill a book. We see no reason why there can't be dozens, hundreds, even thousands of top level domains added - except that this isn't what corporate/government interests desire. We remember fondly the days when domain name registration was free and the net wasn't so focused on money and power. There are many possible ways the net should and could be run. Perhaps we can get there by learning how the net really works and insisting that we have a say in shaping it.

Privacy Issues

Dear *2600:*

This is in response to Screamer Chaotix's article "Examining Student Databases" in 18:4. The university I attend (I won't mention the name, just in case) has a similar privacy hole. It allows public access to any student's phone number, address, and e-mail address. It also displays other little things like hometown, major, and what year of school they're in. It does not, however, display student ID numbers. The main reason it is such a privacy hole is that it is located on the university web page, therefore able to be accessed by *anyone* with a web browser. Slightly unsettling.

Godless Phreak

Dear *2600:*

This may be old news to most, but still of interest to many. While tinkering with a port scanner and some other utilities lately, I've found something rather alarming, even if a little unsurprising.

KaZaA-type P2P clients like Morpheus and Grokster (and KaZaA, of course) do *not* in any way mask IPs from peer to peer. In other words, anyone sharing files with anyone else can easily see the sharer/sharee's IP (I suppose that's what "peer to peer" means). While running the Grokster client, I performed a scan of my own open ports. I noticed that there were six people downloading files from me in the Grokster client and there were six open connections on my machine's port 1214. Five of these ports were tunneled to different remote IPs. The sixth was a duplicate. Back to Grokster... sure enough, the same user was downloading two different files from me.

From that IP address, I was able to see that he was a Comcast high speed user in the southwest running Windows 98 at 1024x768 res. I could sniff all of his open ports and probably could have done quite a bit of damage if I wanted to. I'm sure I could have also snagged *loads* of other info as well. I know that this isn't really big news, but it's still pretty scary to see how easily obtainable (and corruptible) information can be.

For someone with nasty intentions, these P2P sharing programs are simply a gargantuan database of people to phuck with. For The People In Charge, this could easily become the Internet equivalent of a law enforcement official wandering past an open door and seeing something "suspicious." No need for a warrant when you have "probable cause." What percentage of these end users would you suppose even *remotely* understand the need to safeguard their IP addresses and secure their ports? My guess is not very many.

Even someone who may understand a need for security may not realize the blatant threat KaZaA clients present them. These clients are unlike most of the Gnutella variety where the IP addresses are listed in plain sight. KaZaA employs a username to identify its peers. This makes a user's IP less obvious but still easily obtainable. An alias may give the user a sense of anonymity which is, of course, completely false.

bear

Dear *2600:*

I write from my own experience in running web servers off of cable modems in regards to Johnny Slash's letter in 19:1 about Roger's Cable. I've run websites from various RoadRunner accounts for over three years now with decent traffic and have never had problems so long as I "neglect" to tell RoadRunner about them.

Legally speaking, I believe it is more illegal for them to try to discover a server behind your cable modem than it is for you to run a web server (invasion of privacy and trespassing counts versus a TOS violation). So if they call to ask you about your UT server, you can ask them just how they know that and so forth with the usual threats. But ensure that you're not eating up enormous amounts of upstream bandwidth and you most likely will never hear a peep from them.

thoughtcrime

Remember, it's no more illegal for you to try and see what they're running than it is for them to try and see what you're running. But they have the power to cut you off if they don't like what they see.

Feedback

Dear *2600*:

This is in response to Anon O Mous' letter in 18:4. You start off strong advising people to read *Animal Farm* and *1984*. But you falter in saying that we aren't going to change anything. One of the biggest problems in society today is not ignorance but apathy. There are plenty of "proles" out there who know what's going on but don't want to do anything about it. A good example would be the last election when people wanted to vote for a third party candidate but said silly things like "A vote for Nader is a vote for Bush!" Anyone who has that sort of attitude deserves what they get. The concerned and willing have to work extra hard to fight whatever stigmas are out there. I think one of the more important things to come out of H2K was Jello Biafra's keynote speech. "Don't hate the media, become the media." Go out there and drop $14 on getting a domain and starting an online soap box. Don't waste time preaching to the choir (or using tired cliches for that matter!). There are plenty of people out there who feel the same way as we do without being hackers or computer geeks or whatever. A lot of what we fill is part of the greater whole of being human. When we feel we are being mistreated, we want change. Don't give up. The proles are listening and if we take the time to educate ourselves and share the education with everyone else, the future will be a pleasing one.

gir

Dear *2600*:

There are two articles in the 18:4 issue that I would like to criticize. The first is "Student Databases" written by Screamer Chaotix. Screamer writes about how he/she visits their friend at a university and is surprised and disgusted about how easily available the students' information is (i.e., name, email address, phone number, ID number, and address). Screamer writes on to say that typically sensitive info has to be obtained by a hacker using "skill." Welcome to college, friend. The university system is meant to be an open society of learning. If you really are a hacker, look back into the culture's history and you will find a shining example of openness. Pick up the book *Hackers* by Steven Levy. In it, Richard Stallman reminisces about the old hacking days at the Artificial Intelligence Lab at MIT in the early 70's where they didn't even use passwords to protect their personal data. They were doing it for years without any problems and their system was even on the ARPAnet. However, times change and new people came into their community and abused that system just like many people abuse things today. But that's still no reason to turn around and let it happen. As a proponent of free speech myself, I'm glad to see that the universities are allowing this information to be available to me. I'm a student at Georgia Tech and their student and faculty database has helped me out on numerous occasions in locating someone's email address or place of residence. Even if this information was protected and hidden, a determined person (or hacker with skill as Screamer says) can readily acquire this information eventually with social engineering or such regardless. When you join a college, you are joining an open community. And if you really are paranoid about your personal contact information being accessible by a terminal on campus, the university's department of human resources will gladly remove your student information from the database free of charge. Your personal information is solely yours to disclose, but you are not helping to nurture this openness that *2600* tries so hard to advocate. In this situation you're merely stifling it. This leads to a personal view of me vs. the world and this is exactly what corporate America plays off of. If you are a true hacker, be a radical and lead by example.

The second article is "IIS Far From Unhackable" by xile. For the most part it's a good informative article. It reveals the vulnerabilities of IIS rather well. However, I was surprised at where this article ended up. Issue after issue, writers and editors talk about this bad rep that hackers have because of the many irresponsible kids/crackers who think defiling websites or ruining system data is a valiant and noble effort. The editors at *2600* need to look inward at their own pages and there they will find a source of this reputation. Xile says "Now the important part to most of you: editing the web site's main page." Is this the audience you are aiming at? Web site defilers who give hackers a bad reputation? I have been a long time reader and fan of *2600* and I have looked to *2600* as an authority in the hacking culture for some time but this is simply hypocrisy. I thought this magazine was geared toward the curious and those who like to stretch their intellectual capabilities. Maybe I'm wrong. I would have seen no problem in this article if xile pointed out the vulnerabilities of IIS in order to educate people but when he listed step-by-step the procedure for defiling a website by taking advantage of IIS, he started heading in the wrong direction. There is nothing intellectually stimulating in that and it is illegal. I try hard to educate people on what a hacker truly is and I know that there are many views on this. But when I go to show someone my copy of *2600* as evidence that hackers are merely curious, and that someone sees an article like this, my credibility and yours is gone in their eyes. I hope that this is just an article that fell through the cracks and not just something you put in your mag because you needed to fill space.

Buster Doney

Much of what you say we agree with 100 percent. But it would be wrong for us to insist our exact philosophy be reflected in every outside submission we print. If we did, then we wouldn't allow the use of the word "cracker" in your letter since we believe it's destructive to the community. But you're entitled to your interpretation. In general, we don't print articles that simply advocate destruction or malicious behavior - and the vast majority of people in the hacker community seem to agree with this. But you've refined the definition and seem to be expecting everyone else to subscribe to it. It's not that simple. Almost every form of hacking, reverse engineering, exploration, whatever you want to call it, has been defined by someone somewhere as dangerous and destructive. If we restrict one bit of information because of its potential for misuse, then how do we justify printing other bits of information which could be misused in different ways? The article in question actually advises people not to abuse

these holes and to email the system administrator to tell them about the security flaw. It admittedly then goes on to tell people exactly how to deface a web page. But even if we believe that this constitutes "destruction" (and many would argue that web defacements are a form of expression similar to graffiti - also illegal), we still think the information needs to be known and that it can be used for a variety of purposes.

As for campus records, we agree that college is an open environment - for learning. That doesn't mean that information you want to keep to yourself should by default be available to everyone - either on or off campus. Back in the 70's it simply wasn't this easy to find out so much information about so many people so quickly. Individuals need to have some control over their private data - and some choice in how it's made available.

Dear *2600*:

Just got home and realized *Freedom Downtime* was on my doorstep. After watching it I can really say that you guys did an excellent job with this movie. It gets the point across. I've followed the Mitnick case for many years. I even did a high school report on Mitnick which I received a D+ on because my teacher had no clue what I was talking about. If she had actually read my report she might have learned something. I'm going to make a copy for my school and see if they'll show it in class some day, though, knowing schools they will probably want nothing to do with it. Anyway, great job guys. I hope to see all of you at H2K2.

Silent

Dear *2600*:

This is in reference to the article entitled "Another Way to Defeat URL Filters." I am a sort of "math" hacker and there is a *much* simpler way to do this (if this has escaped anyone). An IP address can be considered a polynomial in 256. If this sounds confusing hold on:

Given an IP address A.B.C.D
the resulting number is:
$A*256^3 + B*256^2 + C*256^1 + D$
Example: 207.99.30.230 would be
$207*16777216 + 99*65536 + 30*256 + 230 = 3479379686$

No real need for all the bit manipulations.

Rat

Dear *2600*:

I adored watching *Freedom Downtime*. It did not matter who I invited over to watch it with me. Everyone was able to easily follow along. Just by watching it myself and sharing it with others I saw a chain reaction of sympathy and learning.

As well as being strongly effected by the film, I thought some parts were amusing. The bit about the unlimited Metrocards was fun as well as reading the closed captioning from the television excerpts. It was nice to watch something that has a good balance of seriousness and humor.

Thank you for creating this film and making it available to the public.

Grey Frequency

Dear *2600*:

In response to the letter from chris on destroying CD's, speaking in regards to CD-R, they consist of three things: the plastic disc, a reflective layer, and, on the other side, an organic substance that the data is burned into. From what you said, the reflective layer came off and you assume that it is destroyed... but is it? I do not know what effect it would have on the organic material. If it has none, you could just reapply a reflective layer - something your common Joe won't think of. But if you're destroying CD's, you must be looking for a 100 percent effective rate, not 70 percent.

lunius

Dear *2600*:

I have been dying for the next issue of *2600* for oh, two weeks after 18:4 came out. I wanted to share with you the view of someone new to the scene and who was/is a bit of a skeptic. During the last year of my subscription I have read and reread the views of the people of *2600*. At first I disagreed with many of the views, dismissing them as "a bit too extreme." While extreme, I still respected them for what they were. My major objection was the thought that the good ole' USA was really just corporate America. Well, I listen to a lot of public radio while commuting (NPR is one of the greatest places for (somewhat) unbiased news and information!) and have listened to the Enron debacle unfold and several such things. As I kept reading your mag, I began to see how right you really are. While I do not fully agree with *all* the views and opinions expressed, my mind has been opened to new ideas.

ThieF

That's what it's really all about - opening your mind to ideas. You can do this without agreeing with us, which is something so many people seem to miss.

Dear *2600*:

As per the article you printed by Tokachu, either he was wrong or Alchemedia got upon the program and fixed it. The Lotus Screencam program is no longer able to capture the images. Clever Content displays a message asking for Lotus Screencam to be turned off before the image will be displayed. Turning on Lotus after the image is displayed causes the image to disappear and the same message returns. If you can update any techniques, or if any readers know any other methods, please let the rest of us know.

Klep

Dear *2600*:

I would like to thank you for coming out with such a great magazine. I started my subscription last summer (I just became a lifer) and find it a very useful tool as a person employed in the IT field and as a person who just enjoys using computers. My only fear is that the US government (under the control of the "corporate suits") will try and shut your publication down for trying to expose these security flaws/holes in various computer systems and software packages in your magazine thanks to the DMCA. Of course, if you're silly enough to try to use the First Amendment as an excuse

then they'll have *that* deemed against the DMCA and have that section removed from the Constitution.

James

Dear *2600*:

I don't pay money for a magazine when I can get the same info for free online: http://www.elfqrin.com/hack/index.html. That appears to be the same article that appeared in the latest (19:1) *2600*.

Mike K

You are living proof that no matter what we do, people will find something to bitch about. When articles aren't available online, people want us to make them available. When we tell people how to find the articles we print online, we get letters like the above. Would you have really found the article in the first place if we hadn't printed the address of that website when we printed the article?

Dear *2600*:

Hairball's "Fun Password Facts" in 19:1 is a good intro to the brute force cracking problem, but I think he's a little confused. Most password crackers don't generate a huge textfile with all possible combinations of characters. John the Ripper (and every other cracker coded by sane people) just increments characters stored in memory and then checks the hash of the combination against the target hash. For example, if you wanted to crack a password consisting of only lowercase letters, you'd test aaaaaaaa, then increment the last character, testing aaaaaaab, and so on. This way you can check trillions of passwords in a few hundred assembly instructions (though it will still take a while) rather than using terabytes of disk space.

Ninjak

We don't think the author truly believed that it was necessary to have this kind of disk space. As we understood it, this was illustrated to demonstrate the phenomenal amount of password possibilities that exist and how it's impossible to possess or create a comprehensive "list."

Dear *2600*:

I am writing in response to diabolik's article in 19:1 entitled "Poor Man's 3D." There is a free winamp plugin by nullsoft called "milkdrop" that does exactly what diabolik is trying to accomplish. But, it has *much* better effects. Some are really cool. It requires a little tweaking to the colors of the glasses, but all in all it is quite good looking. You can download it at http://www.nullsoft.com/free/milkdrop.

fremont_dslam

Dear *2600*:

This is in response to "Retail Hardware Revisited." The hardware that dual_parallel was using was most likely a Dell of some kind. I think they have a contract with K-mart. The nice thing about Dells is it's easy to get rid of bios passwords. While you can always remove the cmos battery on most systems, these also have nifty little jumpers conveniently labeled PASS. All one has to do is open the cabinet where the box is housed (it's never locked) and open the case. The one that they keep in the sporting goods department will attract less attention. I would be careful on disassembling the store's hardware - they don't take too kindly to it.

blind

Dear *2600*:

I got my Spring 2002 issue of *2600* in the mail last week and have been reading it ever since. When I came upon Dash Interrupt's letter on page 49 and read your response my mind could think of only one thing. Doublethink. It's getting scarier and scarier out there and it's becoming very Orwellian as I'm sure you and many others have noticed. I just wanted to get the word out and thank you for publishing such a wonderful magazine that allows people to freely voice their opinions, while they still can.

littlegreenguy

Dear *2600*:

After reading the letters section of the last few *2600's,* I decided to write a little letter about the American government and the apparent feelings for it by most of the readers. All I can really say is do not hate the government, hate the people in it. As an American, you have that right. But you have that right only because you're an American. I know that a lot of times our freedoms are infringed upon and we must fight back when this happens, such as the case with Kevin and so many others. But it is not the government. It is the shitheads who are in the government. The easiest way to deal with it? Educate yourself and vote instead of "lose morale for this great country." Just be glad you're not an Afghanistan citizen. OK, off my patriotic soap box.

Suicidal

It has to go a little deeper than that. Sometimes the system itself is corrupt and must be exposed for what it is. It's not so much a question of who to hate but rather what needs to be fixed. And addressing that is more of an obligation than a right.

Dear *2600*:

I would just like to say thank you for making such an educational magazine. You guys have helped me get through high school actually feeling intelligent while teaching my teachers things about computers.

Kronikal

Dear *2600*:

In the Backtalk section of 19:1 you advised Mingus that "Most of what constitutes hacking is the whole process of figuring things out." Fair enough. However, you precede this statement by claiming that "...relatively few people are hackers, even though quite a few either want to be or walk around saying they are." Buh!? Granted, there are plenty of people who claim to be hackers despite having no knowledge of how to go about hacking and, more importantly, no interest in that knowledge. Nonetheless, if the hallmark of a hacker is the ability to figure things out, then surely a great many people are hackers, though most may not choose to classify themselves that way. It seems to me that the more constructive answer to the multitude of pests who ask to be "taught" to hack is to stress that anyone can be a hacker, but a true hacker teaches him/herself.

Czar Donic

Your way of saying it is certainly more constructive but it's also important to understand that while anyone can be a hacker, relatively few actually see this through and far too many attach the name to themselves for no other reason than wanting attention. What we're trying to say is that people need to work at it - like most anything else, it doesn't just happen because you want it to.

Dear 2600:

Rob Rohan's article entitled "Right Click Suppression" (18:4) states that "trying to lock down a page is counter to the whole reason for the Internet anyway - freedom of knowledge." I'm surprised that a vast entity such as the Internet can be summed up with one reason. An example of right click suppression being a means to an end was in the e-learning arena. When I worked as a developer at one such company, we used right clicking suppression as a means to prevent users from viewing answers to online quizzes. The answers could be determined if one were to be able to view the source. Although it was not obvious, you had to do some looking and be familiar with binary numbers to decipher it. Obviously these online testing modules were not of serious consequence - meaning it wasn't like the GRE or SAT online testing. It was simple job task testing for convenience store workers or bank tellers.

The Internet provides a multitude of uses and in certain instances even the annoying right click suppression may be of great use.

Junglee

Dear 2600:

In 19:1 there was a letter in the Backtalk section under the Answers Needed section from a Drew. He was asking permission to use the name *2600* for his band. Since you said that you would rather him call the band something else, why not call the band "Dear 2600?" I think this would be a good name since that is where his letter was published. Do you think you could pass this along to Drew?

Aaron

Done.

Dear 2600:

You had written in a response to a letter that a URL for an @home web page was permanently 404. If you take a good look at http://www.archive.org, you will find that these URLs and their contents are recoverable. These folks have taken upon themselves the Herculean task of archiving the World Wide Web. The URLs recovered with their "Wayback Machine" are not fully functional, but at least the text and pics can be viewed.

Kristopher Barrett

Dear 2600:

One thing I like about your mag is your continuing effort to keep your readers on their toes. When I picked up my Spring 2002 issue, the first thing I noticed about the cover was, of course, Mr. Franklin's bloodshot eyes and the single tear. But upon looking closer I found these words and acronyms hidden in the lines on Franklin's face: WTO, Infinite Justice, RIAA, Cybercrime Treaty, Code Yellow, FCC, CARP,

CBDTPA, Enron, DNA, MPAA, USA PATRIOT, DMCA, and Axis of Evil. These are the only ones I have found. I'm hoping there are more that other readers have noticed.

As always, you guys do an excellent job, but I'll try to refrain from any serious ass kissing. Keep up the good work - I look forward to more hidden messages and watermarks on covers of future issues.

Manic Velocity

Dear 2600:

I have been a faithful *2600* advocate for over two years and I would like to thank and compliment you for getting such a large amount of knowledge out to the public for so long. I feel that your organization has been the most supportive throughout the Kevin Mitnick ordeal as well as being there for any other person who may have been caught in a time of distress. I also have to say that I believe you have rightfully created a loyal group of followers who will continue your practices should you fall victim to any of the current or future lawsuits that you face.

CK

We (hopefully) didn't create followers. If we did it right, we helped to channel some energy in a particular direction. The credit belongs to those who continue to fight.

Trash

Dear 2600:

It's hardly any wonder the general public doesn't like the hacker community. I mean, yeah, I know most of it comes from mainstream society's overall ignorance about many of the details of what we do and don't do and various other things having to do with the hacker community. But I also know that all one has to do to find so much of the lowlife trash that, unfortunately, seems to wind up more or less representing all of us somehow is to go into any conference bridge, IRC channel, BBS, or basically any place large groups of hackers or phreakers congregate. You're *always* guaranteed to find at least one or two idiots(if you're lucky). If you're unlucky, the better portion of the people on that given thing will be total assholes. I realize that your average hacker or phreaker isn't particularly old. In fact, most are under 18. But the fact of the matter remains that these wing nuts don't seem to give a rat's ass about treating anyone with common courtesy and respect. Not to mention the fact that they don't seem to know or care anything about how their actions reflect on us all as a culture.

These self-righteous, holier than thou, "1337" types are poor representatives of the community and reflect badly on all of us. I only wish there was a way to do something about it once and for all! But, in closing, let me just thank you for doing such a good job of casting us in a bit of a better light than the general public seems to prefer to see us all in.

captain_b

You touch upon a problem that has plagued the hacker community from the very beginning. Much of it is directly related to the ignorance of the mainstream, particularly the media. Look at it this way: Can you go up to a major network and claim to be a doctor, a

lawyer, or a carpenter? Odds are they will want some sort of evidence before they do a story on you, that is, assuming they were interested enough to do a story in the first place. But in the case of hackers, all one has to do is tell the media that they're a hacker and, without any sort of proof or display of skill, they are immediately classified as a hacker! This results in all kinds of people claiming that they're hackers when all they really are are attention-seekers. You will find them everywhere. There's not a whole lot we can do about this, short of closing our doors and only letting people we already know into a particular forum. But that defeats the purpose of the forum. The best way to deal with this is for those really interested in what hacking is all about to recognize the bullshit for what it is and, as with most any group, look for those who really do get it. Don't let yourself believe that they don't exist - they always do. Just consider getting past the garbage one of the first tasks you must achieve.

Revenge

Dear *2600:*

The Internet is chock full of information waiting to be abused - or used, rather. This includes every listed phone number in the United States of America. Now, while searching for someone's phone number with their first and last name is nothing new, that's not the only thing we can do. We can now do reverse lookups and get names and addresses from just the phone number. Here is a story, and a good example of available information services.

It was 4 am and while I should have been asleep, I wasn't. The phone rang and I picked it up. It was an automated call - at 4 am! Most of the time I would have just let this go, but I was having a bad day, so I hit *69. It read me out the number 555-555-1212 (have to protect the guilty). That was nice. But I still had no idea who this was. First, I went to http://www.anywho.com/rl.html where I entered the number and it returned the location and name of the phone. It was in Texas. I dialed the phone number and then heard the carrier signal of a fax machine. I hung up. While calling and bitching would have been nice, it wouldn't have been very effective. I decided to send satellite photos of the building the phone was in. For this, I visited the TerraServer site (http://terraserver.homeadvisor.msn.com/) and entered the address. It popped up and I copied the images into a document which I would fax.

I can imagine the look on their faces when they had a satellite photograph of the top of their building sent by someone several states away. I also, not so kindly, asked them to remove my phone number from their list. I haven't heard from them since.

deadkode

Dear *2600:*

Unsolicited commercial email (spam) is crippling the effectiveness of the Internet. Roughly 80 percent of the mail arriving in a typical email user's mailbox is spam. This is an incredible drain on users, involving millions of dollars of lost time for businesses, frustration for users old and new, and the clogging of system bandwidth and disk space.

Technology has not solved the spam problem, nor is it likely to. Filtering technology has been ineffective. Government will not enforce the laws that have been enacted until citizens start to demand action. So far, they have done very little. And the UCE industry has demonstrated a blatant disregard for the law of the land and common decency.

Therefore, we, the users of the Internet, are declaring war on spam. This war will continue until the UCE industry obeys the existing laws. We demand that the UCE industry provide functional opt-out procedures, stop forging return addresses, label advertisements in the subject line, and comply immediately with "do not contact" requests.

The FTC has announced that it is "collecting" spam. You can refer spam to uce@ftc.gov. Since the government refuses to take action to enforce the laws, we will send every piece of spam in our inboxes to the FTC until they take positive action. There is a small underground movement of users who are already doing this on a case by case basis. The goal of "spamwar" is to amplify this and give it a focused strategic goal.

We will conduct this war email by email, making the lives of the spammers hellish until they surrender unconditionally. It is time for the users to take back the Internet.

brujo

Before you get too carried away with your epic struggle to liberate the masses, you should understand a few things. Bombarding a federal agency with redirected spam - even at their request - is unlikely to accomplish anything except to waste even more resources. By calling for government action, you may one day actually get your wish - and live to regret it. The last thing you should want is government regulation of something like the Internet. It would wind up extending far beyond commercial email. All aspects of online speech could be endangered by having an overseeing body. Spam does need to be fought but we believe it can be done using available technical means. We also think that with a little imagination, we can make it pretty uncomfortable and unprofitable to be identified as a commercial spammer. Ideas are welcome.

Help

Dear *2600:*

I am looking for a skilled Hack to enter a government computer site, find, and delete two simple files (or entries). Nothing malicious involved. This really involves justice (or the lack of it) and two entries into a database made for my political views that have ruined my career. Generous reward offered and negotiable. This should prove to be a real challenge to the individual and could lead to a source of possible future income to further your personal endeavors.

Terrance

Most people would consider it malicious to enter into someone else's system and delete a file. If you know that these files on you exist, wouldn't it be better to reveal that fact to everyone and show how the system is being abused? Even if we did agree with what you want to do, you would still only be doing it to help

yourself, rather than to reveal a corrupt system and possibly help a whole lot of others. Also, you ought to know that simply deleting a file will oftentimes not accomplish anything and may in fact call more attention to it.

Dear 2600:

I have a problem and thought maybe you or my fellow readers could assist me. *Every day* I receive ten annoying phone calls that say long distance on my display. I pick up and there is no one there! I have tried yelling and screaming and punching my phone and nothing seems to work. Today within a timeframe of five minutes I received probably 20 phone calls from the same long distance number. The difference with this one is that instead of silence there is a beeping noise every so often. What can I do about this *huge* annoyance?

Adam from Ontario

We're surprised that screaming and punching the phone didn't work. That usually does it for us. But let's explore an alternative method. It sounds to us like this is a fax machine calling you. The beeps usually indicate this. Since you have the phone number, you might be able to figure out who it belongs to, either through a reverse directory lookup or by calling a variation of the number - if it belongs to a fairly large organization you might find their main number ends with "00" in the same exchange. Sometimes fax machines also pick up with humans or voice mail systems that give you the name of the company/person. You could even try hooking up a fax machine and receiving the fax yourself! That's a sure way of getting some info. If all else fails and you still wind up getting these calls, contact your local phone company's annoyance call bureau and get them to deal with the situation. This is a free service unlike the *57 ripoff that many phone companies will try to get you to use.

Dear 2600:

Thanks for your kind information on your interesting website. I do not know where can I find an answer for my question but please trust me that I need to find a way to hack the passwords of one of the users of Yahoo! mail service.

Alice

OK, we trust you.

4/1/2

Dear 2600:

I was going to your website when I found that it had been replaced by cybercrime.gov. Has the mag been shut down?

Bob Smellicular

It's interesting how many people jumped to that conclusion but still wrote to us for an answer. And it gets better.

Dear 2600:

Hey guys. Just wanted to be the first to note that this has to be the most kickass April Fool's joke I've ever seen. Partly because it's pretty believable that the DoJ might try and hijack your domain if the registration ran out. Now watch them sue you for copyright infringement over these pages or something. Wouldn't surprise me.

Nothing None

For the record, we didn't copy any of their pages. All we did was put a different IP number in one of our zone files for the 24 hour period. This kind of a change literally involves a few keystrokes and takes less than ten seconds to set up or change back. It's no more complicated than that. Inside of an hour after the business day began, we received a call on one of our cell phones from the FBI in New York saying that its parent DoJ had received a report that our page was being redirected. They wanted to help us figure out who was behind it. While it was nice of them to leave us this message, we had to wonder where they got a cell phone number that wasn't listed anywhere, why they didn't realize that this was most likely an April 1st joke, and how something so simple as changing a couple of numbers in a file and making one page go to another page is something the FBI and DoJ think is important enough for them to worry about.

Education

Dear 2600:

I'm an 18 year old senior from Cottage Grove, OR. I wrote a senior paper about the injustices that hackers go through every day and what they are really about and fighting for. I used a lot of material from your magazine and from several sources I found online. I have used this lengthy paper to convince three teachers at my high school that hackers aren't the evil bastards that the media makes them out to be. I just thought you should know that some people, even if they are in their "over the hill" years, can change their views and learn to accept other people. I have also been involved in a few heated arguments around school as a result of my paper. Evidently many people believe that the MPAA has the right to continue charging them for their CDs and DVDs after they buy them. Who would have thought?

Wild Karrde

It's inevitable that you'll run into such people but it's also important that you be prepared for their arguments - it sounds like you've met with a fair degree of success here. Good luck and thanks for your efforts.

Dear 2600:

I have been following the fight of the MPAA against the rest of the "not so free world." It occurred to me while reading the transcript of the original trial that at no time was the fact mentioned that one does not have to break CSS in order to copy a DVD. What I mean is the encryption of a DVD is based off content scrambling, not the prevention of reading the DVD. Therefore, if one wants to make an exact digital duplicate of the disc, all one has to do is make a "bit for bit" copy of the DVD and burn the copy onto a DVD blank. Depending on the DVD burning technology used, one could then play that "duplicated" DVD in any CSS qualified DVD player.

This brings me to another point. Why not ask the MPAA or DVD-CCA lawyer to actually "click" on one of those DeCSS links and give a demonstration of how it is "possible" to decrypt, copy, and play a DVD for

the court using the DeCSS code? I would bet dollars to donuts that the MPAA lawyers couldn't even run a Perl script, much less decrypt a DVD without bringing in a computer professional.

Windwalker

You're probably right on that. As for getting them to actually demonstrate something like that, it unfortunately is never quite that simple and we never had the ability to oblige them to do anything. Even though it was clear that DeCSS wasn't a necessary component to any form of pirating, it was still treated as if it were and nothing we were able to show could break down that myth. In fact, that deception was basically the main thrust of the MPAA's case.

Weird Stuff

Dear 2600:

Last Friday I tried to call my local pizza place (using a cell phone) and the strangest thing happened. Instead of reaching the pizza place, I got some machine that said "system... system... system... can not arm" and then a bunch of carrier tones. I tried calling again thinking I must have misdialed but nothing happened. The line just seemed dead. So I hung up and tried a third time, getting the same thing as the first time but without the carrier tones. I got through on the fourth try. Does anyone have any ideas on what this could be? It's really got me curious now.

soloha

Almost certainly you reached some sort of alarm or monitoring system that is installed in this pizza place. In all likelihood it's attached to a second phone line that rings when the first one is in use. It probably answers with this device when the ringing line isn't picked up by a human.

Fun Stuff

Dear 2600:

I am living in Japan. I will be racing pro here and I would like to put the 2600 logo on my car. It will consist of the 2600 logo along with your URL. I will email you pictures of the car when the design is finished. I also have Jinx hackwear going on the car. I think the more we can get people to open their eyes in every aspect of life, not just the technology industry, the better....

Gary

We have a logo?

More Info

Dear 2600:

In 18:4 DarkBlayd mentioned a device which would emit a tone which would fool telemarketing systems into removing one's number from their list. You were correct in your response that most good equipment relies on answer supervision, but there is something you did not consider. The phone company is not required to provide answer supervision to a standard local loop. While it is part of the standard protocol as far as the switch is concerned, it is not always provided to the subscriber. This is because it's becoming less common to run copper all the way back to the

CO, and because it's expensive to lay new copper bundles for residential subscribers. So, if the trunk is fiber from the CO to a MUX and then copper from there to you, there is a good chance you will not receive the supervision unless you request a line with ground start signaling (in which case the signaling is required and they'll make sure it actually works).

Anyway, what I'm getting at with all of this is that because of the chance that signaling may not work on a loop start line, a few phone systems (including cheap COCOTs) listen for the series of tones which proceed the wrong number recording. When they detect these tones they take appropriate action. For example, a couple of years ago I put those three tones on my answering machine before my outgoing message. The result was that if my friends called me from the COCOT down the street, it would return their money but leave them connected for 30 seconds, allowing them just enough time to leave a short message. I suppose a busy signal would work also, but I never tried it. Pretty funny, eh?

maldoror
Tampa, FL

It brings back memories of black boxes that used to work on crossbar and step switches. It's a similar effect for a different reason.

Dear 2600:

Websence, a proxy commonly used at schools, blocks many sites including 2600.com and basically any proxy site you could imagine. Except one. www.proxysite.com is a free tool that allows you to view anonymous proxies to connect to to avoid the Websence block. Just a suggestion for all the schoolgoers.

Bildo

Dear 2600:

Thought some people might enjoy the following test numbers for toll free NPA's 855 and 866. Dialing 855 toll free seems weird, as these two new NPAs were to be placed in service in the spring of '00. However, 855 is still "not in use" according to NANPA while 866 is seeing some use with an in service date of July 29th, 2000. These test numbers are all in the 250 exchange in both the 855 and 866 NPA: 0391, 0392, 0144, 0145, 0109, 0125, 0111, 0110, 0379, 0380, 0069, 0070, 0115, and 0116.

phlux

Dear 2600:

I spent a good amount of time close-up with a few Euro notes of the 5, 10, 20, and 50 denominations. Very close. As in, prosumer scanner at highest possible optical DPI close. I have a lot of images of the optical details (e.g., microprinting, enhanced watermarks, etc.) and done a lot of work into researching the materials, the strips, all the watermarking, and the fluorescence.

I'd like to write an article about this, but it would be graphic-intensive and large. Just warning. Just want to know what sort of restrictions on format I have. I'm assuming either straight text, HTML, or possibly XML. I'm also wondering if I should reduce the de-

Your Eyes HAVE JUST BEEN Sold

by docburton

I read angelazaharia's article "Behind the Scenes on a Web Page" and thought it would be a good idea to add what I know about ad serving and DoubleClick specifically. I used them for my ads for a while and was amazed at how simple yet violating their technology can be. Also, you should check out the manual floating around with instructions on how to work every machine and some other goodies. So do some research for the specifics. In this article I'll give you an overview of what DoubleClick does, how they do it, and some of the potential dangers and weaknesses.

The Business

A web company puts a few lines of HTML on their page that point to ad.doubleclick.net and *wham!* The user's attention has been sold to the highest bidder. Those "tags" allow either DoubleClick or the web company, if they choose, to exploit their users in a variety of ways. The most obvious is the "targeted" ad, which allows them to sell space either very specifically ("searched for the 49ers at 10 am and lives in the 94111 zip code") to very broadly ("one of the sports sites") depending on who's buying.

The main technology that is used throughout the company is called DART. Other ad serving products that we looked at work similarly to this so I'll be more big-picture with this article but still give you the guts of how it works. Also, they sometimes use other technologies for collecting suckers since they've taken over all of their competition. But DART is the most prevalent and the one we'll concentrate on.

There's also an email business that uses some of the techniques below but email is less consistent with support for gifs, jpegs, flash, and the like so making and tracking an ad is much more difficult. However, as we'll see later, privacy goes out the window far more easily than with just a browser.

The Structure of the Ad

When you go to your favorite web page there are several calls made in order to gather all of the information. The first is obviously the HTML of the page itself, and next are every image and object needed to complete the picture. Out of laziness or ignorance the ads usually go to another domain. In our case it was ad.doubleclick.net. This opens up a whole mess of issues on privacy since images bring with them cookies (a *big* mistake made during the protocol creation days) and two companies who've never heard of each other can accidentally share information about their users just because they both use a third party. Not to mention, you asked the site for info about a certain topic and, next thing you know, they've commoditized your "eyeballs."

The most basic style of ad is the link/image combo. This allows for jpegs and gifs only and is composed of an "HREF" and an "IMG SCR=". What you will usually see is an animated GIF somewhere on the page that can click through to a URL (first passing through DoubleClick). The other styles of tags all allow "rich media," meaning they can add HTML, JavaScript, Java, etc. into that banner. How do they do this? By nesting HTML in such a way that your browser will pick out the most sophisticated ad it can handle. (Sometimes they'll sniff what browser you have and just give you a tag that your browser can understand.)

I'm not going to show you every type so grab the source whenever you see an ad that's more than a simple image and you'll see what I mean. The other tags are made up of: IFrame calls that only IE4 and above will use; JavaScript calls for Netscape 3 and above; iLayer/Layer calls for Netscape 4 and above; and Frame calls for just about every browser. They are nested so that if, for example, you don't understand JavaScript, then your browser will pick up the NOSCRIPT section with just a link and image. What this means is that

through the trick of a layer, IFrame, JavaScript, or Frame that ad will be much more powerful, and usually more annoying.

The Call

I'll now give you a loose structure of the network behind every ad delivery. There are two main types of servers used: ad servers and media servers, with hundreds or thousands of each around the world living usually in data centers. That initial call to ad.doubleclick.net ends up at a dispatcher who will then pick the ad server that is closest to you based on your IP and their network map. (You may have noticed that you get a ping every now and then from DoubleClick. What they are trying to do is figure out where you are and test the fastest times to their servers.) The ad server will then take all of the info about you and what you are doing (don't worry, we'll go into detail about that later) and decide which ads to ram down your throat. Once that's decided it will pass the connection along to a media server which has all of the images, HTML, class files, and other objects to form the ad. With rich media the mouse-over will often contain m.doubleclick.net followed by a complicated string, since the ad has already been chosen and resolved.

The media servers work similar to Akamai's servers. They are basically a lot of computers sitting "at the edge of the net" that will send you an image or whatever, usually before the rest of the page loads. All of this happens (including ad selection and delivery) within a few milliseconds which is why someone like *Wired* would be tempted to give their ad space or even their regular images away to another company to deliver.

What They Know and the Cookie

There isn't too much info in the cookie even though this is usually the source of privacy flare-ups and blocking it only somewhat helps. Some of the things you'll find in it are an ID (since cookies are attached to browsers a different browser seems like a different user) and sometimes info about which ads you saw recently (in case there is a limit on how many times you should see a certain ad, or an order that they want you to see the ads in.) The ID is the most important part. When you first come across a DoubleClick ad you are assigned this ID, they record your IP, and begin the process of looking you up. Then when you return some time later and send that ID with your ad request they'll be able to tell where you are in detail.

How do they do it? They claim a variety of ways but the main one is taking your IP and reversing it to find the domain it came from. Now, that domain can tell you a lot of info. Are you using a small provider that you thought was so private? Well, they'll just look them up and see that they are in Nowheresville, U.S.A. (pop. 9) which means zip code 12345 and area code 678. Think

that using a major ISP is any better? Nope. Chances are they've reserved a range of IPs for that local phone number you just dialed into and you're in the same boat. So now DoubleClick has your provider, country, state, city, zip, and area code.

Surfing at work? Even better for them. Not only do they know where that company is located, but what industry it's in, how many employees work there, and the size of its annual revenue, etc. All of this is public info but they just have the department to put it all together and exploit you when you're trying to research Captain Crunch cereal. Think because you blocked cookies that you're safe? Well, they'll just look up your IP then, and get most of same info.

The last major piece is all the stuff in the header of your ad request. The browser type and version, operating system, date, and time of day may all be of interest to an advertiser. Running Opera on Red Hat Linux? I'm sure Microsoft would love to send some offers your way. All these things are easily sold to advertisers by checking a box.

What the Website Told Them About You

Now let's break down the long string that comes after ad.doubleclick.net/. The first is the type of ad requested between the two slashes. For the link/image combo you'll see "jump" meaning it's a link so send back a redirect and "ad" meaning only send an image. The others allow you to have rich media (JavaScript, HTML, pop-ups) and there are four of them: "adi" means send whatever the ad is in the form of an IFrame (including wrapped images); "adj" means send that ad in JavaScript form (a bunch of document.writes); "adl" puts it in a layer; and "adf" requests the ad in a frame wrap. It's the way that you ask for an ad using this code that will determine what form the ad takes.

Now for the fun stuff. The next string before the slash tells the ad server which company's ad bank (and often what section of their site) to grab the ads from. Sometimes it's obvious who they are (lycos.com) or it's a subsidiary (wn.ln I assume stands for Wired Network at Lycos Network) that ultimately points back to the larger company. Other times it's more specific (sports.lycos) or cryptic (sp.ln). I've noticed that the naming conventions vary but are usually straightforward. This is the first narrowing of the pool of ads.

After that you have the second major category between the slash and the semi-colon, such as "/baseball;". Then the scary part begins. From that point on the company can stick anything in there in the form of this=that. I used CGI to

put demographic and page info into the tags (all for a paycheck). Searching for "cars" and got a Ford ad? That's because it says "search=cars" in the DoubleClick URL. Watch out if you're registered on a site because they could put "gender=female" or "g=f" or even "x=1" all to say that you're a lady. Use your imagination as to what kind of privacy you can lose when thousands of the sites you go to all store this info in the same set of DoubleClick servers.

To be complete, you also almost always have "sz=" for the size of the ad, some version of "tile=" for the number of the ad on the page (to avoid redundancy or to send more than one together), and "!category=" to avoid certain types of ads such as adult. The line ends with "ord=[some number]?" and then a random number that might be generated per page per person. I used a time-stamp but the number is meaningless since all it does is make sure that your browser (or proxy server) isn't going to cache the ad and that when you click it goes with the correct ad.

The ads, if they are rich media, can actually use any of this info in the ad itself. So, you may see an ad that says, "Hi, Bradley Peterson" or "Check out the weather in San Francisco." Be aware that rich media is sometimes just a piece of text that is blended in with the rest of the page. If your search results first go to an ad serving company then some advertiser probably bought the word you just searched for. You'll see this technique used in a lot of "advertorials."

What They Know About You

When the ad server sends your browser to a media server it counts an "impression," meaning you saw the ad. When you click on an ad (and why would you ever want to do that?) it first goes to DoubleClick who counts the click, then gives you a 302 redirect to the advertiser's site. At that end there may or may not be "web bugs," pixel-sized clear images, to track how much farther you go into their site. For example they may be on the product info page or the "Thanks for being a sucker and buying my crap" page. The advertiser then knows that one million people were annoyed by their ad, one thousand were stupid enough to click, one hundred almost bought their crap, and one sucker actually did. They can also find out this info based on all of the targetable stuff I mentioned above. For example, Kmart might be interested that people who search for George Bush usually buy guns.

In their network business they'll make a lot of use out of the web bugs. They know that you went to a website about sports and later, when you're on a site about cars, they'll show you a sports ad. It can get very specific, like seeing an ad for a scan-

ner you were looking at a week ago on a totally different site.

To sum up, the info that is recorded about you (and targeted) whenever you see an ad is: any search words you used; domain and type (.edu, etc); your industry; your company's size; demographic info you've given; your geography; time and day; browser info; service provider; OS; and section of the site you're in.

More Evil in the Future

DoubleClick bought the largest junk-mail company in the world and is trying to combine what these scum know about you (just about every credit card purchase, what telemarketers you responded to, etc.) with everything DoubleClick knows about you online. The way they'll do this is by using a web bug on pages where you input personal information. Check those pages where you put in your credit card, address, SS#, or even last name, for a DoubleClick pixel. They may be linking up the ID in the cookie with the entire junk-mail database. They'll then use your info to give you a *really* targeted ad. Bought a printer at the Radio Shack around the corner recently? Well, now you're going to get a lot of ads for ink cartridges.

Email is the most susceptible, and they have a huge spam business. Very often you give your name and address when you sign up for email lists, register with a company, or whatever, and then your web surfing is linked to all this info. Pay no attention to their privacy statements on this, if they say they won't do something, it means that they haven't figured out how yet.

Potential Weaknesses

One of the weaknesses of the tags is found when they use JavaScript to deliver rich media. If the ad servers go down or are slow, the entire page will be frozen since browsers can't render around JavaScript. A server that has a hard time seeing DoubleClick will not be able to deliver the regular page (at least for the Netscape users). We got hammered on this more than once when no one could use our site because of slow ads.

As far as DoS attacks, good luck. They are on several different backbones and have routers that are fairly intelligent with load balancing and so on, so it will be difficult, although it has certainly been done before. Also, they supposedly eliminate from reports any spiders, bugs, etc. by using an algorithm of "too much, too fast." This doesn't mean that the ad won't be delivered, it will, just that the web company won't be charged by DoubleClick. That could be useful.

Blocking them: there is software that basically refuses to make a call to doubleclick.net. This is effective in some ways but not all companies use

the DoubleClick domain (for Public Relations reasons) and simply use IP masking. Probably a more effective way to block their ads is to sniff out the signature tag designs or look for the patterns such as ";ord=".

To shut down their email business, complain to the RBL who will put their email servers (and there are a lot of them) onto a black hole list that a lot of major companies use to block spam.

Also, their reverse domain lookup isn't close to reliable. If you work for a company that is based in Canada but you're in Florida, it appears that you're in Canada. Oddly enough AOL confuses them as well, since they only use a few IPs for everyone - it all looks like it comes from a remote part of Virginia. I'm not going to tell you to switch to AOL, but rather check out that box which translates your cookie ID to an IP and then looks up your personal info. That's a big weak spot for the company.

If you work for a company that advertises anywhere on the net, chances are they use DoubleClick somewhere. Get access to that account and give DoubleClick a "rich media" ad that will do some very nasty things across a variety of sites. Most of the time the person who actually enters your ad won't even bother to look at what the code does and might even give you access to change it yourself. So, target your audience using the above criteria and send them a JavaScript that erases or leaves a message in their DoubleClick cookie. Or tell them that you'd rather host the image (have them redirect it to you) and make some anti-DoubleClick ads (be sure to create a different image

with the same name for when the complaints find their way back to you). A rich media ad is practically an entire web page so use your imagination. Some sites even give their advertisers the entire frame straight out!

More Info

I've always found Customer Support to be very helpful and they will answer most of your questions about how it all works. Don't worry about being a client, the turnover in most Internet companies is so frequent that you can just pick a major, or better yet, minor company (just look for the ad.doubleclick.net on the page) and tell them you are a new "trafficker" or that the webmaster is out sick and you're trying to figure out how this ad stuff works.

If you're unlucky enough to work for a company that uses them, then find a way into their training class where they tell you all about how everything works, as well as what's the best way to exploit the technology and people's trust to make money. (I found the teachers to be *very* helpful when it came to the design of the DoubleClick network, type of routers used, etc.)

Well, I hope this gave you an overview of what online ad companies do and how they do it. It's up to us to explore their structure more (there is plenty of leaked info around) and point out to them the weaknesses in their system. Maybe throw a little civil disobedience in there too to let them know that you are not a person who is willingly exploited so that some huge company can sell you crap that you don't need. Good Luck!

Shout outs to blabpuppet, wiccanwarrior, KarMaKid, and the rest of the Avila crew.

Dumpster Diving: One man's trash

by Grifter
grifter@staticdischarge.org
http://www.2600slc.org

If there's one thing I love to read about and talk about, it's people rooting around in piles of garbage. I don't know why it's so fascinating to me since when it comes down to it, it basically sounds pretty nasty. I just like it.

There's something about going through a dumpster that gets your blood pumping. You know you aren't really doing anything wrong since you're not taking anything of value to someone. But you still get a rush like you're trying to pull off the heist of the century. Maybe not everyone feels that way, but I do. Maybe that's what keeps me going back. That, and the fact that I usually find some things that

have absolutely no business being in the "trash."

What Is It? Why Do It?

Let's start with the basics here, folks. What is dumpster diving? It's really quite simple. It's looking in other people's garbage. Okay, maybe not people, but local businesses and maybe even a local corporation or telco.

It's getting in the car with a few friends, driving up behind the nearest computer repair shop, and walking away with 10-12 Pentium processors. Stopping behind Barnes and Noble and grabbing a few hundred magazines without their covers. And my personal favorite, hanging out behind a cellular distribution center that has a nasty habit of not shredding customer records and throwing away faceplates by the case.

So now you can see why you'd want to be a dumpster diver, and you can see that it's not really as messy as you might have thought. I had a friend who would never go dumpster diving with me because for some odd reason he thought I liked to roll around in the dumpster behind the local Chinese buffet. Why in the hell would I do that? I explained to him that the messiest it ever got was when I'd cut open a bag and get old coffee grounds on my hands. Boo hoo! Needless to say, now he's with me almost every time I go.

What to Wear?, What to Wear?

Now I know what you're thinking. You're thinking, "Grifter, this dumpster diving sounds pretty damn schweet, but I want to be able to get kool stuff out of the trash and impress the ladies. What does the fashionable dumpster diver wear?"

Good question. Let me break it down.

Dark Clothing, Either Black or Dark Blue. It doesn't take a genius to understand that you probably don't want to be seen jumping in and out of dumpsters all over town. Not by the police, who may frown upon your late night hobby, and not by that hot girl next door who might drive past Toys R Us just as you leap from the garbage with an armload of koosh balls.

No Markings That Could Single You Out. I know you love your DefCon 9 t-shirt with the silver screen printing. But leave it at home! Once again, this will draw attention to you. But more importantly, what if someone sees you in the dumpster, and you run? Two days later you walk into that place of business you were last seen diving in - wearing the same shirt. It's going to be pretty hard to explain that it wasn't you. Just take my advice. No flashy logos.

Shoes. Footwear is important if you plan on getting inside a dumpster. It's even important if you don't plan on it, cause chances are, you're getting in a dumpster at some point. I highly recommend wearing a pair of hiking boots or something with a very thick sole. You never know when you jump in a dumpster if the piece of cardboard you're stepping on is supported by a nail just waiting to say hi.

Disposable. Not really disposable, just make sure whatever you are wearing is something you don't really care about. When you're hanging over the edge of a dumpster, you never know what that nasty crap around the rim is. This is also another good reason why you shouldn't wear your favorite shirt.

What Should You Take?

It's important to be well prepared when you go diving. There are things that you'll need to make things go smoothly. You may even want to go so far as having a bag full of these items in your trunk in case you get the mad urge to sort through trash and are away from the home base. But that's up to you.

Flashlights. Probably the most important thing you can take with you while going dumpster diving. There really isn't any point in stopping at 50 dumpsters if you can't see anything in them. There are three types of flashlights I like taking with me: 1) Mag-Lite - Everyone should have one, all the time. It's a Mag-Lite dammit. Plus they are good for knocking things aside and are very reliable. 2) Military - Have different lenses for less visibility and can sometimes be used to grab things with. (They're shaped like a hook.) 3) Compact - I like to have at least one flashlight that is small enough to fit in my mouth, so I can use both hands if needed. I have also heard that headlamps are good, but I think this would be very noticeable. I do like lights with a wrist strap also, so if you drop your light it doesn't end up at the bottom of the dumpster you're in.

Trunk Space. If you're taking a car with you, which I recommend, make sure you have a lot of trunk space. You will be amazed at how quickly your trunk will fill up. And there's nothing worse than having to stop early because you ran out of room to keep things.

Duffle Bag. A duffle bag is nice if you're going to be on foot or are parking the car away from a dumpster and then carting things back to it. Black of course.

A Big Stick. Some people like to take a stick or pole with them to poke trash bags before they cut them open. I don't do this, but hey, it's up to you.

Cardboard Boxes. Odd as this may seem, cardboard can be a lifesaver. If you are stopped by the police or seen rooting around in a dumpster, you can just say you were looking for cardboard boxes. "Yeah, my friend is moving so we need to pack up all his stuff. You would not believe the amount of crap this guy has. Hahaha." Believe it or not, this will work 98 percent of the time.

Common Sense. I will handle this in the next section.

Are There Rules to Dumpster Diving?

The short answer is no, but there are unwritten laws. By following a few simple guidelines and making sure you act like an adult, no matter how juvenile you may be, you can usually have a good time diving. And, as an added bonus, not land your sorry butt in jail.

1) Leave It As It Was. Do not make a mess, and make sure when you leave, things look ex-

actly as they did before you were there. This rule also applies to hacking, so many of you should already be familiar with it. If you make a mess or leave the gate around the dumpster open, someone will notice you were there. Once they see that someone has taken a liking to their garbage, *they will lock it up!!* You leave one day with an armload of goodies, and come back the next to find a brand new padlock on your favorite dive spot.

2) Do Not Make a Mess. See Above.

3) Use Handles if Possible. It's better to have the owner of Uncle Jim's Computer Repair Palace looking for someone named Super Ultra Ninja Killer than someone named Chris. Keep that in mind.

4) Keep Flashlights Below the Rim. Just because you have the best flashlight in the world does not mean you should show it off. Keep your flashlight below the rim of the dumpster and it will cut down on visibility in a big way. Try it sometime, you'll see what I mean immediately.

5) Don't Just Dive In. I don't care what CrashOverride and AcidBurn did in *Hackers.* Throwing yourself over the side of a dumpster without looking is a sure way to impale yourself on a piece of broken wood, put a nail straight through your hand, or fall face first into a pool of glass. Yes, a pool. There is sometimes that much broken glass in dumpsters.

6) Flying Solo. You can go dumpster diving alone, but I don't recommend it. If you're leaning over the side of a dumpster in an alley at 1 am, don't you think it would be a good idea to have someone there to watch your back?

Uh Oh! The Cops!

Do not run!! If the police do happen to show up when you're diving, running is the worst thing you can do. You automatically admit that you knew what you were doing was wrong, so wrong in fact that you thought you should flee the scene.

Now that the cops are there you're going to have to talk to them. This is not the time to play like you're some kind of tough guy, even if you are. Be respectful. I never could understand those people that put those "Bad Cop, No Donut" stickers on their cars. Nice job - now that the cop has seen that, you've pretty much guaranteed yourself a ticket. But hey, at least you made a statement, right?

Apologize for causing him/her to stop. Remember the cardboard boxes you brought? This is where they come in. Don't forget that your friend is moving. This shows that not only were you not breaking the law, but you're a helpful guy too.

In *The Art and Science of Dumpster Diving* by John Hoffman he says if you're asked a lot of questions or whether they can search your car, politely decline, stating, "I know my civil liberties, and I don't believe I have done anything wrong, therefore I don't think it is necessary." If you scream "I know my rights!!" you just turned into a criminal in his/her eyes. Most police don't expect you to know what civil liberties are, and usually won't mess with someone who does.

Do not pull the "Sure, look in the trunk, I have nothing to hide" routine. Trying to throw them off with this does not work. They took the time to stop, they'll take the time to look.

So Where Should I Dumpster Dive?

There is an easy answer to this question and it is: anywhere they don't serve food. If they make food there, then they throw food out. After about three days in the sun, a dumpster full of shrimp fried rice starts to get pretty rank. But to be more specific, I'll lay down a few hotspots.

Computer Repair Shops: Old computers are still good even though their previous owners didn't want them. You can usually find cases, power supplies, processors, and other good stuff behind them. I personally have found enough parts to build several working machines. And that was with about two months' worth of dives.
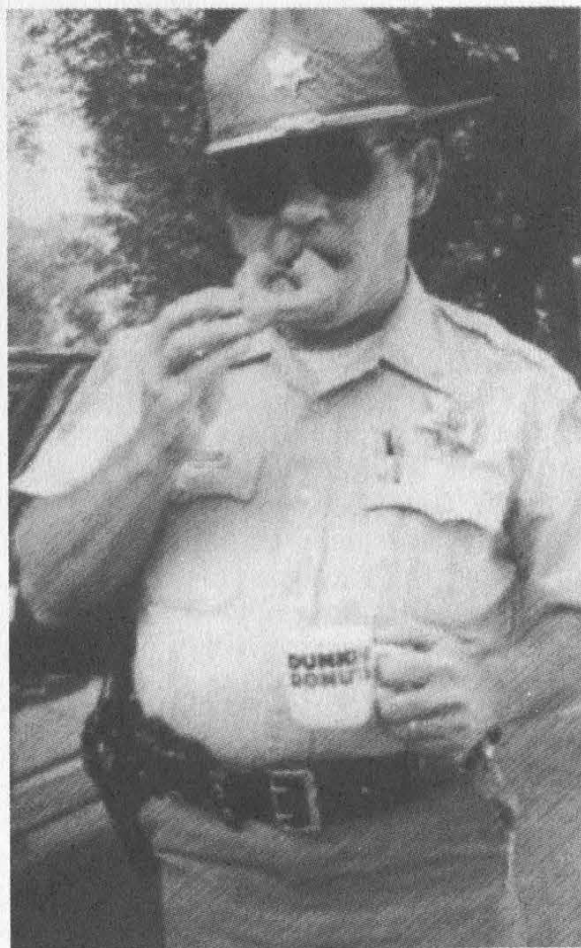
Electronic Stores: DVD cases, speaker wire, telephone cords. An odd assortment of things come from electronic stores.

Car Audio Shops: Used speakers, amps, speaker boxes.

Cellular Stores: I'll just tell you about an experience I had behind a cellular distribution center near me. One night myself and a friend decided to dive behind this distro center. We never thought we would walk away with all that we had. After about half an hour we had:

1) A four inch stack of customer records including home numbers, addresses, cell numbers, and ESN's.

2) About 25 Dish Network smart cards.

3) Two cases of cellphone faceplates.

4) Disks of customer data.

5) A year's worth of financial data still in the Federal Express packaging.

6) A list of the CEO's and upper management's personal numbers including cellphone numbers.

7) A copy of Windows 98 SE including the CD Key.

But more importantly a new favorite place to dive. I am happy to say this dumpster has never let us down.

Satellite Retailers: Smart cards, smart cards, smart cards.

Book Stores: After the month is over, all magazines from the previous month have the covers torn off and are then thrown into the trash. They're still good, except the cover is gone. You'll also find the same for some novels.

Flower Shops: As lame as this sounds, when the flowers are even slightly wilted they can't be sold so they're usually dumped into the trash. If you're the pimp that I know you are, flowers for eight girls can get expensive. Give your girls some of these - they'll never know the difference.

Industrial Areas: Piping, sheet metal, all kinds of stuff in the largest dumpsters you'll ever see. I myself like to frequent the local industrial park where I have gotten all kinds of good stuff. One place makes basketball equipment. They had a dumpster literally full of basketball rims. My friends and I played Shaq all summer, hanging from rims like crazed monkeys. You know those vibrating chairs you see at The Sharper Image? I snagged three of them out of a dumpster. They had small tears in the leather on the backside of the chair. The wall the tear faces doesn't seem to mind though. Full weight sets, weight benches, and even two Health Riders that had broken digital displays that were easily fixed. Industrial areas are very very nice, but be careful. Sometimes they have

their own private security.

Business Complexes: Office trash, the possibilities are endless!

Post-It Notes

Yes, I am dedicating an entire section to the thing that I love to find the most - Post-It Notes. Why do I love them so much? It's because everybody uses them, and they write just about anything on them.

I have found more interesting information on Post-It Notes then on, or in, any stack of paper. Think about it. Anytime someone gets a new password, or if they have to jot down an important phone number, they more than likely will write it on a Post-It before transferring it to their computer, journal, or calendar.

I have found private numbers for very important people on Post-Its. Building security alarm codes. And my personal favorite, payroll account login and passwords. It amazes me the things people write on these little brightly colored pieces of paper. They serve their purpose for a short time and are then balled up and thrown into the trash. How many people think to shred their Post-Its?

So take it from my experience. Cut open bags and look for brightly colored little paper balls. Not every single one will have great information on it. But you'll be amazed at what you find.

Conclusion

Dumpster diving sounds like fun, doesn't it? I could go on and on about the cool things I've found in dumpsters. Like the time I found a case of porno movies in a dumpster behind a comic book shop. And, as if that wasn't enough porn, there was a duffle bag full of magazines next to it. My friend took it all and distributed it to his roommates, which was fun to watch.

True story.

Once I get started I just keep thinking about the cool stuff that's out there. It's 1:30 am and I've got myself all worked up and ready to go. But seriously, you can really find some cool things in dumpsters as long as you're careful and you use your brain. If you keep yourself from getting hurt, and out of jail, you'll find that dumpster diving can become a pretty fun hobby.

If you're already a dumpster diver I hope you found this entertaining, if not educational. And if you've never gone before... get out there! There's good stuff to be found. You might feel weird the first time you do it, but I can guarantee you that by the end of that first night, you'll be hooked.

Have fun, be safe, and bring me back something cool.

Mind Tricks

by Tazz Shippensburg

The purpose of this article is to show how easy it is to make people do and think what you want beyond the standard concepts of asking certain questions to obtain the info you seek. It's more in depth actions but it will certainly pay off big time! It utilizes aspects of justice field and psychological training to use the natural habits of people against themselves.

HandShakes

The handshake is the first sign of dominance. A handshake with a palm up normally represents a person willed towards the submissive side of being. A hand shake with a palm down represents a more dominant, aggressive personality.

Eye Contact

Eye contact is key. It establishes the dominant personality in the situation. Most people hate constant eye contact, so they'll be constantly moving their eyes back and forth. And since most people hate prolonged eye contact and will want to get out of the situation, they'll be more susceptible to going along with your suggestions.
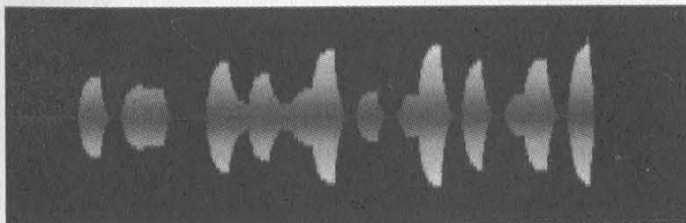
Voice

Speaking with a confident, assured tone plays a part in establishing who's who. It represents someone who knows exactly what they are talking about. When the average Joe Shmoe is talking to someone who sounds like they know what they are doing, chances are he'll drop his guard and go along with it because it sounds good.

The Mark's Reactions/Their Body Language

These are the most important things to read. Everything they do shows what they are thinking. Some of the biggest tells are as follows:
-Fidgeting, nervous body movements.
-Roaming eyes.
-Varied speaking tones, stumbling over words.
-Acting as though they'd do anything to be out of your current field of vision.
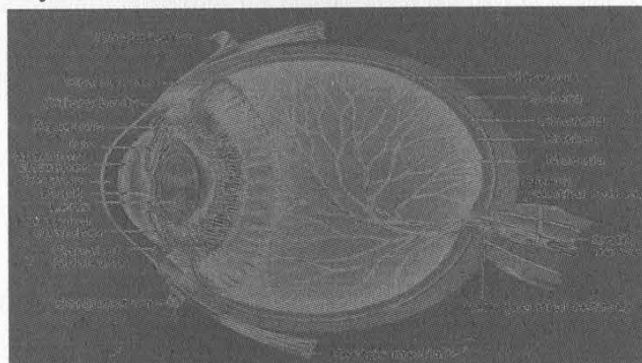
There's other ways you can find out what people are doing/thinking. Let's say you are in a cafe and someone is watching you. You know they are, but you want to be absolutely be sure. Here's what you do. Ready? *Quick!* Look at your watch.

It's that simple. When someone watching you sees you look at your watch, they automatically look at their own. It's a subconscious action that takes place. It gives them the look of "acting natural." Other actions may include:
-Lighting a cigarette.
-Taking a drink.
-Looking across the room at a person and waving like you know them. (Chances are they'll look to see who you're waiving at.)

Remember: Acting like a leader makes people think you are a leader which in turn makes them more susceptible to following you and doing what you want. Now take your new tactics and go mess with people. Enjoy!

tailed images. Right now, they are uncompressed and take up better than half a CD-R.

drew

We'd certainly be interested in an article that offers new insight into this sort of thing. It's best to send the words to us in ascii format and if the images are especially large, just send us a CD-R in the mail.

Issues

Dear *2600*:

I've perused your magazine in the past and have been impressed with the technical competence your articles display. I bought issue 18:4 today and was considering subscribing until I read your letters section, where you bash Libertarians and gun rights.

So the government is AOK in your book so long as they're only abusing capitalists and gun owners, and leaving us poor little hackers alone? That's some hypocrisy. I'm not going to spend money on people who are going to stab me in the back as soon as they get their own pet cause fulfilled. I'd wish you luck on your lawsuit, but why bother? You wouldn't care if the feds bust down my door for owning a gun or not paying taxes.

vroman

We'd say we'll miss you but it wouldn't be true. We like for our readers to actually be able to read what we say, a skill which obviously has eluded you. We didn't "bash," we questioned logic and conclusions. We do this all the time to anyone and anything we encounter. We consider such questioning to be a good thing. Never before have we been met with such hostility from so many angry people at even the mildest form of questions or criticism aimed at these topics. It only makes us want to question them even more.

Dear *2600*:

I understand your position that government should side with citizens, not corporations, but I think you want to influence this the wrong way. You said in the 19:1 Letters that government needs to "keep the corporations in check."

I put it to you that we do not need a strong government to face off against corporations, but rather a weak government which does not grant so much power to corporations! For it is the government from whence corporate power comes. Keep in mind that corporations are legal entities. They don't have common-law rights - only people do. Everything a corporation can or can't do has been proscribed by *legislation* - that is, our "pals" in Washington.

It has not always been the case that corporations were able to aggregate so much money and power, while at the same time ducking the responsibilities which individual citizens hold. For a not-too-long history of how the legal powers of corporations grew, see: http://adbusters.org/magazine/28/usa.html.

Craig

The fact many seem to forget is that the power has already been granted. How do you propose to take that power away? Let's say you succeed in weakening the government. You would have to somehow undo all of the already existing law that favors large corporations and then prevent them from using their tremendous wealth to regain an advantage. How that could be achieved without some sort of oversight is something that is quite difficult to imagine.

Dear *2600*:

I realize this is a tired issue, but I'm giving up on the term "hacker." The media uses the term to describe malicious computer wizards. Even the dictionary defines hacker as being one who breaks into computer systems. I wonder why we are holding on to such a worn out term which no longer describes what we're all about. Instead of spending half the time trying to correct misconceptions about technological activists and being mistaken for fraudulent thieves, why don't we just redefine ourselves as a new species? Create a new concept which people will associate with protecting freedom to innovate, freedom to play around with things you own, and freedom to express yourself. Most people aren't aware of these issues, maybe because they don't see anyone else involved. Those of us involved instead get associated with evil "hackers."

jesse s.

And you will continue to be. The word itself really isn't the issue. The status quo fears those who are capable of understanding things that are meant to be kept from them. You can escape the evil categorization by simply not pursuing such interests. But just changing the name won't do it.

Dear *2600*:

I was quite surprised to read that easyEverything, an Internet cafe, would believe they have a right to censor the pages viewed by their *paying* customers. I will certainly boycott them.

I am rather puzzled by your editorial comment, videlicet: "This is what happens when a big company drives all the little companies out of business with artificially low prices. You wind up playing by whatever rules they feel like setting."

Could you explain to us, when is a company "big?" Could you please explain to us, when is a price "artificially" low? Could you please mention an example of a business which wanted to have some rules, but wasn't able to because it was "too small?"

Under a Libertarian economic regime, corporations won't *abuse* power, because they will never have *accumulated* significant amounts of power.

There *are* still a very few examples of unregulated free markets. For example, commercial fishing boats. Under the current free market conditions, no boat owner can hope to fix the wholesale price of fish. Perhaps you would prefer to shut down this dangerous example of freedom.

Did you know that Eleanor Roosevelt (yes, the wife of FDR) took out, and renewed several times, a permit to carry a concealed handgun? Yes, handgun permits in New York State are on the public record!

American Citizen Living Abroad

We define a "big" company as one which is able to crush its competition because of its bigness and its ability to sell its product for much less than what it actually costs, which is our definition of "artifically low." The easyEverything by us was at one point selling

three hours of Internet time for a dollar. In addition, they had hundreds of computers connected to the net and they were right in the middle of Times Square, probably the most expensive area to have a storefront, let alone do what these people were doing. Compare this to an independently run operation which has to charge $10 an hour to recover their costs. Who do you think will go under first? If you don't like the rules that easyEverything imposes on its customers, boycotting them is a good idea. But what happens when there's no competition left because of the above tactics? You're forced to play by their rules and there's really nothing you can do about it.

We'd like to know how you plan on getting all of this existing power out of the hands of big corporations without the help of government or some kind of time machine. We suspect, not really knowing much about the subject, that there's more of a level playing field in the fishing business which keeps one entity from gaining an unfair advantage. If easyEverything had fishing boats attached to their current business practices, it would probably be a very different story. (Now we're certain to get all kinds of letters from commercial fisherman on the subject.)

And that's a nice bit of gossip about Eleanor Roosevelt but we're not sure what, if any, point you're trying to make with it.

Retail

Dear *2600:*

While reading through 16:2 and 17:1, I noticed several articles about the little photo kiosks you can now find at damn near any Walgreens, Wal-mart, K-mart, Sam's Club, etc. I don't know if anyone cares but I worked at a very high quality photo lab in a small town where we had a kiosk system for two years. Ours was made by Fuji and called the "Aladdin." This thing is nothing more than a touch screen, a high quality scanner, and a plain old PC in a fancy green box. Fuji sends these standard with a floppy, cdrom, and I'm pretty sure a zip drive (ours had one). Ours ran Win NT 5.0(?) and, get this, was connected via a network cable to an IBM server! From there we could choose from about 30 different things to do with the files from the kiosk. We could change the image format, burn it to a CD, send it to the computer in back to retouch the photos, or we could send it to the FE-1, which was the negative scanner on our digital printer, the Fuji Frontier. The really amazing thing about this whole system is that every image has to travel over plain old UTP copper network cabling. The retouching computer mentioned above was also our Internet machine! The whole system was connected to a 2Mb/sec. microwave ISP. So, if one of you out there could determine that Walgreens or one of these places had a kiosk like this, you could just bring a disk or something from home, pop it in, and maybe go exploring. By the way, to exit the main screen in a Fuji kiosk, there is a secret button in the upper right where the normal little x is. When pressed, it asks for a password. The default is 1111. I don't think they can be more than four digits.

DEESil

Dear *2600:*

I don't subscribe to your magazine due to the stupid rumor of being put on a list by the government. Well, to push my conspiracy theory, when purchasing your magazine at my local Barnes and Noble, the cashier first had trouble ringing your magazine up, then looked at me, then asked if I would like to give him an email. I asked what for and he said that the editors of the magazine are trying to find their demographics chart for better distribution. Odd....

fuzzhack

We're doing no such thing. He probably just wants to stay in touch so that the moment you shared at the register won't be forever lost.

Dear *2600:*

In 18:4, the article "Fun Facts about Wal-Mart," A.W.M. talks about portable devices called "960s" or "Telxons." He says that what they are called varies depending on who you ask. This is somewhat true. The 960 is a specific model of Telxon. There is also the 710, an older model with a very limited capacity, so I'm going to limit this more to the 960. The 960 I use is gun-like - it has a trigger to activate the scanner. The interface consists of a small screen, non-qwerty keyboard, a keypad, and other functional keys. It also has a small antenna attached to transmit data. All programs are installed remotely, transmitting from the main store computer after being selected from the 960's main menu. Programs vary from retail chain to retail chain. Only the functions that can cause serious problems are passworded. 960's can vary in style. The two I'm familiar with are the one I just described and a more box style with a side trigger. The rest of the features are the same. If there is any interest I'm certain I can dig up enough for an article.

Angela

Dear *2600:*

Recently I was in Toys R Us and was walking by their "for employees only" computer station. The inventory (I'm assuming) program was moved off to the side of the screen and I noticed the all too familiar blue "E" Internet browser on the desktop. The start button, My Computer, etc., buttons were not present, but clicking on the explorer got me access to the local drives, etc. Just for giggles I entered "www.2600.com" and was surprised to see that there was an active Internet connection. Joy. I had my wife and kid with me so I saved the "old *2600* masthead" as the desktop and closed the Explorer window. On my next visit that computer station was powered down, but the adjacent system was on. You can't minimize the inventory program, but you can drag it out of the way and play around if you like. I left a token of my esteem on that desktop as well and out of curiosity I flagged down an employee and asked if the computer that was powered down was for customer use. He said no, both were for employee use. I asked if it was broken or anything because I could repair it for a modest fee. He said he didn't know but the assistant manager might.

The assistant manager told me they had powered down the system after "a hacker broke into it and left a virus" and that they had an outsourced contract company coming to look at it. I acted astonished and told them I hoped they could straighten it all out. I suggested they should make some changes to their system

to make it harder to get into. The assistant manager in all his infinite computer knowledge assured me "if a hacker wants in, there's nothing you can really do to stop them." Wow, maybe that's an untrue stereotype we should get behind!

Moon Knight

Dear *2600:*

I just finished your Spring 2002 issue. I was shocked to read the letter "The World of Retail" on page 37. I didn't know anyone else did that sort of thing. At the B&N near me, *2600* along with *Adbusters* are relegated to the back of a shelf. At first I thought it was a mistake just like TheDude did - not so. Minutes after moving *2600* and *Adbusters* to their deserved and prominent positions, they were once again subverted, this time beneath an overhanging shelf. At this point my friend and I took it upon ourselves to make a decisive change. Having about 15 or 20 of each in our hands, we proceeded to place one magazine in front of every other magazine on the rack. It really looked nice and I've been back to the store several times to find both *Adbusters* and *2600* in the very front at eye level of their respective sections. Unfortunately this is the only place that sells either or both of the magazines in my area, but a tragedy was certainly averted.

Signal9

There's a difference between poor placement and placement specifically designed to keep us hidden. We're obviously more concerned with the latter as it's a deliberate attempt to silence our words. We appreciate your efforts but encourage readers not to disrupt operations at your local store by making a mess of their system. If you suspect foul play, get as many specifics as you can and let us know. It's made a big difference in the past.

Dear *2600:*

I was reading 18:4 and stumbled upon a letter from mAd-1 mentioning Barnes and Noble, a company I dearly hate as I once worked there and was fired from and banned from because I was rumored to have written down a list of people to kill who I worked with which is not true - I actually was writing an essay on Jeffrey Dahmer - don't ask. The letter was about *2600* not scanning in cash registers and your reply was about their new policy for publishers paying half the cost for lost items, including shoplifted items. I obtained 18:4 by shoplifting. What better way to get revenge than sneak in once in a while and steal? Childish? Very. Satisfying? Absolutely. So I feel like shit knowing I stole from you in a sense. So in turn I have included $5 (full price for inconvenience) and my word to never do it again. I'm sorry.

Neo Retrospect

You may think that shoplifting (or any crime, really) is something you can direct but it results in all kinds of innocent people being victimized. We hope you remember this in all your future experiences and commit to being honest.

Solutions

Dear *2600:*

I like to use military time format on my machine. The format I like is nnnn, so 9:45 pm should read 2145. The problem was that Windows forces a separator. If I use a space I get "21 45" which is ugly. Then I thought that what Windows asks for is "just" a character. So I used the non-printing character 0x1f in the separator field. To insert that character using your keyboard, type 031 (don't ignore the zero) while holding the ALT key. The keypad should be used to enter the numbers. You'll see that this character won't print and you can have the nnnn format with no separators.

husam

Dear *2600:*

Ads, ads, ads, a constant barrage of popups and other annoyances. One of the most favorite companies for web ads: DoubleClick. If web ads have ever annoyed you for whatever reason, then read on and let's banish them for good. For you Windows users there are products such as Atguard that can filter out ads. For you Linux users, especially at your firewall, you can block ads completely. First, find a page with the ads you want to block. I'm going to use http://www.freeopendiary.com. Let's view the source. Immediately we notice an image from ad.doubleclick.net. First to get their IP(s). Yes, advertisers are evil and use several blocks of IPs to make our job harder. Let's use nslookup. *nslookup ad.doubleclick.net* We get back an IP. But wait a few minutes, try again, and we get back a different address. The only way to effectively block all of these darn ads is to block entire IP blocks. Now check the addresses in that netblock. Say your nslookup gets you back 208.184.29.150. Try doing a *dig -x 208.184.29.130* for example. We notice both of these are doubleclick. Try random addresses through 208.184.29.x and make sure we will just block doubleclick. After you are satisfied you are only blocking what you want, it's times to use ipchains or iptables. Hopefully you're running 2.4.x and using iptables. If so, add the rule: iptables -A OUTPUT -d 208.184.29.0/24 -j REJECT. We want to only reject it instead of dropping so we don't have to wait for time outs. And the output chain is perfect because it blocks the request from even hitting the web for the ad. Hope this was helpful to any of you who are fed up with web ads.

quel

More Corporate Abuse

Dear *2600:*

I recently found this company Nissan Computers at www.nissan.com. They are currently involved in a lawsuit with Nissan Motor Company. The owner of Nissan Computers is Uzi Nissan. Nissan has been his family name for as far back as he can trace it. Go to the web site for the full story. Since you have some experience in matters like this, I was hoping you might be able to give him some advice or something. It's sad to see the American dream gone so wrong.

Peter

We're familiar with the case and we believe the Nissan family has every right to use their name in this domain. Not only did they register the site first but they've been doing business under that name since before Nissan Motors even existed! This is a good example of the intimidation tactics that large corporations

engage in and the occasional courageous people who stand up to them.

Observations

Dear *2600:*

Some while back I was sitting around with some fellow geeks passing a rainy day watching *WarGames.* Here's the funny bit. Right after David comes home and his parents are talking about his report card, listen to the newscaster in the background right after David comes in the front door. The newscaster is talking about a three alarm fire at a "prophylactic recycling center" just outside the city. Right after that story is the one about the three minute nuclear scare.

Just a little easter egg in the background of a great geek movie.

drenehtsral

Dear *2600:*

Seems like you can't turn around without running smack into another result of the damned invoking of the DMCA. After running a search on Google for "Enemy of the State backgrounds" (yes, I caught the irony), you'll find the following under the search results: "In response to a complaint we received under the Digital Millennium Copyright Act, we have removed 1 result(s) from this page. If you wish, you may read the DMCA complaint for these removed results." And the link takes you here: http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=232. Unbelievable. We must stop this.

I also think it's interesting that the link that was removed was a site denouncing Scientology, knowing the prevalence of those in the motion picture industry who are Scientologists.

William Rudek

As far as we're concerned, the nuts in Scientology deserve to be hooked up with the nuts in the MPAA. Eventually they will turn on each other.

Incidentally, the link on that page reprints the threatening letter from the Scientology lawyers which happens to list all of the offending links. Another example of how information simply cannot be stifled.

Dear *2600:*

Since the beginning of our generation the elders of our time have been screaming, "You're growing up in a computer era!" and they're right. However, children growing up in this era display a lack of knowledge about computers compared to the last generation of geeks. As I look around myself, looking at my fellow high school peers, I see a lot of arrogance and little real knowledge. I live in a town that is obsessed with art. My school has a dying half a semester of C++ that is the only advanced computer course and I recently solely participated in a programming contest representing my school, while other schools had 3-15 kids who've been prepping for this test a year now. Hell! Even the computer advanced kids spend their time doing computer animation and design.

As I listen to kids tell me how they were "able to do this" or "able to hack into that" what is really going on is a bunch of kids saying "Hey! I found a rank 'prog' combination that got me a password which I could have retrieved with little or no effort anyway, had I any skills myself!" With an outbreak of computer geniuses writing all sorts of programs to make everything and anything easy to do, there isn't much reason for a kid to go and learn anything of value. What parents see on the outside as looking amazing is just one kid mastering a program.

Now don't get me wrong, we have our fair share of gurus my age. But the guru to fake ratio is way too large. Too many kids have lost that hacker mission immortalized by The Mentor in "Conscience of a Hacker." All they want to be are bad-asses breaking into school computers with a minute amount of authority. The really good hackers at my school (now up to three or four) drop a project right when it becomes too easy.

Could hacking possibly be dying from this? What about when all you experienced hackers get knocked off? What are we left with? We're left with a bunch of kids who don't know the difference between a ping scan and a port sweep. As protection technology grows and hacking techniques stop getting better, what's the point of learning any of this stuff? Why hack when you can do something with greater reward (sometimes) like becoming an engineer?

Erovi

The very concept of hacking faces many challenges - from the people wanting to latch onto it for the coolness factor to the people trying to lock us all up and make it impossible and/or illegal to be a hacker. But we doubt either of these threats will ever be able to stop true hackers from existing. To do that, they would have to crush the human spirit and that's an awfully hard task to accomplish.

Dear *2600:*

Did you know there's a group named *2600* in Australia? They are true hackers, like ourselves. They do not call themselves hackers though. You can tell by the intro: "2600 Australia is a loose-knit group of people interested in computer security, electronic gadgetry, communications and just technology exploration in general. We have no official membership though we host a number of mailing lists and hold monthly meetings in cities around Australia. There are approximately 650 subscribers on the list at the present time. One of the other things we do is investigate and discuss details of anomalies in various things." Remind you of anything? It reminds me of when hackers were hackers and not script kiddies or lonely people who break into bank accounts but people who go forth in the search of knowledge at any cost. You can see their site at http://www.2600.org.au/.

zanar

Yes, we have seen their site and we agree with your assessment. We believe any group of such people should proudly use the term hacker regardless of what others may think.

Dear *2600:*

It seems like every issue there are several letters that speak of people who think they are hackers, but simply take up the name because it has become popular. Therefore, anyone who searched through a list of wingding symbols to make sure that *2600* wasn't

sneaking anything by them on page 33 of 19:1 is what I like to think of as a hacker.

Rabid

Dear *2600:*

I'd guess that you guys have probably had your fill of "9/11 terrorist" type mail, but maybe there is room for one more. I was sent a link about the Pentagon crash being a hoax. It looks legit to me but what do you guys think?

Super-Fly

Looking legit often isn't reason enough to believe something. You will encounter all kinds of theories and alleged facts that prove one thing or another. What's important is to always question what you're told, regardless of the source it comes from. Pointing us to a site and saying it looks like it's right is one thing but telling us why is quite another.

Dear *2600:*

Today I read in the news that it is possible to get around Sony's new anti-piracy protection scheme using a black marker and writing on the top of the CD you want to copy to your hard drive. So if this is true then according to the DMCA pens are illegal now? And the stores that sell them? Hrm....

pa

Not pens - markers. We've already disposed of ours.

Dear *2600:*

It's strange, but I think the hacking community could learn a thing or two from the Southern Baptists (gasp). Actually just one thing... we need to unite in political struggles if we're to be at all effective. After Ellen announced that she was gay, the Baptists launched an all out assault on sponsors, the network, producers, or anyone else involved with the show, and as if by magic it disappeared from the airwaves within weeks. Granted, I'm quite sure the Baptists outnumber hackers pretty handily, at least in the US. But, if they can find the will to attack something so trivial as a sitcom star being gay, I don't see why we can't (or won't) become organized on issues such as the slew of ludicrous acts and bills floating around in Washington right now, or the many slams on the hacker community being broadcast over TV daily. Let's get organized here, at least as readers of *2600,* as a political force on the issues that effect us all in the same way. By the way, is there any sort of website that is active in keeping a list of contacts, etc. to encourage the protest of things having a negative impact on the hacker community? With all the legal and political struggles you're involved in, I think it would be instrumental to maintain a site where people interested in taking action could go and find the whos, whats, whys, and hows. If not, maybe I'll start my own.

phobik

As you know, the hacker world is fairly decentralized so there isn't now and is unlikely to be one place for contact info. But there are plenty of excellent sites for the various causes that come along. If we're not one of the sites ourselves, we're committed to providing prominent links to them on our site.

Dear *2600:*

I, along with many other readers, have noticed a shift in the magazine dealing with First Amendment issues as well as a gradual, but inevitable turn toward information activism. Would you be interested in essays or editorials of a sort pertaining to these issues as full article submissions? I would like to submit more technically related articles but that is not where my talents lie. One in particular I was considering deals more with economic theory and how the separation of church and state relates to corporations and state. Though not directly related to First Amendment issues, it may provide some context as to why we have some of these issues in the world today, as well as providing possible direction on resolving them.

Methaline

While we certainly remain interested in these issues and will cover them as much as is necessary, the primary focus of our magazine must be on technology and its manipulation. By all means send in your submissions - even if we don't take it, at least you've written it and it will most likely be seen somewhere.

Dear *2600:*

I never saw this one coming. I was just watching *The Simpsons,* the episode with Mel Gibson guest starring and at one point Homer says "I'm tired of you and Hollywood hotshots like Jack Valenti." *Hah!* Is it possible that Matt Groening caught wind of the MPAA lawsuit?

xcham

Quite possible. We also noticed at the beginning of an episode of "Futurama" (a show we should all get behind to save) that the text said "Coming soon to an illegal DVD."

Dear *2600:*

Using a simple technique, anyone can hack an AIM account. The catch: They are random AIM accounts and you don't choose who you hack. It is still very rewarding. It has worked many times for me and I thought I would send you guys my little trick.

All you need to do is open AIM, go to "People", then "Find Buddy", then "By Email Address". Some people when they sign up for AIM put in an email address that is gibberish. They don't care what address they sign up with. Well, being an avid AIM user, I know that if I own an AIM user's registered email address I can get access to their AIM account. So, in that "By Email Address" field, all you do is type something like asdfhsd@hotmail.com. This might bring up a list of names. If you see a username you desire, just go to Hotmail and sign up the gibberish you used, asdfhsd@hotmail.com. Then go to AIM's lost password site and type in the username. That user's AIM password will be sent to your new Hotmail account. *Voila.* I've gotten a few neat screen names this way. It takes a while to find ones you like. I like logging on to people's accounts pretending to be that person. Wonder how many couples have broken up because of me. *Heheh.*

aimfan69

Review: Hacker Culture

by Douglas Thomas
$25.95, University of Minnesota Press,
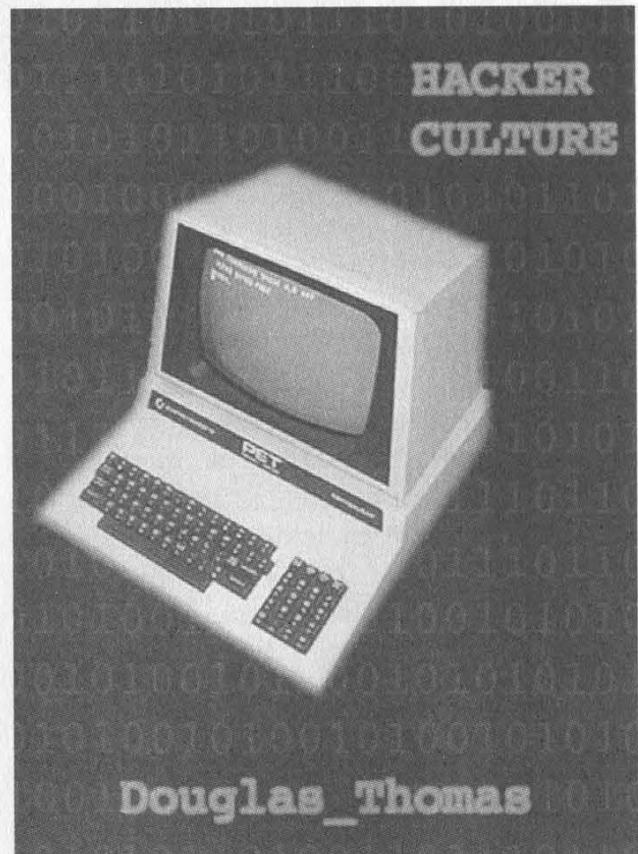**288 pages**

Review by Ben Mccorkle

In a lot of ways, Douglas Thomas' *Hacker Culture* is the book that, were I a bit older and more entrenched in the scene, I wish I had written: smart, fair, with equal and discerning attention paid to historical detail as well as cultural critique.

Thomas' study of the hacker underground does an adept job of moving beyond the often overblown rhetoric characterizing the hacker/rest-of-us divide. Rather than get mired down in the "us vs. them" debate - the paranoid claims of a monolithic system of politico-corporate oppression, or the supreme vilification of the "dark side" hacker as the prototypical cyber criminal of our financial data and even our very identities - he places these iterations within a broader cultural context.

Thomas reads the history of hacker culture as competing relationships to technology (a term he investigates and expands so that it includes far more than just computers and phones). He suggests that we are working through a complex emotional problem as a society - namely, trying to control our anxieties about technologies we don't completely understand. The hacker, then, stands as an ideal figure upon which to heap that anxiety. As the Information Age threatens to destabilize our traditional concepts of security and secrecy, public and private life, and identity, hackers are often in the vanguard position of this movement because of their dramatic and (possibly malicious) exploits, and therefore make perfect scapegoats. Popular representations of the hacker in films and in the news in turn are often the subject of ridicule by "real life" hackers because these depictions do more to propagate the cartoonish figure of technological evildoer than paint a realistic portrait of a group whose motivations are far more complex and benign.

Cultural theory aside, *Hacker Culture* offers a thorough historical overview of nearly five decades of hacker lore. Thomas hits on most of the key moments, figures, and documents of the tradition (Microsoft vs. Lopht and cDc, the MOD/LOD rivalry, the activist uprisings surrounding Kevin Mitnick and Chris Lamprecht, and "The Hacker Manifesto"), but he also extends the history backwards, into the computer labs of MIT, Cornell, and Harvard during the supercomputer projects of the 50's and 60's, reminding us that hacking has had a much longer symbiotic relationship with the very military, governmental, and academic institutions it confronts today. Though he occasionally lingers a bit too long on some moments (is it hyperbole to imply that the films *War Games* and *Hackers* had generation-defining impact?), both his narrative and interpretation of these events are ultimately engaging and compelling. In the end, we are left with an indispensable record of hacking origins, as well as an explanation of the changes in the scope, ethos, and philosophy of the hackers' world.

As a longtime scenester and a frequent correspondent to *Wired News* on the Mitnick saga, Thomas brings to this project considerable street cred, certainly. But he also offers a unique rhetorical and philosophical perspective that allows for associations between the virtual and actual body of the hacker, various state-sanctioned mechanisms of punishment, the late 20th century's almost ontological dependence upon a cult of secrecy - discourses of power, punishment, and resistance circulate throughout this history (so read up on your Nietzsche and Heidegger, folks). I, for one, would be interested in following the reaction to this book from members of the hacker community, as this reading attempts to hold a subversive counterculture up to the institutional scrutiny of academic discourse.

CBDTPA: Another Privacy Concern

by area_51

As if we didn't have enough to worry about today in terms of privacy, Big Brother now wants to have the capability to "put a cop in every computer." In the "Consumer Broadband and Digital Television Promotion Act" (S 2048 IS), Senator Hollings (D) of South Carolina has proposed a bill that would force the computer and consumer electronics industry to place a copy-protection mechanism in any device which "reproduces, displays or retrieves or accesses any kind of copyrighted work." This definition would allow for all computers, MP3 players, TV sets, cable boxes, VCRs, DVD Players, digital cameras, stereo systems, CD-Burners, and scanners, not to mention a host of other devices, to be subject to the regulation of the government. Every device would be required to have firmware or software that would prevent copies of copyrighted material from being made, or else the sale of the device would be declared illegal.

"The private sector needs a nudge. The government can provide that nudge," Senator Hollings said to the Senate during a March 21st hearing on the bill. "We will empower government enforcement so that all consumer devices comply. If they don't, the government... will have to step in."

Such developments will make new laws such as the DMCA easier and easier to enforce, and sets a dangerous precedent for the future. Besides, the government doesn't need to give the private sector a "nudge." Is the government losing money due to piracy? No. The private sector is, and it is the private sector that should negotiate among themselves and come to a reasonable solution.

I am in no way advocating piracy. But I worry that such a law will infringe upon my everyday entertainment activities and my privacy. Looking over a transcript of Mr. Holling's speech, I note he did not use the word privacy once in the entire document, and it seems to not be a concern of his. While his recommendations call for a device that would block the ability to copy or access illegally copied content, a prototype device or concept has not even been conceived. The bill could very easily be amended in the future so that the device would report back the copyright infringing activities of a particular user, and this concept could be further exploited still.

The senator states that "the legislation specifies that no copy protection technology may prevent consumers from making a personal copy for lawful use in the home of non pay-per-view television programming. I want to be clear on this point; no legislation can or should pass Congress in this area that does not seek to protect legitimate consumer copying and fair use practices." However, I am very skeptical of infringements of rights not occurring. What if I want to copy a (legally purchased) music CD, for example, to my hard drive, and then burn a different mix of songs (including some from the CD I copied) onto a new CD. How would the software or firmware enforcing the copyright laws know that my new CD isn't violating a copyright? I suppose that it could only allow me to burn the song once. But what if I want to burn the song again to a different CD, to create a different mix of songs? How would the software know that I am not giving the CD to a coworker or friend?

How about DVDs? In several years DVD burners will be available at a low cost, and these devices will inevitably have such enforcement measures packaged with them if this bill is passed (it provides a year from the date it is passed to have a final plan ready and implemented by the private sector). Let's say I have a DVD movie and I want to copy it for backup purposes (i.e., if the original were ever to become scratched beyond repair, destroyed, or lost), how will the software know that I am making a backup copy and not making a copy of a DVD I rented at my local Blockbuster and then returned, or that I am not giving the copy to a friend?

There are hundreds more scenarios that would apply to such a bill. Consider even the DeCSS case - one of the points in the case was that DVDs could not be played on Linux systems without the DeCSS code. A law such as this would enable further restrictions, causing

even greater problems with compatibility.

Then again, we as hackers would more than likely find a way to circumvent this technology for legal purposes. But the bill strictly prohibits the alteration or disabling of any copy-protective device. Soon the nation's jails will be littered with hundreds, if not thousands, of such people and this will cause additional negativity and illicit activities to be associated with hackers.

The dangers of such a technology surely outweigh the benefits for consumers. Even Rhett Dawson, the president of the Information Technology Industry Council, told *Wired Magazine*, "We don't think this will help consumers use technology to enjoy movies or other content more. If it were enacted it could stand in the way of consumers enjoying the benefits of innovation by having the government make decisions that are best left to the marketplace."

In addition, the bill will also regulate digital TV signals.

So what can be done about the bill? It is still in Congress, so I urge you to contact your congressional representative. You may leave a message for the Senate Judiciary Committee at http://judiciary.senate.gov/special/input_form.cfm?comments=1. If you go to http://www.digitalconsumer.org/cbdtpa/cbdtpa-inf.html, you will be able to send an automatic fax to Congress.

You may monitor additional progress made on the bill and its current status at http://thomas.loc.gov by entering in the bill's full name or number (both included in the opening paragraph of this document). You may also view a full copy of the bill at the site.

꬞𝓝𝓾𝓵𝓵 𝓢𝓮𝓼𝓼𝓲𝓸𝓷𝓼 and Enumeration

by AcidFlame
flameacid@hotmail.com

I wrote this article because of the large shortage of articles on null sessions and enumeration. For this tutorial I used Windows 2000, though it is possible to use null sessions and enumeration on *nix systems and Win9x.

First of all, what are null sessions? Null sessions are connections to Windows shares with no username and no password. They are usually connections to the IPC$ (Inter-Proccess Communication) share on a Windows computer. This share is hidden if you try to browse it in Windows, but usually you can see it if you type in this line in the command prompt:

net view \\TargetComputer

This will show all the shares including IPC$. Next I made a null session to the TargetComputer:

net use \\TargetComputer\IPC$ "" /user:""

If the other computer allows null sessions you would probably see "This operation completed successfully." This means that your computer made a connection to the TargetComputer.

The next part is enumeration. The IPC$ share is a share that contains a lot of data about the TargetComputer (users, lists of shares, groups, etc.). You can request all that information off of that computer if it allows you to do so (most of the time it does!).

One of the best programs for this is a program called enum.exe, which is a dos program that you can easily find on the Internet. By running enum.exe and listing a few options and the TargetComputer you can see all the users, groups, shares, etc. I'm not going to go into detail with the complete list of information you can get. I tested this program on WinNT 4, Win2000, and WinXP. It works on WinNT4 and Win2000, but WinXP blocks out most of the information. Many computers are unsecured from this (for example, I tried it on our school districts' domain server and ended up with all the names of the 5000+ users). Enumeration also helps if the username of the Administrator is changed. By running enum you can see the name of the new Administrator in the list, in this case you would see:

SpongeBob (Built-in account for the administrator)

There is also an option to turn this off which requires you to go into the system registry and insert a new key, which would enable you to disable null connections to your computer. In the folder HKEY_LOCALMACHINE\System\CurrentControlSet\Control\LSA\ create a key called RestrictAnonymous and set it to 1. This will block out null connections.

I hope this helps secure your computer or improve your knowledge.

Greetz to Guybrush, DadyShEre, Kommando, and OrangeBeast.

MarketPlace

Happenings

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

SAN FRANCISCO OPENBSD USERS GROUP - now meeting once a month at the Zephyr Cafe, 2nd Thursday - for info see http://www.sfobug.org.

For Sale

CABLE TV DESCRAMBLERS. New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

MAKE ANY SLOT MACHINE PAYOUT 200-400 credits. Works on IGT-s machines. No contact. Also available, blackjack counters. E-mail mcorballi@atlanticcity1.com if you want to discuss it further.

INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO? *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobby-broadcasting.com.

WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

LEARN LOCK PICKING It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

OVER 150 TELECOM MANUALS are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

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

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

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

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

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

LOCKSMITHS: I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

Wanted

NEED TECHNICAL ILLUSTRATOR. I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!

FEMALE HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

KIDNAPPED BY THE SECRET SERVICE, charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at:bigdarren2001@yahoo.com.

MICROCHIPS UNDER YOUR SKIN - Are you monitored - computer brain implants - parametric cavities - GPS tracking implants. You may have been implanted already by your government. For more information on humans being turned into human LoJacks and government mind control programs with U.S. Government x-rays showing unauthorized brain control implants in my skull. Please visit and support the Boycott Brazil web site by distributing this ad to free classified sites and newsgroups globally. www.brazilboycott.org

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

MISUNDERSTOOD HACKERS UNDERSTOOD. Write me. Consultations are no charge, and protected by clergy/client privilege. Trained telecom & electronics tech. billy_sunday@techie.com.

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

Announcements

PRANK PHONE CALLS. Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

HACKERMIND: Tune in Thursdays at 10 pm ET by opening location 66.28.48.80:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personals

ANOTHER HACKER IN PRISON! Don't cry for me, I did it to myself. I would like information (for educational purposes only, of course) where I can buy, how to build, etc., an RF device that I could point at a given garage door and it would scan and descramble, open sesame. I'm extremely interested in this technology. Anyone with more info or ideas, please contact me via snail mail at: Mark Carnley P-24536, F2-116 L Chuckawalla Valley State Prison, PO Box 2349, Blythe, California 92226. Will answer all.

YOUNG MAN WANTED for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.

STARTING A HAXOR SUPPORT GROUP and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, 817592, 1098 S. Highway 2037, Fort Stockton, Texas 79735. All inquiries will be answered.

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

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Autumn issue: 9/1/02.

ARGENTINA
Buenos Aires: In the bar at San Jose 05.

AUSTRALIA
Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA
Graz: Cafe Haltestelle on Jakominiplatz.

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

CANADA
Alberta
Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").
Edmonton: Edmonton City Centre, Lower Level West in the food court by the payphones.
British Columbia
Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.
New Brunswick
Moncton: Ground Zero Network, 890 Main St.
Ontario
Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.
Quebec
Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND
Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.
Exeter: at the payphones, Bedford Square. 7 pm.
Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.
Leeds: Leeds City train station by the payphones. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND
Helsinki: Media Piazza near the Modesty coffee shop (Toolonlahdenkatu 2).

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

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

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

ITALY
Milan: Piazza Loreto in front of McDonalds.

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

NEW ZEALAND
Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Murphy's Bar in Cuba Mall. 5:30 pm.

NORWAY
Oslo: Oslo Sentral Train Station. 7pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

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

SOUTH AFRICA
Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN
Gavle: Railroad station.

UNITED STATES
Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.
Arizona
Tempe: Game Works at Arizona Mills Mall.
Tucson: Barnes & Noble, 5130 E. Broadway.
Arkansas
Jonesboro: Indian Mall food court by the big windows.
California
Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Orange County (Laguna Niguel): Natale Coffee, 27020 Alicia Parkway, #F.
San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.
Colorado
Boulder: Fatty J's food court, 13th and College. 6 pm.
Connecticut
Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia
Arlington: Pentagon City Mall in the food court. 6 pm.
Florida
Ft. Lauderdale: Broward Mall in the food court by the payphones.
Gainesville: Borders Book Store cafe off I-75 and Newberry.
Orlando: Fashion Square Mall Food Court.
Georgia
Atlanta: Lenox Mall food court. 7 pm.
Hawaii
Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.
Idaho
Pocatello: College Market, 604 South 8th Street.
Illinois
Chicago: Union Station in the Great Hall near the payphones.
Indiana
Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Borders Books on the corner of Meridian and Washington.
Kansas
Kansas City (Overland Park): Oak Park Mall food court.
Louisiana
Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.
Maine
Portland: Maine Mall by the bench at the food court door.
Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.
Massachusetts
Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.
Michigan
Ann Arbor: Michigan Union (University of Michigan), Welker Room.
Grand Rapids: Rivertown Crossings Mall, second level in the food court.
Minnesota
Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.
Duluth: Barnes & Noble by Cubs. 7 pm.
Missouri
Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Barnes & Noble on Battlefield across from the mall. 5:30 pm.
Nebraska
Omaha: Oak View Mall Barnes & Noble. 7 pm.
Nevada
Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.
New Mexico
Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain &

arcade. Payphones: (505) 883-9985, 9976, 9841.
New York
Buffalo: Galleria Mall food court.
New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.
North Carolina
Charlotte: South Park Mall, upper area of food court.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
North Dakota
Fargo: Barnes and Nobles Cafe on 45th St.
Ohio
Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.
Cleveland (Bedford): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).
Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.
Dayton: At the Marions behind the Dayton Mall. 6 pm.
Oklahoma
Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.
Tulsa: Woodland Hills Mall food court.
Oregon
Portland: Coffee People Northwest, 533 NW 23rd.
Pennsylvania
Erie: The Edge, 715 French Street.
Philadelphia: 30th Street Station food court, smoking section.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.
South Carolina
Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.
South Dakota
Sioux Falls: Empire Mall, by Burger King.
Tennessee
Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Barnes & Noble, Hickory Ridge Mall.
Nashville: J-J's Market, 1912 Broadway.
Texas
Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
Houston: Cafe Nicholas in Galleria 2.
San Antonio: North Star Mall food court. 6 pm.
Utah
Salt Lake City: ZCMI Mall in the food court near Zion's Bank.
Vermont
Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.
Virginia
(see District of Columbia)
Washington
Seattle: Washington State Convention Center, first floor. 6 pm.
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 (Wauwatosa): Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

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

Spanish Payphones

Barcelona. This phone could easily be mistaken for a UFO.

Barcelona. A payphone from one of the *other* phone companies.

Barcelona. We can only guess that there was a heated argument on this phone.

Barcelona. At the train station.

Photos by h4h

Australian Payphones

Concord. One of the really old payphones with rotary dials.

Sydney. One of the new payphones found in shopping malls. Operated by TriTel.

Sydney. Typical Telstra payphones. Can you tell which scene of *The Matrix* was filmed here?

Burwood. A closer view of a Telstra (formerly Telecom Australia) phone.

Photos by Patrick Webster

Look on the other side of this page for even more photos!