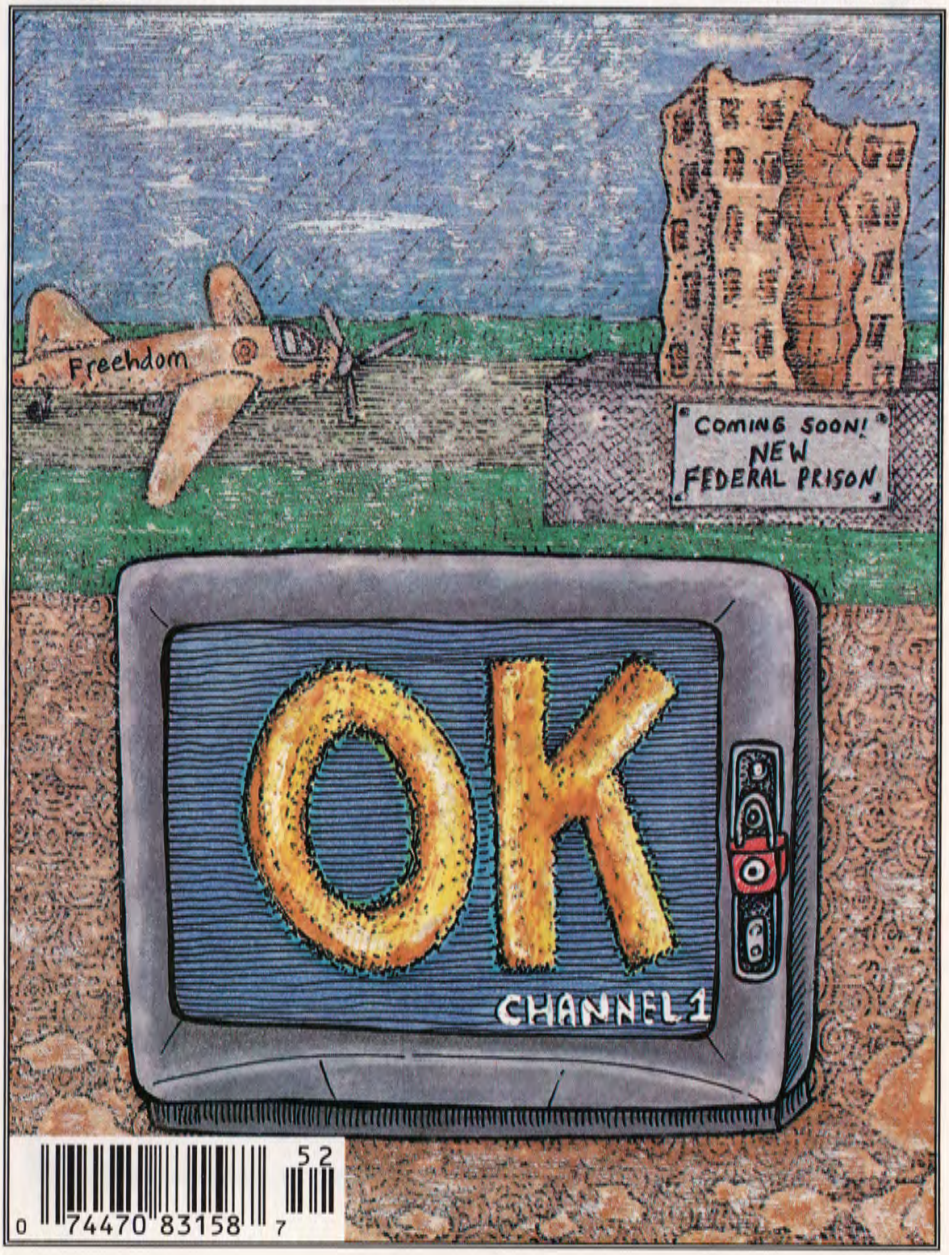
2600

The Hacker Quarterly

VOLUME TWELVE, NUMBER TWO

$4 ($5.50 in Canada)

SUMMER 1995



0 74470 83158 7 52

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Holly Kaufman Spruch

Office Manager
Tampruf

"In a dramatic confirmation of how vulnerable Defense Department computers connected to the Internet actually are, the Defense Information Systems Agency revealed that it has conducted mock attacks on more than 8,000 DOD computers over the last two years. The DISA team successfully broke into more than 88 percent of the computers. Less than 5 percent even realized they had been attacked."
- Federal Computer Week, February 6, 1995.

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Mr. Upsetter, Voyager, Dr. Williams.

Prisoners: Bernie S., Kevin Mitnick.

Network Operations: Max-q, Phiber Optik, Piotrus.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Technical Expertise: Rop Gonggrijp, Joe630.

Enforcement: Sarlo.

Shout Outs: Tom Mandel.

GUTS

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.*
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 516-751-2600,** ***2600*** **FAX Line: 516-474-2677**

the bernie s. saga

It's almost a given that the first few pages of *2600* will be devoted to the latest travesty of justice, the most recent in the long string of harassment against computer hackers. Regretfully, this issue will not be an exception. In fact, this time what we're talking about could have such profound effects on the rest of us that nothing will ever seem the same. It may sound a bit over-dramatized but we feel the facts have no trouble supporting our cynical conclusions.

Bernie S. (Ed Cummings) was involved in *2600* for most of our existence. If anyone could answer a question on scanners, surveillance, or the technical workings of a certain piece of machinery, he could. His presence at the Hackers On Planet Earth conference last year provided many informative lectures to a fascinated audience. Like most good hackers, Bernie S. believed in sharing the information he was able to obtain or figure out.

At the time of this writing, Bernie S. sits in federal prison, held without bail and without any prospect of a trial in the near future. The more we find out about this case, the more we believe that nobody really knows why he's been imprisoned.

It started outside a 7-11 in Pennsylvania when Haverford Township Police came upon what they believed was a drug deal in progress. They were wrong. What they were witnessing was a transaction involving crystals which could be used to modify Radio Shack tone dialers into red boxes. The key word here is "could" since crystals themselves can be found in a multitude of sources and their possession or sale is far from illegal. Bernie S. believed in making technology accessible to the public and providing something as basic as a crystal was one way of achieving this. However, the police did not understand this and thought they were onto some really big nefarious scheme to do something really bad. So they searched the vehicles of Bernie S. and the people he had met there. They confiscated all of the crystals as well as "suspicious" reading material such as *The Whole Spy Catalog*, a must for any serious hacker (available from Intelligence Incorporated, 2228 S. El Camino Real, San Mateo, CA 94403). They said everything would be returned if nothing illegal was found to be going on.

Then the United States Secret Service was contacted. Special Agent Thomas Varney informed the local police that there was no other use for a red box (and hence, the crystals in question) but to commit fraud. The Secret Service even went so far as to go to a payphone with the Haverford police to demonstrate how an illegal red box call is made. Based upon this, Bernie S. was forcefully arrested at gunpoint by numerous law enforcement personnel and thrown into state prison. All of his books, manuals, copies of *2600*, and anything electronic were seized. The charges were possession of a red box (a non-working Radio Shack dialer that someone had asked him to look at) and unauthorized access to a phone company computer. Apparently the thought behind the latter charge was that if Bernie S. had used a red box, he would have had to have signalled a computer with the red box tones simply by playing them. And so, unauthorized access.

The judge refused to indict him on this charge because it was so far-fetched and because there was no indication that Bernie S. had ever even used a red box, let alone a phone company computer. Ironically, the Secret Service and the Haverford Police had already done both, in their eagerness to

capture Bernie S. No doubt with all of this in mind, the judge set bail for the remaining charge of possession of a red box: $100,000.

The fact that such a bogus charge and exorbitant bail were allowed to stand shocked many. And shock turned to disbelief when a student questioning this on the Internet found himself threatened with a libel lawsuit by the Haverford Police (see page 26). This was truly turning into a spectacle of the bizarre. Bernie S., meanwhile, endured week after week of squalor and inhuman treatment in a state prison.

Then, one day, the Haverford Police announced they were dropping all charges in the case after Bernie S. spent more than a month in prison with rapists and murderers. It almost appeared as if they had realized how flimsy their case actually was and how unfair it was to penalize someone so severely who hadn't even accused of doing something fraudulent. But this was not to be. The local police had made an arrangement with the federal government that substituted the old red box charge with new federal charges accusing Bernie S. of possession of hardware and software which could be used to modify cellular phones. Was this really the best they could do? Bernie S. had openly advertised this software which had been used legitimately by many to create extensions of their cellular phones. Many hackers learned about this technology at the HOPE conference. But because this software could also be used by criminals, the government decided to charge Bernie S. as if he were one of those criminals. And for this, the government has declined to set any bail.

To give you an idea of the intellect we're dealing with, here's a quote from Special Agent Thomas Varney's affidavit:

"During my review of the items seized pursuant to the state search warrant, I determined that Cummings had in his residence the following items that could be used for the cloning of cellular telephones:

"(a) Three cellular telephone cloning computer disks.

"(b) A lap top computer that had a cloning software program on the hard drive which I confirmed by observation.

"(c) A computer cable that would allow for cloning of Motorola brand cellular telephones.

"(d) Several cellular telephones some of which had broken plastic surrounding the electrical connectors to the battery pack. The breakage of the plastic is a required step before cellular telephones can be connected to a computer for cloning.

"(e) A book titled Cellular Hacker's Bible.

"(f) Photographs depicting Cummings selling cellular telephone cloning software at an unknown event."

We congratulate Varney on being the first person to grasp the concept of photographs being used to clone cellular phones. However, until the scientific evidence is in, perhaps we'd just better strike item (f).

Items (a) and (b) are the same - (a) is a disk with a computer program and (b) is a computer with the same computer program. With a little more effort, the next item could have been a house with a computer program in it, but the Secret Service probably felt that a laptop computer would be of more use around the office. (A large number, if not most, of computer hacker cases never see owners reunited with their computer equipment.) So if we follow the logic here, it's possible that Bernie S. got himself thrown into prison without bail because he figured out how to make an extension of a cellular phone and wrote a computer program to do this. Way back before the Bell breakup, people were afraid of getting into trouble for plugging in extra phones without letting the phone company know. We

(continued on page 21)

Pioneering New Antiviral Technologies

by Adam Young

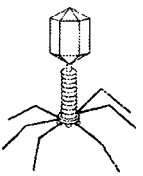
I am a hacker and a computer scientist and I have studied viruses from both perspectives since the mid 1980's. Knowing how viruses work helps to distinguish between good antiviral software and bad antiviral software. Similarly, knowing how antiviral programs works helps one to write better and more effective viruses. This article summarizes many years of my independent study on computer viruses.

This article is divided into several sections. In the first section, I correct the misinformation in an article in *2600* called "Protecting your Virus". Background information is then provided on the use of cryptographic checksums for antiviral purposes. In the third section I assume the role of an antiviral developer and explain an idea of mine that could significantly reduce the viral threat to society. The last section covers how this new method can be bypassed by certain viruses.

This will be of use to virus writers and antiviral developers alike. It contains information that can help antiviral developers make software more resistant to viral attack. It also explains how to correctly "protect your virus" and explains one possible method to bypass programs that do cryptographic checksums.

How to Really Protect Your Virus

In order to explain the new antiviral development, the concept of "polymorphic viruses" must first be explained. A polymorphic virus is a self-replicating program whose object code changes to avoid detection by antiviral scanners. This change can be made to occur once every generation of the virus or more, depending on how safe the virus needs to be. The topic of polymorphic viruses was incorrectly given in the article, "Protecting Your Virus" by Dr. Bloodmoney in *2600 Magazine,* Vol. 10, No. 3. Dr. Bloodmoney provided a "viral protection mechanism" that will, to the contrary, cause viruses with this mechanism to be easily detected by antiviral programs. The concept of polymorphic viruses has been around since at least the 1980's. The Internet Worm exhibited certain polymorphic attributes. Refer to the comp.virus newsgroup on the net for more on the subject. The following is the structure of a virus that can evade detection by antiviral scanners:



Decryption Header
Jump to Main Part of Virus
Body - MtE
Body - Main Part of Virus

Here is how it works:

1) The operating system sends control to the virus.

2) The Header executes and decrypts the entire body of the virus.

3) Control jumps over the MtE routine to the main part of the virus.

4) The main part of the virus executes and the virus replicates. The MtE (mutating engine) is executed to make the child virus have a different header than the parent. A random number is generated. The random number is XORed with each machine word in the body of the child to ensure that the encrypted body of the child is different from the encrypted body of the parent. The random number is then written to the header of the child virus.

5) Control is sent to the host program.

The Dark Avenger is credited with the term MtE. He is the infamous hacker who distributed source code for a MtE function. This source code is not very special since it is easy to write the function once the purpose of the function is understood.

The mutation routine creates modified versions of the decryption header in the viral offspring. Dijkstra once said that all that is necessary to represent program structure is sequence, iteration, and condition. As it turns out, very often portions of "sequence code" in programs can be rearranged without changing the output of the code. The mutating routine can therefore generate headers with varying instruction sequences. Many mutating routines also interleave "dummy" instructions between the useful instructions in the header. The following is a list of example dummy instructions in pseudo assembler:

```
OR      #0, reg1
ADD     #0, reg1
SUB     #0, reg1
MUL     #1, reg2
DIV     #1, reg1
NOP
```

The above instructions are based on the mathematical property that x + 0 = x, x - 0 = x, etc. Microprocessors support such instances of these instructions even though they obviously accomplish nothing. By randomly interleaving dummy instructions in the header, the header becomes harder to detect by antiviral scanners. Therefore, by using this method both the header and the body are mutated from generation to generation.

Dr. Bloodmoney's mechanism uses a header that never gets mutated. Therefore, all a scanner has to do is search for Dr. Bloodmoney's header. Polymorphic viruses are loved by virus writers because they cause the number of false positives during antiviral scans to increase.

Cryptographic Checksums

A checksum is defined as "any fixed length block functionally dependent on every bit of the message, so that different messages have different checksums with high probability"1. In the case of checksums on programs, the programs' object code is the "message". A program can detect viral infection by performing a cryptographic checksum on itself when it runs. If the checksum fails, the program concludes that it has been modified in some way, and notifies the user. A checksum will almost always indicate an infection when a virus attaches itself to a host that performs integrity checking.

Since most programmers do not even know what a cryptographic self-check is, self-checks are often not included in final products. Another reason why they are not widely used is that the software needed to perform strong checksums is not widely available. The disadvantages to self-checks are that they are not needed in programs and that they use a small amount of CPU time. The amount of CPU time used is insignificant compared to the increase in product reliability. This is why all well written commercial programs perform integrity checks.

The Need for Availability and Standardization

I have seen too many public domain programs succumb to infection by pathetic viruses, and I have seen too many programs perform weak self-checks. It is embarrassing how many viruses flourish on the IBM PC compatible platform. You want to know why there are so few Mac viruses? Everyone wants to know why. I know why. The main reason is that more Mac programs perform self-checks than

PC programs. It's that simple. In the rest of this section I will explain how all programs can be made to be more resistant to viral infection.

It may not be obvious at first, but this new antiviral development is in the best interest of society and hackers alike. Hackers are egomaniacs who pride themselves on knowing more about computers than everyone else. It therefore follows that every hacker wants to make a name for himself. How many people have written PC viruses? 1,500 or 2,000 people? If writing a virus that spreads becomes more challenging, then only the best hackers will be able to do so and only they will achieve recognition.

The need for standardization is apparent from my own research. Very few programs perform self-checks. Of those that do, very few perform strong cryptographic self-checks. Most self-checking programs simply verify their own size in bytes and verify that certain resources and overlays are present. This is not good enough. A virus could delete non-critical resources in a host, infect the host, and then buffer the end of the code with garbage so that the size of the host is the same as it was originally.

I propose that the standard libraries of all popular commercial languages should include a strong cryptographic checksum function. This would significantly reduce the viral threat to society. For example, the ANSI C standard library should contain a function called selfcheck(). The following is the prototype:

```
int selfcheck(void); /* returns true if
    checksum succeeds, false otherwise
    */
```

If this were standardized and included with all major compilers, then programmers would have easy access to a strong cryptographic self-checking routine. It is widely known that most viruses spread through the public domain. If public domain software developers had this function in their standard libraries, then it would be easy for them to call the function in their programs. Then, in time, only a small subset of viruses would be able to spread effectively. Also, these viruses would be larger and more complex since they would have to circumvent this protection mechanism. A large virus is much easier to detect than a small one.

The next question is, why hasn't this already been done? Strong cryptographic checksum technology has been around for quite a while. I think I know the answer to this question. It probably hasn't been done because it would be too easy to write a virus that disables the proposed checksum routines. For example, consider the following attack. Hacker X is writing a virus for the PC platform. He knows that the commercial C compiler called "compA", has selfcheck() in its standard library. He also knows that selfcheck() is in the library of the popular C compiler called "compB". For the sake of argument let's say these compilers were used to make roughly 90% of all public domain software for the PC platform. Hacker X then compiles the following program using each compiler:

```
#include <stdlib.h>

main()
{
selfcheck();
}
```

He then analyzes the object code of each program and chooses two search strings. Hacker X then programs his virus to search for these functions in any potential host. If the functions are found in the host, the routine selfcheck() in the host is overwritten with NOPs. The very last

instruction in selfcheck() is made to return TRUE. Therefore, whenever the infected program calls selfcheck(), TRUE is returned.

One could therefore conclude from the above argument that if programs included standardized self-checking routines, then viruses would soon include standardized selfcheck() scanners!

As it turns out, this problem can be circumvented. To see how, let me ask the following question. Is polymorphic technology only useful as a viral technology? Of course not. I propose that in addition to adding selfcheck() to the ANSI C standard library, a mutation engine should be added to all ANSI C compilers!!! The new ANSI C compiler would then work as follows. Every time a program that calls selfcheck() is compiled, the compiler completely mutates selfcheck(). This mutated version is then included in the final program. The linker insures that selfcheck() is placed at random between the functions from the source files. Adleman proved that detecting an arbitrary virus is an intractable problem. In a similar manner, one can conclude that using this method, detecting selfcheck() by a virus is an intractable problem.

If the above idea is implemented, everyone who uses standard libraries will be able to significantly increase the security of their programs by simply including the following code:

```
#include <stdlib.h>

main()
{
if (!selfcheck())
    {
    printf("You got problems pal!\n");
    exit(1);
    }
/* rest of program */
}
```

This would significantly enhance the security of all Division D ADP's (i.e. Macs and IBM PC's). See the DoD Orange Book for details.

How to Bypass Cryptographic Self-Checks

I have included this section for comparison purposes to the above section. It is important that the general public realize that cryptographic self-checks are not the be all and end all of preventative measures. The aforementioned method is to be used to supplement viral protection systems, not to replace them.

Consider a three phase virus. The virus can reside in RAM, in a program, or in the boot sector. When the virus is run in an application it tries to infect the boot sector. When the computer is booted, the virus in the boot sector infects RAM. When the virus is in RAM it tries to infect programs. Rather than having the virus patch an operating system routine so that it infects a program when it starts up, let's assume it patches a routine such that it infects applications when they terminate. Now traditionally, when the virus finishes executing in a host, it remains in the host and sends control to the host. If the host calls selfcheck(), the virus will be detected. But what if, prior to sending control to the host, the virus disinfects itself. Does this make the virus more vulnerable? Think about it.

Bibliography

1. Denning, Dorothy E., "Cryptography and Data Security," Addison-Wesley Publishing Co., 1982, p. 147.

2. Adleman, Leonard M., "An Abstract Theory of Computer Viruses", Lecture Notes in Computer Science, Vol. 403, Advances in Computing-Crypto '88, S. Goldwasser(ed.), Springer-Verlag, 1990.

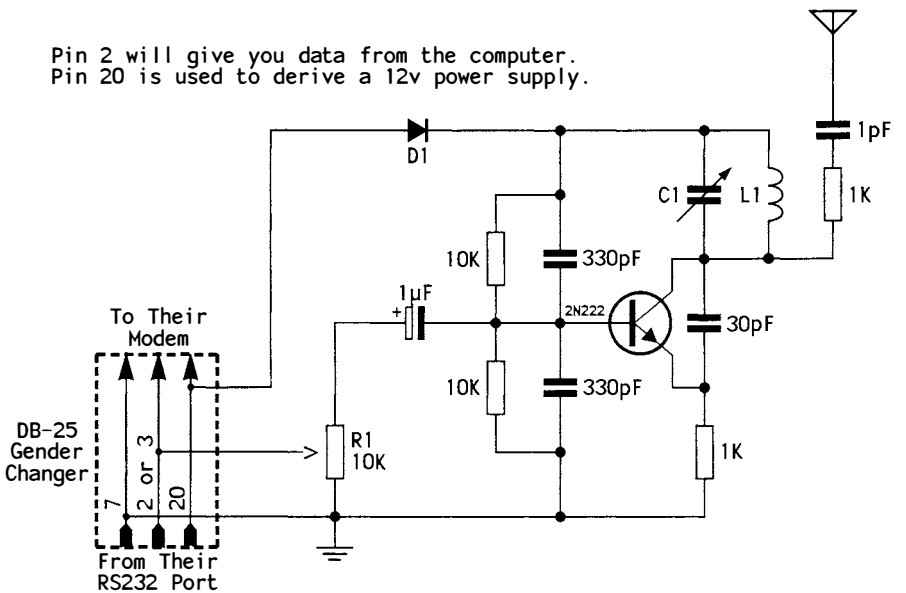
The GenderSnooper

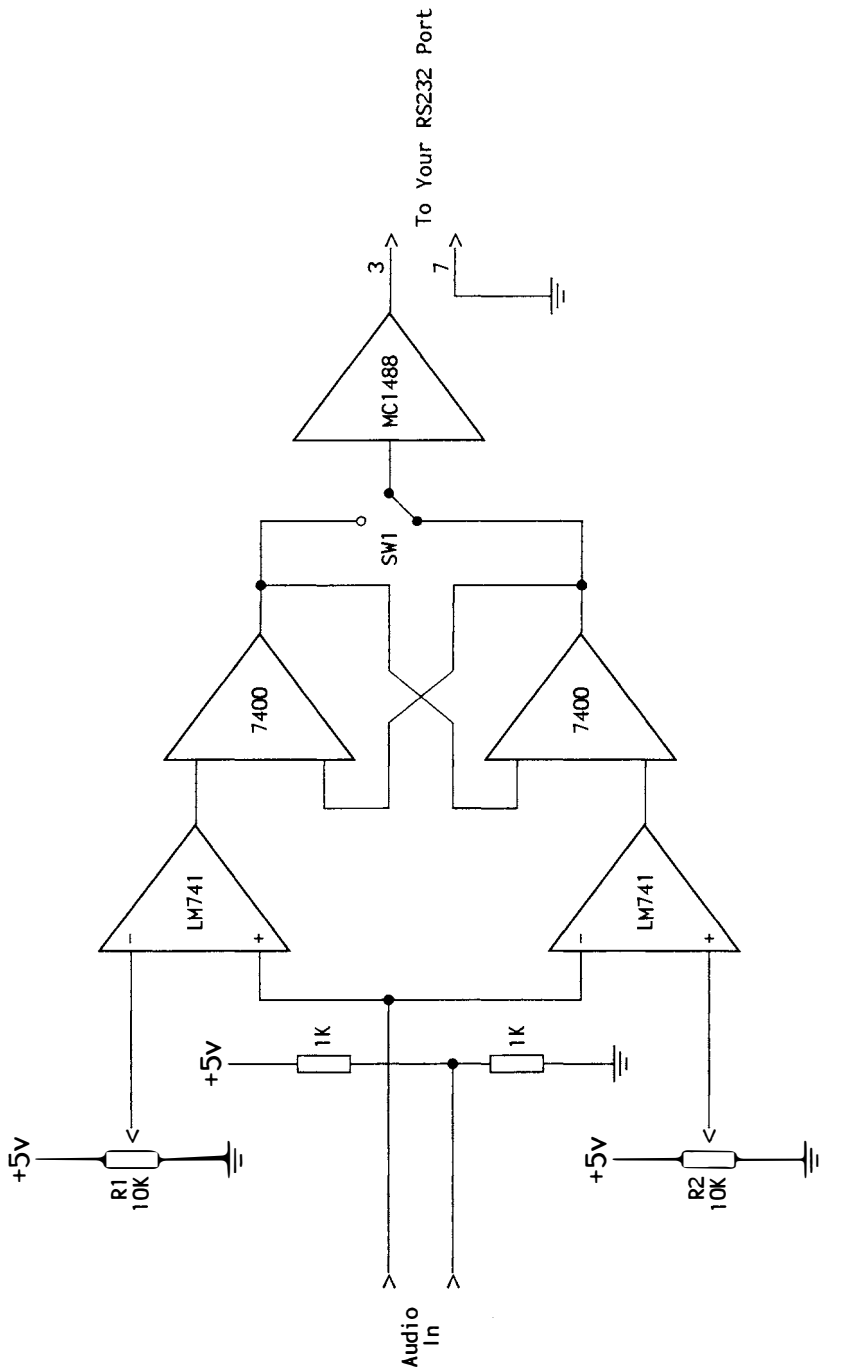
by Commander Crash

So you have this problem that seems simple enough to solve... you want to get the numbers your school uses to upload their grades to the main computer. You figure it would be an easy task to hack their PC's by installing a key capture TSR... but wait! They use some screwball proprietary computer you haven't got the time nor the patience to figure out. Or maybe getting to the PC is so hard to get to, you don't want to bother going back to it a second time. What now? Give up? No way! They use an external modem that uses an RS232 data link. What if it were possible to monitor all data the computer sends down its RS232 cables? Perhaps by slipping something inline with the cable, you could retrieve those much needed passwords and dialup numbers. Never heard of such a device you say? Well, the wait is over. The GenderSnooper does just that, and looks exactly like a gender changer.

The schematic shown below is for the transmitter. The one I built was housed inside a gutted gender changer. C1 and L1 create the tank circuit which sets the frequency transmitted on. These values are chosen based upon the typical equation for a tank circuit found in most any electronics theory books on RF. The transmitting range depends highly on the frequency chosen, and the length of antenna wire used, as well as the orientation of the antenna. For best results, use the FM broadcast band. Most FM radios have a very wide bandwidth and can support reliable reception of baud rates up to 19.2k. Most scanners, however, only have a bandwidth of 15 khz or so. This results in crappy reception at higher speeds, but it still works. R1 should be adjusted while you listen to the received signal from either an FM radio or your scanner.

The figure on the right depicts the receiver circuitry. LM741 op amps and the 7400 TTL chip, as well as the MC1488 chip




To Your RS232 Port
3
7
MC1488
SW1
7400
7400
LM741
LM741
1K
1K
+5v
+5v
+5v
R1
10K
R2
10K
Audio
In

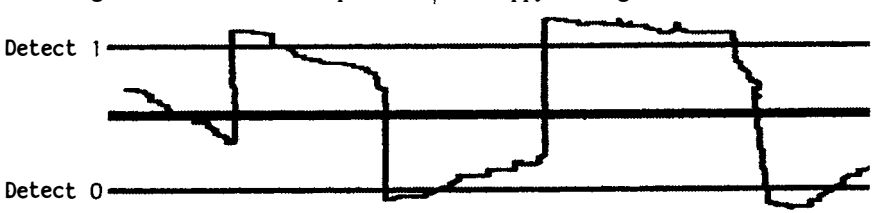
are all available presently at your local Radio Hack store. Calibration is *very* critical. In order to calibrate the receiver, you must first locate two PC's within a few feet from each other. Place the GenderSnooper on the port of one, and load up your favorite terminal proggie. Start some large upload of a 50 meg text file at 300 bps. Now go over to your FM radio or scanner (whatever you are using to receive with) and find the signal. It should sound like alternating, low frequency tones. Once you are sure you've got the signal tuned in, it's time to hook up the receiver and calibrate it. Load up a terminal proggie on the other PC, and plug in the receiver into the serial port and scanner.

Calibration of the transmitter is easy. Adjust R1 until you can't hear the signal in your receiver. Now, *slowly* turn it until you hear it. Don't go too high! Too high of a setting will distort the signal. Now here's the fun part. Calibration of the transmitter is very difficult, so you need to have lots of patience. Get your multimeter out, and adjust both pots in the receiver until they are both delivering exactly half of the supply voltage into the op-amps. Adjust R1 and R2 so the voltage is slightly above 0. What are you getting on your screen? If it is still garbage, raise R1 and R2 again. Keep doing this until the signal looks clear. If you can't get a good signal, then try re-adjusting R1 on the transmitter, or try flipping switch SW1 to the other position to invert the signal. With a little patience, you'll soon get it. Essentially, all you are doing is moving the "detection" levels for 1 and 0. See the figure below. You should repeat this calibration process at higher and higher baud rates until it works at the highest one you expect to use. After you have accomplished that, then you should begin moving the transmitter and receiver farther apart. I achieved a maximum reliable range of about 550 feet using the FM broadcast band at 19.2k bps.

So how does it work? It's quite simple. The transmitter simply sends out pulses of RF with every bit transition of the target computer's port. The receiver picks up these pulses in the audio signal. For a "1", the signal pulses positive, then slowly drifts down. For a "0", the signal pulses negative. Between these pulses, however, there is nothing but noise in the signal. The receiver simply outputs the same logic signal (1 for a positive pulse, 0 for a negative) between each pulse.

As you might have guessed, this device has many applications. It has been greatly helpful in getting into the local library's computers, the DMV, and a few others. Of course, I had their permission to test the device, and it was for educational purposes only! If you don't already own a portable PC, get one. It doesn't matter if it's a laptop, notebook, or palmtop. Just make sure you can get it around the target without being suspicious. I purchased an HP2000LX palmtop. It has a built-in serial port, is no larger than a checkbook, and comes with built-in communications software. I used this in combination with a walkman inside my coat, and just stood around the target in most cases with my capture file open. Worked like a dream!

Happy hacking!



ATM TRICKS

by Helen Gone

During college I alternated semesters as an electrical engineering co-op student. This was for the pursuit of bucks to stay in school and some experience. One co-op semester, I met a group of about ten computer science students who were pretty much forced to work 50/60 hours a week "testing". "Testing" was looking for errors in 3rd party PC software. "Testing" was extremely dull/boring/tedious/monotonous/etc. and it made for a lot of unhappy co-ops who wished they had other co-op jobs. This testing was comprised entirely of doing repetitive keystrokes with the odd batch file now and again. Repetitive keystrokes simply meant they took each menu tree out to its very end, filled out some paperwork, then started at the next branch, and worked it out to the end and so on. One guy had been working on Lotus 123 for his whole co-op. He was the unhappiest of all.

Anyway, this technique seemed relevant to my ATM interests and I soon started some "testing" of my own. With as many times as I hit the ole money machine, it was pretty easy to work the menus over pretty well for anything that seemed soft. The task led me to begin noticing the obvious differences between the manufacturers of ATMs, then slowly, the subtle differences between different hardware and software revs. I've never documented any of this. I simply started remembering the differences, especially the differences in the similar machines that were owned/leased by different banks.

Number 1

One rev of Diebold machines began to stand out as the one with the most problems. Its most notable feature and flaw is its cash delivery door. You all have used it. It's the one where the door stays locked until your cash is delivered (and while delivering, it makes that heartwarming chug-chug-chug "oh I got bucks" sound) at which time it starts beeping, saying: "Please lift door and remove cash" and then makes that wonderful "bang!" sound when you crash the door to the top to see your well-earned money laying in a stack inside this clear anodized box. This machine became my central interest because of the door. The designers all (mechanical/electrical/software) made a bad assumption concerning the door. I put the three designing disciplines in that order because that is typically the order the BS slides. Good software can usually save the screw-ups the others make - usually. The other feature/problem, which I found during my "testing", was the use of (I'll guess) a watchdog timer to recover from software bombs. If the software did not tickle the watchdog in some allotted time, a hardware reset would occur. The reset typically resulted in the loss of your card. These Diebolds seemed particularly sensitive to the hitting of Cancel during different operations. Some revs would say thank you and spit your card back, while other revs would begin not tickling the watchdog, and of course - reset. I soon learned that trips to different branches of my bank for extra/replacement cards became necessary. My bank was cool in the fact that they could make cards in-house, and I did not have to wait a couple of weeks for the card to come back in the mail, either usable or cut up with an ever-so-sweet letter explaining who I should call should I not understand how to use my ATM card. Also sweet-talking the people at the bank where the card was "captured" the next day sometimes got the card back.

Going back to the main feature/flaw, the designers made the assumption (**Assumption #1**) that if a cherry switch, located somewhere inside the door mechanism, had made closure then this meant the user, the ATMee, had removed the bucks. We'll guess some pseudo-code might look like (just because I've always wanted some code in *2600*):

```
UnloadBucks(MaxBuck$)
DoorWithFlawIs(UnLocked)
Print "PLEASE OPEN DOOR AND
   REMOVE CASH"
While We'reWaiting
   EverySoOftenTickle(The WatchDog)
   TellBeeperTo(BEEP)
   If DoorSwitch == CLOSED then
      MaxBuck$ = Removed
      We'veNotWaiting
   endif
EndWhile
etc.
```

And, ta-da! The flaw is simply that the door could be open and cash removed without the switch ever having made closure. The switch can be heard to click (this varies of course) around the first 1/3 motion of the door. A small hand or a popsicle stick works just fine with an added bonus if the myth holds true that the camera takes your photo once the door is opened. See Assumption #1. For completion several more things must next occur. The first is waiting. With cash in hand and switch never closed, the machine will just loop, beeping and asking you to remove your already removed cash. The second is the Cancel. Most revs spit your card back at you and correctly assume that you magically removed the money. The target rev did not behave this way. At t >= 30 seconds and Cancel key hit, the poles shift over to that imaginary side of the plane and the machine resets. Money in hand, card in machine, but hopefully another card in pocket! The final chapter shows up in your monthly statement (see below).

Assumption #2. If the machine bombs during a transaction even past the point of delivering money, a transaction error assigns you the cash back. This weekend, the kegger's on me, huh! I've been out of college seven years now and can say that these machines are today quite few and far between due mostly due to the door/switch flaw. The replacement machines have any number of configurations, most with no doors at all or a totally different door approach. I'm pretty sure the laws concerning tampering with ATM's have also been replaced as well.

Number 2

This one I just saw the other day is pretty much the impetus for writing this whole article. It's not so much of a hack other than observing the plain stupidity of a company providing customers with an ATM-like service. This nameless company provides a card reader/keypad/terminal/printer inside their establishment. At the terminal you swipe your card (no card cap-

DATE	AMOUNT	DESCRIPTION
7/11	-350.00	WITHDRAW 7/11 LOC-D 1972/2002
		1000 MAIN STREET
		ANYWHERE USA BIGBANK
7/11	+350.00	DEPOSIT 7/11 LOC-D 1972/2002
		NET RES ERROR 3R3-01312000342-809
		TRANS AT LOC-D BIGBANK

ture here!), enter your PIN, and then the amount you want. The printer promptly shells out a receipt and informs you to take it to the counter for the bucks. After you sign it, the salesperson then takes the receipt and gives you the amount indicated. Simple, with the single point cash idea, and life is just way easier with this low maintenance machine. My transaction had one slight hangup which was pure coincidence. The printer became somewhat jammed and my receipt had no place for me to sign. The receipts are quite similar to those of any credit cards where there is a white copy on top and a yellow one for the customer underneath. At seeing the problem, the salesperson comes over and first opens the bottom up and fixes the jammed printer. A key is needed here. Next, enter the shaky world of high tech computer terminal security: a five digit code is entered into the terminal. No magic key card swipe then code combination, just a plain old five digit shoulder surfable code. Five digits, press Enter and the terminal displays "Authorized Reprint - Press Enter for Reprint". Here comes my new receipt and the machine is back in swipe-a-card mode. Looking over my new authorized reprint I do find one small clue to indicate this is not the original. Easily missed, it says "Reprinted" midway down amongst a slew of other bank babble. Sign it, get the cash, and go. Now [nameless] is a large nationwide chain with many locations even within the city - what are the odds that the same code will work at another location? Sure enough. Walk in, five digits, press enter then enter again, tear off the print out, sign it with some mess, take it to the counter and do the ole "Boy, that Brad Pitt sure is a cutey, huh!" distracter, and - tada! - you just got handed the same amount of money the last person got. Since it was a non-network function, [nameless] is the loser, the reprinted account never knows the difference. As for how do you get the chance to shoulder surf the code? Refeed the copy on to itself? Spill coffee on it? You see it over and over how rules that apply to the user do not for the administrator. The user is required to have a card and code while the administrator needs just a code. The administrator usually means many (salespeople, managers, etc.) and the policy to direct many appears to weigh much heavier than any fear we install.

Special thanx to FlyCac Technologies and iBruiseEasily for some thoughts and memories.

citibank atm fun

by Ice of Spides

Apparently at least one CitiBank ATM at each branch has special access. It's my guess the access is for some sort of system-wide maintenance, but it might be special account access for employees or others. Or perhaps it's simply regular ATM access without the fancy graphical front end.

To find if a machine has this feature, ignore the instructions to dip your card. Instead tap your finger twice in the top third of the display. (Citibank machines have touch-sensitive screens, and they display software buttons.) This is the only part you can perform without an ATM card. If you hear a beep with each tap, you're golden.

The ATM will now show a "DIP" instruction. What graphics there are from this point on are crude, apparently because the public was never intended to see them.

The only way to proceed now is to dip your ATM card, so be warned that your identity, and everything you do, can be known to CitiBank. This alone provides the bank with some protection against any serious hacking. Don't say I didn't warn you.

After the ATM detects the dip, the screen will display a set of four choices. In the center is a text-entry box, one character high, and perhaps twe!ve or fifteen characters long. Each tap in this box enters an asterisk. Surrounding this text-entry box are four buttons, each with a different shape, labelled Enter, Go, Exit, and #. Don't be fooled by the absence of a keypad; this is primitive stuff here. The # button is where you type in your secret PIN. Tap once for each number and tap the Enter button to enter that number. For instance, if your secret PIN is 6543, tap the # six times, then the Enter, then the # five times, and then Enter, etc. Each press of Enter adds an asterisk to the text entry box. After your PIN has been entered this way, press the Go key.

If you typed inaccurately or pressed buttons in the wrong order, a clock face and Wait message appear, and then a Pacman's Death sound signals failure as "Sorry!" is displayed. You're popped back onto the first public screen.

But if all went well, a new screen now appears, with Exit and Go buttons at the top, and Cash and Deposit buttons at the bottom. (The Deposit option will only appear if you use a Citibank ATM card.) You can withdraw money from your account using the same crude method of counting. A double-sized receipt prints at the conclusion of your transaction, which raises the possibility of this being an undocumented service for sight-impaired people. At the conclusion of a successful transaction, victory music plays - guaranteed to get you stares from fellow bankers.

Note: when put into this special mode (two taps on the upper right hand side of the screen), the ATM will remain there for at least a few minutes. Some branches have this "feature" in all of their machines making it very easy to cause massive confusion for anyone attempting to use them.

AT&T

520 Broad Hollow Road
Melville, NY 11747
516 420-3000

March 16, 1995

[redacted]

Dear Mr. [redacted]

DID YOU KNOW? If a hacker successfully penetrates your telephone system's security, you could be billed for OVER $10,000 PER HOUR for FRAUDULENT CALLS? Is it any wonder that PHONE FRAUD is such a HOT topic with business?

You need to know how VULNERABLE you may be to fraud, and what you can do to protect your business from being victimized by telephone hackers! Even if you have safeguards in place, an "it can't happen to me" attitude just isn't realistic. You need to know how to make your business phone system as "hacker proof" as possible, and formulate a disaster plan that will provide an immediate response if your system is compromised.

AT&T offers educational seminars to give you tips on how to avoid fraud. We explain where and how hackers and frauders operate, common scams they use, and how to keep your business clients, and new capabilities we are developing. In an interactive forum, we talk about YOUR concerns and answer YOUR questions.

We would like to invite you to a seminar at 520 Broad Hollow Road, Melville, New York on Thursday, April 13, 1995 from 8:30 to 11:00 A.M. We have invited Robert Palmer from AT&T Corporate Security to discuss telephone fraud with you and answer your questions. Please call (516) 420-3039 by April 7, 1995 to confirm your reservation. Thanks for your prompt reply. We look forward to seeing you at the meeting, and are sure you will find it was time well spent.

Sincerely yours,

Damaris Fernandez
Account Executive

This is the quintessential "lean on customer" letter from AT&T that is intended to put the fear of God into them so that they'll comply. After all, it would be a shame if something were to happen to this nice business of theirs, wouldn't it? For a monthly fee, AT&T will offer protection. Of course, AT&T will benefit either way since they'll still bill the customer for fraudulent calls. And, since the customer probably got their phone system from another company, AT&T won't be interested in any excuses....

DAY OF THE HACKER

by Mr. Galaxy

I run a BBS in Atlanta, GA. This is a true story of how my BBS was hacked, and how I came to appreciate it.

Several years ago I started a bulletin board in Atlanta, GA. I tried several "test" versions of the available popular bulletin board systems of that time and ended up choosing to run a Wildcat BBS. The software installed quickly, and as the manual said, I was up and running within the hour.

Wow! I was excited! What a neat hobby! Over the months, the BBS grew and grew. First, I added one hard drive and then two. Later, I added one CD ROM, then another, then another, and even another. Wow! This was neat stuff. People began calling from around the world. I started "meeting" new and exciting people. At the time, I was very security conscious. Each person had 30 days to try the BBS, and then if they didn't subscribe, they would get downgraded to a very low access level. People joined and joined, and all was right with the world.

Then I started having weirdos call. Some would log on without filling out the short questionnaire. Others would fill the questionnaire with false information. I started getting pissed off. I then decided to buy a caller ID box. These boxes had just come out, and I was determined to stop these guys. Each night I would carefully compare my activity log against my 40 memory caller ID box. Those entering false information were locked out. A log book was kept of the evil-doers. Bam! I'd locked one out. Smack! I'd then lock another out.

Wow, this was fun! What a great time I was having. I was a super SYSOP. I had the power! Don't mess with me! I was getting some folks pissed off. Fake logins increased. Threats increased. I countered with the phone company's phone block feature. *Ha!* Don't mess with me... I'm a super SYSOP!

The BBS continued to grow.... I now had a massive system. I was keeping out the evil enemies... and winning! My doomsday was about to begin, yet I wasn't afraid because my software user manual told me that *no one* had ever hacked a correctly set up Wildcat BBS.

I was so proud of myself. I had written my own BBS upload virus-scanning program. I used a massive batch file to scan upload files with two virus scanners and an ANSI bomb detector. *Ha!* Let them try something! They can't beat me!

Well, they tried and tried to beat my super system.... Every time they tried, they failed. Again and again they tried. Again and again they failed! *Ha!* I was a super SYSOP. Don't mess with me! I grew more confident.... I was invincible! Let them attack! I had the super computer, the super intellect.... They were nothing more than insects to me! The laughter in my mind grew in its intensity....

Doomsday Strikes

One night I arrived home later than normal. Boy, I was tired. What a long day.... As I was about to fall into bed, I decided to check my email on the BBS. I turned on my monitor and saw a message which stated I had an "Environment error...." At the time I was using DR DOS 6. I grabbed my DR DOS manual and tried to find out what this meant. After not being able to find any meaningful information about this error, I decided to reboot my computer. After all, I was used to the machine freezing.... I had so many TSR's loading in for my four CD ROMs that freezing was common. I often had to reboot my computer to restart my system after someone had attempted to download from one of my CD ROMs. I wouldn't say this freezing problem happened every night; in fact, it really only happened once or twice a month, but I was never surprised when it happened. When I came home and saw this error message, I just assumed this was one of my usual "freeze-ups".

I rebooted the computer. The machine whirred and clicked as it started up. As it booted, I noticed that when the computer executed the MSCDEX.EXE program in the AUTOEXEC.BAT file, the file appeared to load, but the indicator lights on the CD ROMs didn't blink in sequence like they used to do. Damn! I asked myself what was happening. I couldn't figure it out! On a whim, I grabbed my anti-virus scanning program and scanned my computer. Bells started to sound. Oh crap! I had the Screaming Fist II virus! How had it gotten there? I began to swear in several languages.

My computer rebooted itself. Damn! This time the machine refused to completely boot up. A cursor sat there in the top right hand corner of my screen, doing nothing! I reset the machine again! Nothing! I was worried. The hard drives in my machine were compressed using SUPERSTOR. In order to boot up my machine from a clean floppy, I not only had to find a clean DR DOS boot-up disk, but I also had to find the correct compression files to run in my new CONFIG.SYS file. After 40 minutes of failed attempts, I was finally able to boot my system. I ran my virus cleaning program, and then rebooted my machine from the hard drive. My machine was running! Yea!

I had won! I was a *god!* Don't mess with me; I'm a super SYSOP! Then, midnight struck. My machine bleeped and reset itself. *Huh!?* What had happened?! My CMOS was erased, gone! My computer now no longer knew what types of hard drives I had or what type of floppies I had. The list went on and on. Oh man, I was furious! I vowed to search the Earth forever for this evil hacker of destruction.

I labored on into the night. Due to the nature of my job, I was experienced with computers, and I was able to recover within a couple of hours. I finally restored my CMOS, cleaned the infected files, rescanned my system with other virus scanners, and got my system working. It was now 4 am... I was exhausted. With a smirk of satisfaction I went to sleep... *after* I had disabled the uploading function.

The next day I scoured the activity log. Ah ha! The guy had called at 2 am the previous morning, and I simply had not noticed the problem until late at night later that day. Unfortunately, when the BBS went down, people had called again and again attempting to get on the board. The caller ID had lost the call! So many people had called that I had lost perhaps the most important clue as to my caller's identity. Damn!

At this point I decided to determine what the hacker had done to zap me. As I can best determine from the activity logs, the caller had performed a multi-file batch upload. He had uploaded a file called PKUNZIP.BAT and another file, COMMAND.COM. I began to understand what this guy had done. I was impressed. This guy knew how Wildcat BBS's work!

When a file is uploaded to a Wildcat BBS, the file is often uploaded into a directory called C:\WILDCAT\WCWORK\NODE1. In the Wildcat manual, the SYSOP is given some sample lines of a file called SCANFILE.BAT. SCANFILE.BAT is the batch file that the SYSOP creates to scan files that are uploaded. I had used the sample lines from the manual as a template to create my super SCANFILE.BAT batch program. My attacker had batch uploaded a file called PKUNZIP.BAT and an additional infected COMMAND.COM file. When my SCANFILE.BAT file tried to unzip the files in my C:\WILDCAT\WCWORK\NODE1 directory, the PKUNZIP.BAT file was run rather than my legitimate PKUNZIP.EXE file! The PKUNZIP.BAT file ran the infected COMMAND.COM file, which in turn turned the Screaming Fist II virus loose upon my system before the SCANFILE.BAT batch file ever got to a point where it could scan the uploaded files! What the attacker didn't know and couldn't have known was that I was using DR DOS, not MS-DOS. When the infected COMMAND.COM file was run, the virus loaded itself into memory, but DR DOS didn't appear to like the non DR DOS COMMAND.COM program. I believe at this point DR DOS essentially "puked" giving the now infamous environmental error.... It was this error or conflict with DR DOS that actually kept many of my files from being infected. In all, only about 25 files ever became infected. Unfortunately, the files that did become infected governed the drives' compression routines. The great "problem" was restoring these files. I didn't have a ready backup, I didn't have my files where I could easily find them, and I couldn't find my operating system files. The super SYSOP wasn't so super after all.

After several days of analysis of what had happened, I rewrote my SCANFILE.BAT file, turned my upload feature back on, and began the BBS again. I was now very respectful of what this guy had done. In fact, as the weeks passed, I came to appreciate the intellect and cunning of this hacker. I hope that one day I can have a conversation with this special person. If this special person is out there and can figure out who I am, I hope he will call me. I'd love to meet him....

Since the time of my "hacking" I have come to respect my fellows in cyberspace to a much greater degree. I now feel that I am a part of this wonderful infinite world. Have I, the hacked, become a hacker? I suppose it depends on your definition....

D I V E R T E R S

by Ray Nonte

A call diverter is a piece of hardware attached to a phone line that will forward an incoming call to another phone number. This type of call forwarding system is done externally, separate from the phone company services.

So how can a phreaker take advantage of this situation? When you call a diverter, you will either hear a "click" and then ringing, or a ring and then a "click" followed by ringing. The "click" is the sound of the diverter being activated. Your call is forwarded onto the line being paid for by the business that owns the diverter. The trick is to seize that line and dial out from it.

Capturing the line used by a local diverter will provide a clean connection since you are dialing off of its dial tone as if it were your own. This means that you can dial any phone number you wish as long as the person/company with the diverter hasn't blocked access to any exchanges.

If you happen to call a number that traces, the trace will show the number of the diverter, not the phone you are calling from. In this respect, diverters are usually safer than long distance extenders, but there are no guarantees. The advantages to this kind of setup make it ideal for phreaking incognito:

Trace-free calls (can only be traced back to the diverter, not you!)
Free long distance calls
Free 900 calls

How To Use A Diverter

Call the number of a known diverter. Your call will be diverted to the forwarding number. When the party at the other end answers, politely state that you dialed the wrong number and wait for them to hang up the phone. Do not hang up your phone. Stay on the line and wait for the dial tone. (Some telco central offices are programmed not to drop to a dial tone after an outgoing call to prevent just this sort of thing.) The dial tone you hear will be of the diverter. You have now successfully seized the diverter's phone line and can freely dial out on it. All calls will be billed to the diverter. Also, if an attempt is made to trace your call, the trace will point to the diverter and not you.

Diverters are not perfect - they have their share of problems too. Some diverters will disconnect the forwarding line after a certain amount of connection time has passed, 10 to 15 minutes is typical. This is a watchdog feature used to guard against phreaking attacks. Other diverters will click when used, every minute or so.

Where To Find Diverters

Diverters are usually found on the phone lines of many doctors, plumbers, etc. - any person/business that requires round-the-clock accessibility. Use your local yellow pages to locate a business that advertises 24-hour service. Dial the phone number and listen carefully. As mentioned earlier, you will either hear a "click" and then ringing, or a ring, then a "click" followed by ringing. When the party answers the phone, get them to hang up (e.g., wrong number tactic). Wait for the dial tone and then you're in business!

I recommend that you verify that you have seized the diverter's line by dialing an ANI or ANAC number. If it reads back the number of the phone you are calling on, then you are not on a diverter. If it reads back a different number, you have successfully located a diverter. Write down the number and keep it in a safe place.

One of the most famous diverters of the past involved the phone company itself. In fact, this method may still work in some parts. The caller would dial the credit operator and ask for the AT&T credit operator. When the operator answered, the caller would ask for the AT&T credit operator. The local credit operator would put on a recording telling the caller what number to dial. After the recording disconnected, the caller would get a dial tone belonging to their local credit office!

Conclusion

Call diverters are a wonderful tool for you to add to your phreaking arsenal. Be careful though. After you've located a diverter, don't abuse it or the business is sure to pull the plug leaving you to start all over again. I've found it best to build a list of known diverters and then cycle through them as I need them. The business is less likely to notice one or two long distance calls per month vs. a whole bunch of them!

(continued from page 5)

realize now how absurd such thinking was. Yet we're reliving history, only this time the penalties are much more severe.

Item (c) is a cable. Let's just leave it at that.

Item (d) consists of cellular telephones, none of which were illegitimately obtained or used for fraudulent purposes. If any of our readers are interested in how a cellular phone works, we encourage them to take it apart and experiment with it. Any evidence that Bernie S. was doing any more than this has yet to surface.

Finally, the *Cellular Hacker's Bible* is a book anyone interested in electronics and the phone system would want to read. The federal government has managed to outlaw radio frequencies but they have yet to outlaw books. With agencies like the Secret Service doing their dirty work, it's only a matter of time.

So what do we have here? Apart from an inept, backwoods police department specializing in intimidation tactics and a federal agency bent on keeping a vice grip on technology, not a whole hell of a lot. Nothing listed above constitutes a crime, at least not in a democratic society. In a suspicious and fearful regime, however... books, ideas, technical ability - these could all be considered threats. And by permitting this to go unanswered, either through encouragement or through silence, we move steadily down that dark road.

This whole series of events and their consequences is a disgrace to our judicial system and it's essential that we fight back. Every organization which claims to have an interest in justice should know about this. Hopefully, the majority will take a strong stand against what has happened here. The alternative is practically unthinkable - imagine a world where reading, experimentation, and software are the only ingredients needed to put a person in prison indefinitely. There would be very few people looking at these words who would be safe.

There are two ways you can write to Bernie S. in prison. One is by sending him mail directly at: Ed Cummings 48919-066, FCI Fairton, A-Left, P.O. Box 280, Fairton, NJ 08320. You can also send email to bernies@2600.com and we will forward it to him. (This method is preferable in case he gets moved to another prison after press time.) Remember that all of your mail will be read by prison authorities. We encourage you to write whenever you can since no visitors are allowed and this is his only contact with the outside world.

NEW ADDRESSES

To make your life easier, we now have dedicated Internet addresses for various things:

info@2600.com - to get info on 2600.
index@2600.com - to get a copy of our index.
meetings@2600.com - for info on starting your own meeting.
subs@2600.com - for subscription problems.
letters@2600.com - to send us a letter.
articles@2600.com - to send us an article.
2600@2600.com - to send us a general message.

(You can reach most of our writers on 2600.com. You may have to figure out their usernames, however, since we don't publicize individual users unless requested by them.)

HACKING AS/400

by Mantis King

The AS/400 is widely used in Argentina (South America). I do not know if they are used very much in the USA, but I hope this information will be useful to many 2600 readers all over the world.

OS/400 Release 1

This information is applicable to all the releases of the OS/400 operating systems. If there are changes, they are explained in each release's detailed description below.

AS/400 has a PC interface called PC Support. There is other third party software supporting the interface. The PC Support software allows file transfer, emulating a work station, print serving, file serving, messaging, and other user support.

I understand you will try to hack the system from other systems far away. If your remote jobs are not accepted, it may be that the machine has the job action parameter QRMTSIGN set to *REJECT (pass-through sessions are not allowed to start on the remote system). Other values of QRMTSIGN may be:

**FRCSIGNON: all pass-through sessions must go through the normal sign-on procedure. If your profile names are different, the pass-through will fail.*

**SAMEPRF: sign-on bypassing is only allowed for users whose user profile name on the remote and target system is the same. If the user profile names are different but a valid password was specified, the sign-on display is shown.*

**VERIFY: sign-on bypassing is allowed for all pass-through requests and no checking of passwords is done if QSECURITY value is 10. Passwords are mandatory for higher levels and are verified before automatic sign-on occurs. If the password is not valid, the pass-through attempt is rejected.*

*Program name: the program specified will run at the start and end of every pass-through session. Pass-through programs can be located in QGPL, *LIBL or *CURLIB.*

If your remote jobs are not accepted and it is not due to the QMRMTSIGN, another possibility might be that the *PCSACC parameter (which allows personal computer access) is set to *REJECT that prevents all such access.

If your remote jobs are accepted, there is no restriction on the minimum length of passwords. So you could find passwords like "A" or "AA" for example.

This Operating System does not handle password expiry date, password lifetime, and password history features. All these bugs were corrected in release 2 (more details below).

The system may have different security levels:

Level 10: no security active, does not require a password to sign on!!!

Level 20: the resources are not protected but passwords are active.

Level 30: offers security features. Passwords and resource security are active.

You can see the security level using DSPSYSVAL SYSVAL (QSECURITY) and you can change it with CHGSYSVAL. Although QSECURITY can be dynamically changed it requires an IPL to become effective. This release has many bugs related to control the user's terminal. For example: If you are a *ALLOBJ user you can use your authority from whatever terminal. You can have multiple sessions with a single user profile (two hackers in the system from different terminals with the same user profile, ha ha).

DST

If the Security Administrator has not restricted its use, you could have access to this very important software. The DST (Dedicated Service Tool) is a utility that allows virtual storage to be modified. DST has a program debug facility which allows users to interfere with the program during execution and obtain control at microcode level to display or modify memory variables. It also allows the installation of the operating system and the modification of Program Temporary Fixes (PTFs) to the systems microcode. The *SERVICE special authority is required to use DST, but remember that if you are in a system with security level 10 you will have access to this software.

The default passwords for the DST utility is QSECOFR. For the full use of DST (including changing DST password) the default password is 22222222. For basic use (does not allow password change) the default password is 11111111. If you want to know if you have access to the CHGDSTPWD command, type:

*DSPOBJAUT OBJ (QSYS/CHGDSTPWD) OBJTYPE (*CMD)*

That will list all the authorized users.

IBM Standard profiles

SECOFR: security officer
QSYSOPR: system operator
PGMP: programmer
QUSER: user
QSRV: IBM service user
SRVBAS: basic service user

Both the last two are used by the IBM engineers. All these profiles are supplied by IBM to all its AS/400 machines, so you will find these profiles in every machine (if the security officer has not changed them). The default passwords are the same as the user profile, for example:

Profile name: QSECOFR
Password: QSECOFR

You should keep in mind that many system administrators do not change the default passwords. You should try these passwords!

The AS/400 has inherited security features from the S/36. The inherited features are:

Authorization list security
Default/mandatory program menu
Current library
Levels of security (none, password, resource)

(I have written a detailed text about hacking S/36 available on underground BBSes in Buenos Aires, Argentina.)

AS/400 has also inherited some security features from the S/38. But AS/400 shows a new feature different from the S/38, if you have READ access at the user profile and UPDATE at the group profile level, then you will just get READ access.

If you find the hacked machine has security level 10, it requires only a user name to sign on. All users can access objects after signing on. The system creates a user profile when a user name does not exist. You will not need to manage object authorities, there is no security active, so the menu and initial program security are not active. It's great, isn't it? IBM sends the machine in this condition (security level 10) to the buyers and some system administrators do not change the default values.

Getting Info About the System

Sometimes the AS/400 may be running as if it were a S/36. To check it you can run:

QSPCENV

If you find *NONE the system is operating under an AS/400 environment. If you find S36 the system is operating under a System/36 environment.

In AS/400 a maximum number of logon attempts can be set. If you perform a greater number of attempts than the ones established the system will generate an error register in the log file. You should always try to keep unnoticed your presence in the system. So, for example, if you have a password and are into the system and you've got a more powerful one, but it is not a sure password, you should check what the maximum number of logon attempts allowed is. If the maximum number is six, you can try your doubtful password five times and no error registers will be created in the log file.

The QMAXSIGN represents the maximum number of sign-on attempts allowed to the users. The IBM default is 15, *NOMAX means unlimited numbers of attempts. To know the maximum number of sign-on attempts, run the command:

DSPSYSVAL SYSVAL (QMAXSIGN)

If you want to know all the authorized user and group profiles, use the command:

*DSPAUTUSR type (*GRPPRF)*

This will list all group profile names and the user profile names within each group. It will also list, at the end, any user profiles not within a group.

If you want to see a full listing of all user and group profiles run the command:

*DSPUSRPRF USRPFR (profile name) TYPE (*BASIC)*

You can know which users have special authorities, for example:

**ALLOBJ: system security officer*
**SAVSYS: operators*
**SECAM: administrator*
**SERVICE: IBM engineer*
**SPLCTL: operators*

The INITIAL PROGRAM may have different values:

**MAIN: you have access to the command line.*
**NONE: no program is called when the*

user signs on.

Program name: specify the name of the program called.

If you log onto a system and you get trapped in the INITIAL PROGRAM you can use the ATTN key to break out. Then using LMTCPB (Limited Capability) parameter you can look for the profiles with the values:

**PARTIAL: the initial program and current library values cannot be changed on the sign-on display. But you can change the menu value and you can run commands from the command line of a menu.*

**NONE: you can change the program values in your own user profile with the CHGPRF command.*

If you want to list all libraries on the system, run the command:

*DSPOBJD OBJ (QSYS/*ALL) OBJTYPE (*LIB) DETAIL (*FULL)*

If you want to see the contents of any library use:

DSPLIB (library name)

If you want to know the object authority for a library use:

*SPOBJAUT OBJ (QSYS/library name) OBJTYPE (*LIB)*

If you want to know system and user library lists use:

DSPSYSVAL (QSYSLIBL)

and

DSPSYSVAL (QUSRLBL)

If you want to know the object authorities of all the security related commands you can use:

*DSPOBJAUT (QSYS / command) (*CMD)*

Some of the most important commands are:

CRTUSRPRF: create user profile

CHGUSRPRF: change user profile

DLTUSRPRF: delete user profile

If you do not find *EXCLUDE in your authority it is great!! You can use all those commands.

Some objects may be protected via authorization lists (as in the old S/36). If you want to know all the authorization lists use:

*DSPOBJD OBJ (QYS/*ALL) OBJTYPE (*AUTL)*

And if you want to know the users on each authorization list use:

DSPAUTL (name of list)

If you want to know the authorities of a specific file or program you should use:

*DSPOBJAUT (name of file) (*FILE) for files*

*DSPOBJAUT (name of program) (*PGM) for programs*

Logs

Sometimes the machines are processing too much information and they are a little bit low on hard disk space. The first thing a System Administrator will do is to disable the logs. If you want to extract the history log records relating to security profile changes (to see if your unauthorized activities were logged), use the DSPLOG command:

Message ID CPC2191 is for deleting a user profile

Message ID CPC2204 is for user profile creators

Message ID CPC2205 is for changing a user profile

OS/400 Release 2

It keeps the security structure levels (10, 20, 30) as in Release 1 but there are other system values related to security. For example:

QAUTOVRT: controls the automatic creation of virtual device descriptions.

QINACTIV: controls the interval in minutes that a workstation is inactive before a message is sent to a message queue or that the job at the workstation is automatically ended. Possible values are:

**NONE: no time-out validation.*

'5'-'300': specify the interval for time-out (in minutes)

I am sad to say that Release 2 has also introduced measures to control the user's terminal. For example, to prevent users from having multiple sessions with a single user profile, it is possible to restrict users with *ALLJOB to particular terminals and it enforces a time-out if the terminal is inactive for an extended period:

QLMTDEVSSN: controls concurrent device session. Possible values are:

0: a user can sign on at more than one terminal.

1: a user cannot sign on at more than one terminal.

But the worst of Release 2 is that it has enhanced the password politics. Let's see it in detail:

QPWDDEXPITV: controls the maximum number of days that a password is valid, that is to say the change frequency. Possible values are:

**NOMAX: the system allows an unlimited number of days.*

'1' - '366': a value between 1 and 366 may be specified.

QPWDLMTAJC: limits if digits can be next to each other in a new password. Possible values are:

'0': adjacent numeric digits are allowed in passwords.

'1': adjacent numeric digits are not allowed in passwords.

QPWDLMTCHR: limits the characters that cannot be in a new password. Possible values are:

**NONE: there are no restricted characters.*

character string: up to 10 specific characters may be disallowed.

QPWDLMTREP: limits repeating characters in a new password. Possible values are:

'0': characters can be repeated.

'1': characters cannot be repeated more than once.

PWDMINLEN: controls the minimum number of characters in a password. Possible values may be from 1 to 10.

QPWDMAXLEN: controls the maximum number of characters in a password. Possible values may be from 1 to 10.

QPWDPOSDIF: controls if each position in a new password must be different from the old password.

QPWDRQDDGT: controls if a new password is required to have a digit. Possible values are:

'0': digits are not required in new passwords.

'1': one or more digits are required in new passwords.

QPWDRQDDIF: specifies if the password must be different than the 32 previous passwords. Possible values are:

'0': can be the same as the previous ones.

'1': password must not be the same as the previous 32.

QPWDVLDPGM: specifies the name of the user-written password approval program. Possible values are:

**NONE: no program is used.*

Program-name: specify the name of the validation program.

Logs

If you want to look at the logs, use the command:

*DSPLOG LOG (QHST) PERIOD ((start-time start-date) (end-time end-date)) MSGID (message-identified) OUTPUT (*PRINT).*

Example of the time and date:

((0000 941229) (0000 941230). The date format depends on the value of QDATFMT and it may be MMDDYY, DDMMYY or YYMMDD.

Messages

Identification	Explanation
CPF2207	*Not authorized to use object in library.*
CPF2216	*Not authorized to use library.*
CPF2228	*Not authorized to change profile.*
CPF2234	*Password not correct.*
CPF2269	*Special authority *ALLOBJ required when granting *SECADM.*
CPF2294	*Initial program value may not be changed.*
CPF2295	*Initial menu value may not be changed.*
CPF2296	*Attention program may not be changed.*
CPF2297	*Current library value may not be changed.*
CPF22A6	*User creating an authorization list must have *ADD authority to his user profile.*
CPF22B9	*Not authorized to change authorities in authority list.*

OS/400 Release 3

I really do not have experience with this release. This is all the information I was able to collect. We have seen that the verification of the security on the AS/400 is built in at the microcode level. So, it could be bypassed by programs developed in Assembler, C, or even Pascal or with the DST as we have seen. This loophole was removed with the introduction of level 40 security in Release 3 of OS/400.

It has also introduced an audit log that contains information about security related events. I do not know more about this release yet.

From astro.ocis.temple.edu!neitzert Tue Mar 28 23:05:19 1995
Return-Path: <neitzert@astro.ocis.temple.edu>
Received: by astro.ocis.temple.edu (5.61/25)
id AA01437; Tue, 28 Mar 95 23:04:42 -0500
Date: Tue, 28 Mar 95 23:04:42 -0500
From: neitzert@astro.ocis.temple.edu (Christopher K. Neitzert)
Message-Id: <9503290404.AA01437@astro.ocis.temple.edu>
Apparently-To: chris@ts6-2.upenn.edu
Status: O

Several friends of Ed 'Bernie S.' Cummings have prepared this press release due to the fact that a man is being held on $100,000.00 Bail for possessing the right electronic components to trick a pay phone into giving free telephone calls. His promotion of these devices is not against any law in the land, however the Governements of Deleware County, Pennsylavania and United States are acting as though their own laws do not matter to them.

—

Delaware County Pennsylvania, USA

Ed Cummings, also known to many in cyberspace as Bernie SS was arrested on March 13th, 1995 for 2 misdemeanors of possession, manufacture and sale of a device to commit Telecommunications fraud charges. He is being held in Delaware County Prison in lieu of $100,000.00 Bail. His story follows.

On the evening of the 13th Bernie S. received a page from his mail drop. Some people he knew from Florida had stopped in at his mail drop thinking it was his address. They were looking to purchase several 6.5 Mhz Crystals. These crystals when used to replace the standard crystal in the RADIO SHACK Hand Telephone dialer, and with some programming, produce tones that trick pay phones into believing they have received coins. These are commonly referred to as Rred boxesS and got their name from an actual red box pulled from a pay phone in the late seventies by some curious person.

Ed Cummings met these people at a local 7-11 where he was to sell the widely used electronic timing crystals for roughly $4 a piece. The purchaser only had two twenty dollar bills and Ed Cummings no change. Ed Cummings went into the 7-11 to get some change to make the transaction. A police officer noticed a van parked in the parking lot of the 7-11 with several African Americans inside. As Ed was leaving the 7-11 he noticed fifteen police cars pulling into the parking lot of the 7-11.

Next thing he knew the police were asking him if they could Trifle through his car. He said no. Moments later as he was talking to a Detective and noticed another police officer going through his car. He asked the officer to stop. They did not, in all the police confiscated a few hundred 6.5Mhz crystals (which he resells for roughly $4 a piece) and a large box of 100 dialers. The police told him they would get back to him, and he could have his electronics back if the contents of the bag were legal. In the contents of the seized items was one modified dialer, that a customer returned after modification explaining that it did not work, a broken red box.

The next day Ed 'Bernie S.' Cummings was over at a friend's house working on their computer when eight to ten plain clothed armed men burst into the house and ordered him and his friends to freeze. They cuffed him and took him to a holding cell(what jail?). There he was left without a blanket or jacket to sleep with in the cold cell.

That evening the Secret Service had been called in when someone figured out what the dialers and crystals would do when put together. The United States Secret Service found his home and entered it, while they were questioning him.

The next morning at his arraignment he was finally told of the charges he was being held upon. They were Two misdemeanor Charges of manufacture, Distribution and Sale of devices of Telecommunications Fraud. and Two Unlawful use of a computer charges. His bail was automatically set to $100,000.00 because Ed Cummings refused talk with the police without his attorney present.

The Secret Service presented to the judge a 9 page inventory of what they had found in his home. On that inventory there 14 computers. 2 printers. Boxes of bios chips for the systems he worked with. Eprom burners which the Federal Agents had labeled RCellular telephone chip reprogramming adaptersS Eproms are used in everything from Automobile computers to personal computers. They also confiscated his toolbox of screw drivers, wire clippers and other computer oriented tools he used for his consulting job.

The Judge dropped the Two unlawful use of a computer charges due to the fact that the evidence was circumstantial and the county had no actual evidence that Ed had ever used the computers in question.

As of 3/27/1995 Ed Cummings is still in Delaware County Prison awaiting his trial. His trial has not yet been scheduled and Ed will most likely not raise the One Hundred Thousand Dollars needed to be released on bail.

If anyone hsa any questions or comments direct them to this newsgroup and my email box.

Thanks.
Christopher K Neitzert

—

christopher k neitzert neitzert@astro.ocis.temple.edu Film and Video Student
InterNetworked Multimedia Design, Implementation and Administration
office: 215.467.3001 Fax:215.467.3412 Service: 215.505.6637
Coming Soon to this space: Chapel Perilous Project Velcro!
Support Your Local Free Net!
Linux: Choice of a GNU generation! http://astro.ocis.temple.edu/~neitzert
"When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl." -jpb
Finger for PGP2.6 or RIPEM Keys.
Opinions here are not those of temple university nor my clients.

This public letter on the net

TOWNSHIP OF
HAVERFORD
DELAWARE COUNTY
POLICE DEPARTMENT
DARBY & MANOA ROADS, HAVERTOWN, PA. 19083-3699
(610) 853-2400
FAX (610) 853-1706

CHIEF OF POLICE
GARY E. HOOVER

DATE: 07 APRIL 95

TO: CHRISTOPHER K. NEITZERT
CC: TEMPLE UNIVERSITY PRESIDENT

FROM: DET. JOHN MORRIS

SUBJECT: COMMONWEALTH VS. CUMMINGS

1
PAGES TO FOLLOW

The information contained in this facsimile message is privileged and confidential, and intended only for the use of the individual or entity named above. If the reader of the message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify us by phone immediately, and return the original message to us at the address listed above by the United States Postal Service. Thank you.

A HOME RULE MUNICIPALITY

Christopher Neitzert,

I am surprised to see that someone from Temple University would send out a press release without actually checking the facts prior to trashing a persons reputation. It is obvious that the accusations against this department and I are made without any evidence, since it is so far from the truth.

You and Temple University have attacked my credibility and reputation. I have received calls from friends and business associates appalled at my conduct, as advertised and told by you and Temple University.

I therefore have contacted the Fraternal Order Of Police to have your press release turned over to S. Stanton Miller Esq. for any civil liability against you and Temple University for defaming my character and for libel.

Det. John K. Morris #1763
Haverford Twp Police

got this threat from the cops

"Letters are the cornerstone of any civilized society."

Privacy Concern

Dear 2600:

Regarding someone's concerns over privacy of your subscriber list, section E211.4.2 of the Domestic Manual requires that publications sent by Second Class have a "known office of publication" open during "normal business hours where the publication's circulation records are maintained or can be available for USPS examination." A Second Class permit also requires that you tell the world, as you did on page 2 of your Autumn 1994 issue, the number of subscribers and newsstand copies sold (which impressed the heck out of me - I didn't know you were that big). So Big Bro is allowed to look at your subscription lists!

Have you considered mailing by bulk third class instead? The basic rate is 23.3 cents per piece (anywhere in the U.S.) which is probably not much more than you're paying now and there's no zone-based rate, no need to file a "Statement of Ownership, Management, and Circulation" or requirement to have a "known office of publication". Or how about offering the option (at a higher cost, obviously) of getting *2600* by first class mail in a plain unmarked envelope? (I still prefer to buy mine at the newsstand, though.)

Speaking of the USPS and the NCOA database mentioned on page 6, the USPS' database is now also being used to identify CMRAs (Commercial Mail Receiving Agencies, or "mail drops") to commercial subscribers (such as credit card companies who are concerned about applicants who use a mail drop as their "residence address").

Also, for anyone interested in all kinds of used and antique phones (original candlestick phones, Ericofons, even phonebooths)! You should get the mail order catalog from Phoneco, P.O. Box 70, Galesville, WI 54630 Phone 608-582-4124, fax 608-582-4593.

Anonymous in MD

Protection of our mailing list always has been one of our highest priorities. While second class mailing allows the post office to look over your shoulder a bit, we don't believe we're giving them anything they don't already have. They don't have access to our subscriber lists. What happens is this: every three years or so a postal inspector comes by and picks ten names at random from our subscriber print-out (they never get to keep or copy this rather large printout). We have to show that most of the ten people actually requested our magazine, usually by producing a subscription request. This doesn't concern us since the post office can get our subscribers' names and addresses by simply looking at the envelopes we send out. We don't believe they are using this rule to focus on hackers - a number of the ten names are usually large corporations. But it was admittedly odd that last time one of the names they picked at random was Kevin Mitnick. (We were unable to find his paperwork.) Even with this weirdness, we don't believe this is a threat since virtually every magazine in the country has to go through this. And, if it is a threat, we'll never know if we don't play along for a while. As for alternatives, first class mailing would nearly quadruple our mailing costs and third class would ensure that we're at the very bottom of the priority list.

Hacker Techniques

Dear 2600:

I obtained Oasis for the Macintosh about three weeks ago. Since Oasis still displays itself as a space on the extension manager in System 7.5 when you name it with spaces and since anyone who peeks inside the extension folder can see Oasis as a space when listing by name, there was an apparent weakness in using it on other computers. Nothing blows more chunks than getting caught. Thus, being the paranoid person that I am, in order to make the 12K extension even more discreet, I essentially combined Oasis and the AppleShare extension. By combining the two, if the text files are discovered where Oasis stores your information, your targeted person will never know where the dated text files are coming from. Oasis becomes part of the user's system software; therefore, even the most advanced user would not guess to look into each piece of system software for clues as to what is causing the text files.

In order to combine the two, use ResEdit and copy and paste each item into the respective resources. You can even tell it where to put the dribble folder. Please let it be noted that the above procedure only works when the computer turns on the AppleShare and is connected to an AppleTalk network. I have not tried merging Oasis with other pieces of system software, but I am sure it will work. If you have enough time on the remote computer, I suggest making the dribble folder invisible.

If anyone has any suggestions for better ways to hide the key capturing text files, please write in.

Pumpkin Smasher
Natchitoches, LA

Dear 2600:

We stumbled across a little Unix hacking trick your readers might find worthwhile. This particular hack affects only "hpterms", which are HP-UX's version of xterms. Basically, HP built a lot of functionality into the hpterm which does not appear in an xterm. The best part of the functionality is user-definable "soft keys", which are programmable using escape sequences. For example, if a user typed *ESC & f2 a 1 k 3 L pwd* it would define his or her soft key #1 to be the 3-length command string "pwd".Then, if that user typed *ESC & f 1 E* it would execute soft key #1, and the pwd would execute. And of course more creative commands than "pwd" are allowed - like, for root, an escape sequence that adds a new root user to the /etc/passwd file.

Now this seems innocuous, but the great thing about it is that a user does not have to execute these strings, but simply have them displayed in an hpterm window. Therefore, if those escape sequences are embedded in a normal text file, and the user views that file, their soft key would be programmed and executed, with their privilege. We discovered that this also works in mail - if a user gets a mail message and reads it in an hpterm window, the escape sequences still make it to the window. Of course, you'd want to have the command begin with a "!" For a shell escape, unless you can do all you want within mail.

The one drawback to this scheme is that when the soft key is executed the command and its output are displayed to the screen. We have not found a control or escape sequence that turns echo off, so you run the risk of alerting knowledgeable users if you use this trick. It is very powerful, however, in that it exploits read privilege rather than execute privilege and can therefore reach anybody using an hpterm. And on HP-UX systems, only the really knowledgeable use xterms rather than the default hpterms.

There are lots of other escape sequences, all documented, that do other cool things like disabling the user's keyboard, etc. Use wisely.

Mickey and Mallory

Dear 2600:

This is to Black Knight who wrote in about his problem with the password protection on the disks of the Apple IIe's at his school (Summer 94). There are several ways to get around this dilemma.

You and the friend you want to share files with could name your passwords the same exact word. If this doesn't work, you could try my procedure below.

To begin with, a BASIC program on an Apple IIe is stored in the memory location $800. DOS is stored in $B000. When you reset the computer, these locations are the first to be erased. But memory location $C00 doesn't get touched during the reset. So, move your program to $C00, reset the computer, boot your friend's disk, move the program back to $800, and save it on your friend's disk. To do this, boot your disk, load the program you want to copy, and get to the BASIC prompt (]). Type:

] Call - 151
** C00<800.BFFM*

Put your friend's disk in the drive. Now hit Control-white apple-reset simultaneously to reset the computer. When your friend's disk boots, log in and get to the BASIC prompt. Type:

] Call - 151
** 800<C00.F00M*
** (Control-C)*
] SAVE WHATEVER

Your program is saved on your friend's disk as "WHATEVER".

Wicker Man
DeKalb, IL

Dear 2600:

After reading the "More Window Tricks" in the most recent issue, I was reminded of something else that many stores will do to keep prying hands outta their machines. Many stores feel that having a password on the default screen saver is bad for business, so they use other protection technics, so that customers can play with the machines, but not damage them.

Here is the most common form. These INI settings are always in the Progman.ini file and normally under the heading of [restrictions]

NoSaveSettings=1
EditLevel=4
NoFileMenu=1
NoRun=1
NoClose=4

All of these are rather obvious, so I won't go into an explanation of what they do. Fortunately, the stores seem to think that putting these switches in is all they need to do. Also, they delete the File Manager Icon, as well as the Dos Prompt Icon. Simple enough to bypass. Open the Notepad and edit the Progman.ini file. Put a semicolon at the beginning of each line, and then just give the machine the three finger salute twice. Thus rebooting the machine. Once the machine ends up back in Windows, you'll have full control of the machine.

As for the password on the Windows default screen saver - if you want, just look in their Control.ini file. Search for Password, and you'll find whatever their password is. Feel free to change it afterwards.

Streaker

War Dialing

Dear 2600:

Dr. Delman's article entitled "The Risks of War Dialing" in the Winter 1994-95 issue requires at least a brief response to set your readers straight. Without attempting to address the specifics of any particular state's law, the implication that there is no law which would directly apply to war dialing must be corrected (and should be a lesson not to rely on law enforcement or security people to know what the law is). Below is an excerpt from Title 47 of the Code of Federal Regulations, Section 64.1200.

(a) No person may:

(1) Initiate any telephone call (other than a call made for emergency purposes or made with the prior express consent of the called party) using an automatic telephone dialing system or an artificial or prerecorded voice,

(i) To any emergency telephone line, including any 911 line and any emergency line of a hospital, medical physician or service office, health care facility, poison control center, or fire protection law enforcement agency;

(ii) To the telephone line of any guest room or patient room of a hospi-

tal, health care facility, elderly home, or similar establishment; or

(iii) To any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service or other radio common carrier service, or any service for which the called party is charged for the call.

It should be fairly obvious that war dialing most exchanges will hit one or more of these numbers, moreover, you will never know when you have done so. In order to see this regulation for yourself, ask the librarian at your local law library to point you to 47 C.F.R., section 64.1200.

Clint Sare
Texas Bar #00788354

The article in question quoted a law that could be used against war dialing but questioned its effectiveness. The same applies to the law which you quote - the primary design of it being to protect emergency services and hospital patients from computerized sales pitches, as well as to protect pager customers from being paged en masse with some sort of commercial service or fooled into calling a premium service. Since each of these offenses would require the offender to leave some sort of a signature (like a phone number to call back), catching them wouldn't be overly difficult. War dialing is different since the purpose of the call is simply to see what answers. It's also almost impossible to catch a war dialer unless the dialer targets one site repeatedly or the phone company is watching the dialer. Remember, the most a war dialer can do to a customer with a single line is ring their phone once or twice, then hang up. Not very many people would consider one such instance enough to launch a federal case.

Dear 2600:

After reading the Winter edition of *2600 Magazine*, some comments about a few of the articles. The risks of war dialing was of particular interest to me, as I have had a slight run-in with SouthWestern Bell's security! I really didn't think about setting up my war dialer to dial randomly, but in number order, and that was my downfall. After spending a day or two dialing, all of a sudden my lines both went dead without any warning. I went to the local payphone and called telco repair and they said "Your account if flagged sir. One moment and I'll connect you to the person who flagged your account." I was then transferred to SouthWestern Bell's security office and had to talk to one of their security personnel. Security said that they knew I was "war dialing" and that this was "illegal", so they ordered my lines disconnected until I talked with them. Basically they gave me a warning and said don't do it again. My lines would be reconnected later in the day. I'm not sure if what they did was even legal, or if they would have even caught me if I hadn't stupidly been dialing in numerical order.

Also, I have worked in the cable TV field for five years before switching to a totally unrelated field, and have a few comments regarding James Allen's letter to your fine magazine.. While cable theft is indeed a problem, there are a few facts that he neglected to mention. The one-way addressable boxes some cable companies use are just that, one-way. The cable TV company has *no way* of telling what channel you are watching (this requires a two-way cable system), and trap systems are still *very* plentiful, if not growing every day! Some systems operate both trap and addressable pay channels on the same cable. Usually the trapped channel is only one or two channels, usually HBO and/or Showtime. The problem you have with an addressable converter is that your new $2,500 bigscreen TV that is supposed to be cable ready is *not* cable ready if the channels are all addressably descrambled. This tends to piss off a lot of people, as well as hotels that want a local cable feed for HBO. So the cable company now can say, "Well if you just want HBO, you don't need a descrambler" and if you want pay-per-view, you are out of luck, but at least those subscribers are somewhat happy that they can receive at least one pay channel without losing their cable ready TV's that they paid big money for. Also, in two-way addressable systems, there is a way to defeat the cable company's intrusion of your privacy by simply building a filter to block all signals below 54 mhz (Channel 2). The two-way boxes transmit back to the cable company usually at a frequency of 30 mhz. Build a filter to block out below 54 mhz and the cable company cannot receive *any* return info from your box. In fact, in some cable systems, you can install just such a filter, order pay-per-view (on an impulse pay-per-view system, a box that sends your box's info to the cable company to start billing) and the cable company never receives the order, but your box will descramble the channel! This doesn't work on all systems, but on some. Also, some cable companies that run "positive trap" systems (where a trap is *required* to receive that channel) are very easy to defeat. Just pick up a copy of *Popular Electronics* or whatever, and order a channel 3 or 4 (whatever your converter or VCR output is) *positive* trap and install it on the output of your converter or VCR. This will remove the injected interference on *all* positive trapped channels!

Lineman

Numbers

Dear 2600:

Within the Pacific Telephone system, in southern California, and other areas, is a unique and often useful feature. Within the 213 and 818 area codes there exist number pairs for each exchange which are tied at the C.O. and are for the use of linesmen who need to be able to speak to each other from remote locations (usually on poles, or at "B" boxes). It works like this: XXX-1118 and XXX-1119 are pairs. Dialing the 1118 half yields a test tone at (usually 800hz). There is no ring signal from the C.O. Another person dialing the same prefix followed by 1119 will be instantly tied to the 1118 line, and the tone stops. You can arrange with a friend to make communication at, for example 11:30 pm on the 466 exchange. At 11:30 you dial 466-1118 and gettone. He or she dials 466-1119 and you are instantly connected without either party knowing the source number of the telephones you are calling from. We used it for party rendezvous purposes by instructing friends to call on the Dunkirk 4, or Hollywood 6 line, and wherever we were, we could reach friends without the need of C.B.R.'s or pagers.

For clandestine purposes, of course, this offers a fairly trace-proof means of communication. I have found it to work in Minneapolis, MN and Seattle, WA. There may be slightly different number pairs for different carriers. Experiment and have fun!

We used to get a kick out of hacking four or five MCI or Sprint access codes, and then with the use of MCI and Sprint numbers in major cities, route a local call via New York to Atlanta to Dallas to Chicago to Memphis to Boston to Miami etc... eventually back to the local number. It is humorous to think what the carrier did if they attempted to locate the source of the call and it kept originating at another office of that carrier.

I still remember my earliest introduction to phreaking, back when coin phones had bell tones representing the denominations of money inserted. I saw a guy with three little bells on a block of wood - when the operator instructed him to insert 40 cents he would hit the appropriate bells with a metal bolt producing the bing, bang, bong, and the operator would thank him. This was in the early 70's before DTMF and TSPS's.

TAG
Sheridan, OR

Dear 2600:

I've got a few numbers here that I thought, with your large and vast array of technology, you might be able to let me know what they are for: (313) 480-9999 - recorded message twice "You have reached the Ypsilanti (which is the city I live in) DSO" then I believe it hangs up. Also (810) 471-9998 gets you an Ameritech operator who asks "What number did you dial?" Actually all the 999x numbers do weird things around here. 9996 is always the high tone of a loop. 9994 is a high tone, then drops off in just about every prefix. I probably shouldn't bother you with trivial stuff like this but like you I am curious.

Mike

Actually that 9999 number is our first encounter with an Ameritech switch recording. NYNEX keeps theirs at 9901. Keep exploring.

Dear 2600:

Several years ago i stumbled upon a very interesting number run by my phone company (SouthWestern Bell). It all started one day when i was messing with the 971 feature that allows you to make the phone ring. You dial 971, then you hear a dial tone. Next you dial 2# and you get another dial tone. Then hang the phone up for one second, pick it back up and hang up for the last time, and your phone will begin to ring. Anyway I proceeded to dial 971, then instead of 2#, I dialed 9# and to my surprise a recorded message read 9-5-5-9-5-0-1. It wasn't until months later that I realized this was a phone number. (I was only 13.) I immediately called it and heard a ring. After a few minutes no one answered and I gave up. A few months later when I was home on vacation and was extremely bored, I called and let the phone ring for some odd 30 minutes when suddenly I realized it wasn't ringing anymore and I heard voices on the phone. It seems the phone breaks in occasionally on random numbers and about 75 percent of the time to other people who call 971. It's kinda fun to tell people you are the phone company who has broken in on the line and what they are doing is against the law. (Of course I eventually tell them the whole story for they must be cool if they are doing something creative and explorative on the phone, and most of the time they are just making the phone ring to show off to their friends.)

Data

Dear 2600:

Here's something of interest: (303) 294-9259. Apparently it verifies if your Caller ID is sent or blocked. The uses are obvious.

Major Zeek

And since no matter how we call the thing it tells us that our number was sent, we have to wonder if this is just a number that happens to have that recording on all the time.

Dear 2600:

Well, believe it or not, that Ottawa phone trick (mentioned in Winter 1994-95) that's used to put the phone in service mode works on our US West "Millenium" payphones in the Minneapolis/St.Paul area. These phones can be found in the following places in Minneapolis/St. Paul: Mall of America, Minneapolis/St. Paul International Airport (both terminals), Ridgedale Shopping Center (Minnetonka), Interchange Office Tower (St. Louis Park), and maybe a few other locations yet to be discovered. While we're on the subject of "Millenium", the Mall of America's phones have been outfitted with pushbuttons that allow you to call US West payphone repair, Mall Information, and Mall Security, all for free.

Airwolf
Twin Cities

Questions

Dear 2600:

I've received two issues of *2600* so far and have enjoyed both of them. I don't promote spreading knowledge about cracking into systems (unless for the benefit of system administrators) or foiling various services (Ma Bell, credit cards, etc.), but hey - I'm an electrical engineer and everything you print is damned interesting.

I have a request and a suggestion. Your Summer 1994 issue contained a script file which would let Unix users learn who's fingering them. Unfortunately, my school's system doesn't use the MIT finger. Actually, I've heard that there are several versions of finger floating around. Would it be possible to print a program (or have one downloadable) which would work for *any* version of finger? I've heard it's possible, but everyone here is too busy to get into the programming.

Do you think that your programs, text files, and just about anything technical might be easier to read if they were printed in a monospaced font? I had problems typing in the .fingerrc code because I couldn't tell where spaces were (a really big deal) and whether the single quotes were single quotes or apostrophes. I have a feeling that no one would mind easier-to-read code.

Thanks a lot. Your publication reminds me a lot of *YIPL*, the Youth International Party Line stuff from the phreak days of the 70's. I'm glad that, unlike *YIPL*, *2600*

is not publishing phone credit cards numbers or other illegal and annoying stuff.

GF

We have finally instituted a uniform typeface for programs so that this shouldn't be a problem. We're also in the process of putting our program listings up on our ftp site to further simplify things. Regarding your finger problems, every version of Unix works just different enough to ensure that such difficulties exist. We're sure somebody on the net has what you're looking for.

Pirate Alert

Dear 2600:

Back in October 1991 we released CardIt, a credit card verification/generation program for the Macintosh (hey, the scene was barren...) based on algorithms published in *2600*. It was pretty much a quick and dirty "get me into it now" program (hacked out for the most part by Yankee Flatline) with a bare bones interface and slightly adjusted algorithm, with appropriate sound bites snagged from a Consolidated album. At the time, we simply wanted the ability to get around setups which relied upon this verification technique to exist on the Mac, and to have it be distributed to everyone.

Well, it seems to have made its way around, pissed off the people at service providers, and recently generated a wave of ResEdited hacks. We recently downloaded a "MacCarder" file containing three copies of CardIt which had each been changed slightly, pretending to be (ha!) legitimate new programs. This cracked us up, and probing further into the "About Stolen Program" box revealed that some of the ResEdit wizards have decided that their hard work needs to be rewarded with cold hard cash! They were asking $20 for our program! We died laughing at this and decided to set the record straight a bit. We released CardIt v1.0b1 with a creation date of Wed, Oct. 16, 1991, 11:45 AM. The program's examine/generate windows are not moveable and there is a radio button to swap between "Mod 10" (doesn't work) and "Normal". All of the ResEdit hacks we have seen simply change the splash screen from our "UpLink/LoST Presents..." to theirs, take out the cool sound bites from Consolidated, and swap out the other small things like version numbers and whatnot. None of them can get around the moveable window problem or change the way they compile numbers.

We decided that it should be stated at some point that this is going on. If someone were to actually send these people cash that would just suck, you know? Hackers/Krackers/Carders and the rest of the planet prey on what people do or do not know. Hell, CardIt is a tool which takes advantage of this, so we must put the info out there to everyone that many of the versions of credit card generation programs out for the Mac are hacked versions of CardIt. If you like their splash screens better than ours, send them whatever you like. We never asked for anything and don't expect anything, but won't let anyone profit from our program simply because we never put it out that the program is *free*. If anyone has paid for one of these versions, they have been had, and that sucks. We expect that readers of *2600* are apt to be far more leery of anything that someone tells them than most people would be, and this just proves that people try anything. We are not pissed or anything at anyone hacking CardIt and asking for something in return - they are just trying to get by - but will not let them succeed simply because we didn't put the correct information out to the world.

On a better note, we have also recently seen a program which proclaims that it "...is what CardIt was supposed to be..." and in many ways is. It pulls from a small database of banks and will provide the name of the bank a card is from (we guess from the files published in *2600*) and has been written and compiled four years after CardIt, so it should be a bit faster to boot. We raise our red boxes to the programmers on this. Otherwise, UpLink and LoST have released Holy Wardialer to version 2.0 (now replaced by Assault Dialer by Crush Commander) CardIt 1.0 and some other small beta NUA attackers which never saw true release. They were originally distributed from a cluster of boards run by Red 5!, Hellbender, Crush Commander, and Yankee Flatline. We have some items planned for release in the next year or so. Thank you for helping us to clear this up.

Red 5! and Hellbender,
UpLink/LoST

Answers

Dear 2600:

In response to Lady Penelope's plea (page 42, Autumn 1994) for cryptography info, this should be what you have been praying for. Check out Bruce Schneier's *Applied Cryptography - Protocols, Algorithms, & Source Code in C*. ISBN# is 0-471-59756-2 and it sells here in the U.S. for $44.95. Take the ISBN# to your library or book store and they should be able to get it for you. In it are detailed explanations on numerous protocols, including RSA, PGP (Pretty Good Privacy), Clipper, etc. Source code is available from the author: Bruce Schneier, Counterpane Systems, 730 Fair Oaks Avenue, Oak Park, IL 60302 USA. This book should be required reading for all cryptoheads. I would send you a copy, Lady Penelope, but the NSA (National Security Agency) regards this book as "munitions" under export law!

Name and Address withheld

Hopefully the post office will help us smuggle your letter out of the country.

Dear 2600:

A poor beleaguered letter writer in your winter 1994-95 issue (Volume Eleven, Number Four) asked how to get around the foreign PTT terminating a telephone call when his international callback system had DTMF sent through it. To Terminated in Long Island: the answer to your dilemma is to "spend money". Given the spread on your international callback system, you should have plenty of it.

First get a personal computer based callback system. Many international callback boxes are locked up hardware architectures. Ditch these now, because they aren't flexible and they can't change with the next curve the PTT's will throw at you. PC systems can.

New PC-based systems using computer telephony circuit cards from companies like Dialogic or Rhetorex are completely open. This is an exploding industry and there are dozen of companies offering a full spectrum of

products which are often inoperable. The PC systems can be variously configured with a buttload of features, to include speech recognition cards. With small vocabulary, speaker independent speech recognition, you can get around entering DTMF tones. It also allows for customers that only have pulse phones, which is a huge market. Skeptical? ATT has laid off 8,000 operators because the circuit cards can recognize "0" through "9", "Yes" & "No", as well as any human. And yes, of course, foreign languages are available.

How do I know all this? Because I'm doing it, and it kicks ass. What about software? There's over 40 application generator software packages. App Generators allow you to assemble working PC telephony software by merely dragging and dropping Icons - it's totally codeless. Want to know more? Get a *free* subscription to *Computer Telephony Magazine* by faxing a request to (215) 355-1068. This is a killer rag.

A fully functional system (12 line capacity) could be assembled in a month for about $25K. And there are books on how to do it. You'd better run to catch up.

Gump
Sacramento

Bookstore Stories

Dear 2600:

Just started reading your zine and I really enjoy it. Let me tell you my bookstore story. I used to work at B&N Bookstores in the Bay Area. We only received about six copies of your magazine and they would sell out quickly... this is one reason that I never got to read it. When I would ring it up, the customers would never tell me what your magazine was about, so tell them to lighten up! Some info for the people buying at B&N... we always have a list of magazines but it is not always updated. Sometimes it is alphabetically arranged and other times by topic. Magazines always come in on a random date - even the person in charge has no way of knowing. It is almost impossible to order other types of magazines or ask for additional copies of ones we stock. Occasionally we get a few magazines that we don't normally stock, but these are usually European mags. Best thing to do is find out who is assigned to magazines and ask them *nicely* to reserve a copy when it comes in. Remember, they are under no obligation to do this. B&N pays crappy for overworked help so kindness goes a long way.

Now, on my second item. The BART system running in San Francisco and the East Bay has payphones by a company called AmTel. When I punch in "*", "0" and then wait, it would read off an amount of money in the 10 to 20 dollar range. So I had assumed that it was the amount of money made by the machine, until I had a few read off "11 cents" and "15 cents". So what's the deal? I can do this at any payphone at BART but I don't know what it means. How could someone make an 11 cent call? (*85 gets you a supervisor, *8#3 gets you voice-mail - I'm going to keep searching the system!)

Confused and Learning
The Black Carpet

If you knew about some of the reactions our readers get when they tell people what 2600 is about, you'd understand their hesitation to bring more into the circle. We'd like to know more about these payphones - we suspect they're adding total revenue, including credit card calls.

Dear 2600:

The other day, i was visiting the local Barnes & Noble to snag a copy of *2600*'s winter edition. As i was checking out, the clerk looked at me funny, and said, "There's some good articles in this one, you'll enjoy it." I was, needless to say, surprised, and started chatting with her. Apparently, she and her husband are avid readers of *2600*, *Phrack*, and all those good ones. This happened only five hours after I bought a tone dialer from Radio Shack (so I don't have to remember all those phone numbers) where the clerk told me what my local BBS handle was, my exact reason for purchasing the dialer, and how much he wished he knew how to build what i was going to build.

It's funny how small the world can seem, and it's great to know how many people out there are on *our* side, rooting for electronic freedom.

Pestilence/517

Caller ID Question

Dear 2600:

My question is about Caller ID. I recently sent a fax to CNN's *Talk Back Live*. When I sent this fax I used the standard *67 to block the phone number. I sent the fax from Chicago to Atlanta, made a normal fax connection to the CNN Fax Server (ID), and went back to playing.

The CNN Server (computer voice generator) called me back to thank me for participating. What's up? I used the *blocker!* This concerns me about our privacy. How can I block calls and feel secure that my number is blocked? Does CNN now have me on their sellable mailing list of techies because I use a fax? Or did they use an auto-call back? I have to wonder.

Chester-Buzz

*You don't mention whether or not you called an 800 number. If you did, *67 would not block your number from showing up on CNN's ANI display. It's also possible your phone number was printed on top of your fax or on their fax display. You would have had to have keyed it into your fax machine at some point in the past. We doubt Call Return would work between Chicago and Atlanta. It's also unlikely that nationwide Caller ID kicked in since it theoretically won't be in place until December. If it already works in your area, *67 should block your number unless your local company uses a toggle system where *67 simply switches your line from the default setting. NYNEX had such a system but finally changed it so that *67 always blocks and *82 always unblocks. When nationwide Caller ID arrives, these will be the standard codes.*

Lack of Security

Dear 2600:

Here's an interesting little tale which certainly taught me an important lesson and hopefully might also have some usefulness to your other readers. Recently, I was more or less bribed to, shall we say, disenfranchise myself from my lucrative yet maddeningly boring position at a certain well-known university. The whole affair was a classic study in the politics which dictate the organized "research" at these great

centers for free thought and individual inquiry.

I could go on for days about all the subtleties of that last one, but I want to neither bore the reader nor infuriate myself in doing so. Most of my work at said job was done on a Sun SPACStation and, being the only one in the office who could ever turn the bloody thing on, I had super-user access to the machine. At the time of my departure, there were a lot of my personal files on the computer and, considering that I was planning a little vacation to celebrate my newfound liberation, I didn't feel any great push to download them. I figured that since I was the one with the root password, it was pretty much up to me to decide when (and if) I was ready to fork it over.

Although I was confident I'd covered all possible security holes, there was one item I overlooked. Sun ships their operating system on CD-ROM these days and it's possible to boot the machine directly from it rather than the hard disk. When doing this, it gives you the option to install a "mini-root" file system on the swap partition. This is really meant to be used when installing the entire OS for the first time; however, this act apparently also allows one to edit files on unmounted partitions, most notably /etc/passwd. As you no doubt realize, all you need to do from there is delete the encrypted root password and then set it to whatever you fancy using the passwd command.

I say "apparently" because I got this information from a rather incomprehensible documentation memo which my replacement had rather considerately created. Thanks to his bumbling incompetence as a system administrator, I've since regained super-user access through more covert means (allowing me to get said memo, as well as my files) and am currently deep in the process of insuring that there are enough backdoors to allow me to regain root whenever it suits me. Although I no longer have physical access to the machine to test this method, it seems to make intuitive sense given what I know about Suns. He did, after all, somehow manage to change the root password in my absence. Do you see any reasons why this wouldn't work? At any rate, I find it rather interesting to think that all one needs to gain root on a SPARCStation with a CD drive is a Solaris CD-ROM and perhaps a lockpick. If I recall correctly, one can also reboot from a tape, so the same methodology would apply with a copy of Solaris on an 8mm tape.

Although I must admit that I'm rather new to the world of hacking, I'm rather encouraged/surprised to see firsthand what a joke the security on a supposedly uncrackable machine can be. Of course, I have to concede that I had a hefty advantage in this case and my task would be considerably harder on some alien machine, having no knowledge of the internal structure and security measures. However, I've heard rumors that there are sites on the Internet itself which hold sophisticated password-cracking software. That almost seems too good to be true, but stupider things have happened. Have you considered putting together a directory of the best H/P sites on the Internet for an upcoming issue? What method is used to encrypt passwords under Unix systems? The user documentation does not say it's not "crypt", but of course it doesn't tell you what it is.

There's one final issue I'd like to get your thoughts on. First off, let me say that I'm very glad there's a publication devoted to those of us who refuse to be restricted by someone else's vague notion of legality in exploring the full potential of these wonderful tools we call computers. Although I can't believe that the Feds haven't shut you down yet as some threat to national (in)security, you have my deepest support in evading such a fate indefinitely.

While I have gotten many a wonderful idea from following each issue, I know that there are others with a more fascist agenda who are poring through them. What is your opinion on knowing that assorted government/corporate entities will be absorbing whatever bits of wisdom you publish and then using this information against us to tighten up security in the future? What's your policy on accepting subscription orders from such groups? Yeah, I know: you can walk into any decent bookstore and pick up the latest issue, so they're probably going to find out anyway. It's just that I hate to see my opponent's mission made any easier....

Another Thought Criminal
SF

We're putting together a library of information as well as pointers on our anonymous ftp site at 2600.com. You may find what you're looking for there. Passwords on Unix systems are encrypted using a one-way trapdoor algorithm that employs DES. As for who winds up reading our magazine, it would be pointless for us to worry about it. If we start restricting information to certain people and/or groups, we inevitably wind up restricting our own growth. That's what a lot of our opponents would like to see.

NYNEX Outrage

Dear 2600:

Our basic service where we live consists of Call-Waiting, Three-Way-Calling, and Flat Rate. Last month, we subscribed to Call-Forwarding with a free connection charge. Then, we called up the business office to cancel an extra listing we had put in the phone book and didn't want anymore. Fine. Last, we ordered a new "free" white pages directory. All's well until the bill comes.

We get the bill, and what do you know, it's $130! Wow! There's no way. So we take a look at it and find this. We were charged $16 for a "free" installation charge for call-forwarding. We were charged $23 for a yellow pages directory when it was *supposed* to be a white pages and was *supposed* to be free. We were charged for *two* custom calling packages (i.e. Call-Forwarding, Call-Waiting, Three-Way-Calling) when we only had one (a package is any two or more of them) and then charged for a *non-published number*. What had NYNEX done? They lied about the free installation. They charged me for a free phone book (and sent me the wrong one as well), and best of all, when we asked to get rid of our directory listing, the operator at the business office thought we meant to get a *non-published* number and when she realized that's not what we meant, she took it out so a non-published order and then a non-published credit showed up on our bill, which is fine, except along with that is a $9 service charge to change the number at directory assistance! So basically, we were overcharged nearly $50, and more to come.

Our lines were crossed with a radio station's recent-

ly. Well, NYNEX decided they would send a repairman over to our house *without even calling to tell us*, put a recording on our phone line saying "the number you have reached is being checked for trouble" and then charging us for the visit which we didn't request in the first place (and the problem wasn't even in our house)! Think that's it? Nope. Last month we were charged with calls to a certain number which we had never made, $40 worth of them.

What the hell is going on?

Scammed in NY

You've entered the world of NYNEX. Better get used to it.

Advice

Dear 2600:

Some advice to Pestilence, who wrote in the Spring 1995 issue. Quit it. I was busted when I was *fourteen* for using extenders (among other things). It wasn't fun - and it definitely wasn't worth it. I can't imagine what would have happened if I hadn't been a minor.

Fortunate Sun

Dear 2600:

I personally feel that *2600* should revisit its apparent "print it all" policy dealing with letters/ads. For example, there is a seven line help wanted ad from someone who wants someone to write/call him and explain to him what an ANSI bomb is. Another wants you to send $3 to get a copy of an ANSI bomb detection program. I think it's important that as a magazine you help to educate those new to the community, but at the same time keep us from wading through letters every month asking what a red box is, or why a certain person's red box doesn't work. I would at least suggest that right above the address to send letters, you put "RTFM". Just my couple of cents.

Lincoln

We certainly can't pull an ad because we think the person placing it needs to learn more. As for letters, we only print a small fraction of what we receive. And a fraction of those will be from beginners who need some basic answers and pointers, not a harsh rebuff. That comes later.

On ATM's

Dear 2600:

In the article about the ATM's it says *no one* ever watches the camera at any bank.

This is false. I used to have programming classes at a local bank. These classes were taught at the operations center. The guard one day explained what was on his monitors. Since this bank had branches all over Virgina, Maryland, and parts of Tennessee, he had screens of all the local branches (about 15 total). About five were dedicated to the ATM's, and five were for the banks' interior. This black and white screen was showing the ATM's and inside of the bank, switching between each branch. He could call up any camera at will *and* they could do quite a bit of detail. They could show a car's plates across the street.

Kamakize
Virginia

Different banks obviously have different policies concerning cameras. It's possible the cameras you're referring to were focused on the ATM area itself, not the customer. The article was referring to the camera inside the ATM itself.

Spin Control

Dear 2600:

I recently came upon the following information and was wondering if you could shed any light as to its validity. I have tried it in the 810 and 313 area codes from various exchanges and it does return results.

One may dial 107 321 404 988 966 4 to learn whether a Clipper chip is installed on your telephone exchange. When you dial this number, you will get back a recording in a digital voice consisting of:

1. *Your telephone area code*
2. *Your seven digit telephone number*
3. *Nine zeros in three groups of three (000 000 000)*
4. *a pause of a few seconds*
5. *a digit - if this digit is "0" then a Clipper chip has not yet been installed at your exchange. If the digit is "1" then there is a "Federal Government Level" Clipper chip installed. If the number is "2" then there is no "Federal Government Level" Clipper chip present. Any other digit signifies that it is installed.*

Presence of digits other than zeros in the "000 000 000" segment indicate state-level and city-level use.

The Black Panther

Someone should forward this to the Clinton administration so they can see what effect their Clipper chip talk is having on the populace. There is no truth to any of this whatsoever. What you are dialing is a nationwide ANAC number operated by AT&T: (404) 988-9664 but it's only reachable with carrier access code 10732. It's been around for years.

Handy Tip

Dear 2600:

I must thank you for teaching me a new hack that I really didn't have prior knowledge of (hard to believe). The last issue mentioned you can make a special tool by heating the piece in question and melting a forming tool. Obvious it may seem, but it has allowed me to do my work *much* better. One suggestion: use a suitable mould release (I find 15-40 motor oil fine) and be *very* precise with the temperature. Polyethylene for instance forms best at around 300 degrees (that's 500 F for you Americans).

Bilsf
Amsterdam

Address letters to:
2600 Letters
PO Box 99
Middle Island, NY 11953

or internet address:
letters@2600.com

RADIO REVIEWS

by Blue Whale

Several years ago we trekked out to Austin, Texas on an ill-fated journey to witness the Steve Jackson Games trial. While the trial never materialized for us (it was postponed a week, in one of those legal maneuverings that occur for no reason in particular), we did manage to salvage the trip by hanging out in Austin (one of the hippest places around) and by testing out what was then considered some of the best commercial radio equipment available.

Texas is a great place to go scanning, with its endless miles of open road and its military ranges spanning the distance between population centers, and we were prepared with nothing less than Icom's IC-4SRA and Opto Electronics' frequency counter, model 2600, of course. The idea, as I recall, was to catch local frequencies on the Opto and then listen in on the Icom. As it turned out, the Opto turned out to be the weaker link in this radio dyad. First off, to actually get a verifiable frequency you had to watch the LCD while random "background noise" frequencies flashed by. Then, if by chance you happened to spot a number which more or less remained constant, you then had to flip the "hold" switch and hope that the frequency wasn't yet another pager system or birdie or what have you (our model was state-of-the-art; earlier models did not even have this highly prized hold switch). Then, just when you thought you had this little system down, the sun would set and you'd have to break out the night vision goggles to read the LCD in the dark. Needless to say, we ended up breaking that Opto unit in a fit of blind retribution, and dreaming up a wish list of features that we thought the unit should have included.

Enter the Scout

The Scout is the embodiment of everything we wanted on that trip. With this one product Opto has redeemed itself in our eyes. It is truly a hacker's dream. Basically, it's a palm-sized frequency counter with a back-lit LCD that stores up to 400 filtered frequencies and supports reactive tuning and computer interfacing. The unit also has a beep mode and a silent vibrating mode to alert you to frequencies it captures.

Typical operation involves turning the unit on, say, in vibrating mode, putting the unit in your pocket where it vanishes out of sight, strolling around somewhere, and then experiencing the thrill as your Scout occasionally vibrates to alert you to a captured frequency. Unlike our old unit, the Scout utilizes a filter to exclude the random background noise that so irked us out in Texas. Signals must be 10 to 20 dB stronger than the background noise in order to squeak by the filter and register as a frequency (you may, if you wish, turn the filter off, in which case the Scout will function like a normal counter).

What happens when you get a frequency depends upon what mode you're in. If you're in beeper mode, you will hear a beep of course (one beep if the frequency is already in memory; two if it isn't). Additionally, you can set the backlight to switch on for ten seconds (this is very useful when you're in the car, as you may not hear the beeps but you will certainly notice the blue backlight). In vibrating "stealth" mode, the vibrations replace the beeps and you cannot set the backlight to automatically turn on. You may cycle through the frequencies at any time by going into memory recall mode. This will display not only the filtered frequencies you've captured, but how many hits on each frequency (up to 255).

The Scout utilizes an internal NiCad battery that charges fairly quickly, sometimes in an hour. When powering the unit down, you must place it in recall mode in order to keep the frequencies that you've captured in memory. This is by far the most annoying design flaw in the unit. Instead of the Scout defaulting to recall mode, it takes an effort to place the unit in this state. As a result, if you accidentally switch the Scout off (or, as is more often the case, someone you're showing the unit to does) and you do not have the Scout in recall mode, you will lose your frequencies. The Scout must be placed in recall mode each time you want to shut it off with the memory intact, and once you place it in recall mode you cannot use any of its features, so that it's not like you just hit some button when you first get the Scout and forget about it. Basically, everyone I know who owns a Scout has, at one time or another, lost frequencies because of this.

A Note About Models and Versions

The Scout has gone through a number of software and hardware revisions since its original inception. The latest one appears on our bills as "Scout 3.1" which now supports reactive tuning with AOR's AR8000 (a wide range cellular-capable receiver, also reviewed in this article). Version 2.0 will also support reactive tuning with the AR8000 although you will need to use a small battery-sized circuit board in between.

R10A FM Communications Interceptor

While the Scout is certainly worth the $449 you will spend on it, the Interceptor at $359 is questionable. Some people swear by it (see, for example, Thomas Icom's article, *Cellular Interception Techniques*, in the Spring 1995 issue of *2600),* but my own experience leads me to conclude that the Interceptor is not for most people, hackers included. It is definitely not for someone who is thinking of purchasing their first receiver. First off, the Interceptor is not a receiver in the conventional sense. The best way to describe it is to compare it to a frequency counter, only instead of displaying the strongest near-field frequency, you hear the signal deviations. The result is that the Interceptor will automatically "tune" to the strongest signal it encounters, be it AM, narrow FM (NFM), or wide FM (WFM).

In theory you can take your Interceptor with you in the car and listen to all the cellular conversations you want. In practice you will be annoyed and frustrated at your inability to selectively tune the various areas of the spectrum you wish to monitor. If you live in a city or some other highly saturated area, your Interceptor will be practically useless, as all you will get most of the time are pager signals and commercial FM stations. While the Interceptor does come equipped with a skip button that allows you to skip to the next strongest frequency, it is not very effective as strong signals will block out the weaker ones you will invariably wish to listen to. In rural areas, the Interceptor is somewhat more effective, as there are obviously less competing signals.

Finally, I must point out the most annoying quality of the Interceptor, that being its inability to maintain two-way communications signals. Although the latest Interceptor comes with a "delay scan" meant to correct this problem, the fact is that it doesn't work. Thus, the second your local police dispatcher releases his mike, you will lose the signal and once again be listening to pagers or commercial FM or what have you. Pressing the skip button a few dozen times may get you back to the conversation, if only for a brief moment, but who wants to monitor something this way? It's too bad that the Interceptor does not come equipped with that beloved

"hold" switch that is thoughtfully included on Opto's frequency counters.

APS104 Active Pre-selector

Not worth it. At $995, the APS104 is certainly one of the priciest toys you will buy from Opto. The problem is that the features just don't match up. Basically, the APS104 (measuring approximately 7" by 4" by 1.5") goes between your receiver (a Scout or Interceptor or what have you) and your antenna. You then tune a 4 MHz pass band between 10 MHz and 1 GHz by rotating a knob up to ten times. The APS104 will block all frequencies above or below this pass band, resulting in a theoretical increase in range for frequencies that fall within this band.

My problem with the APS104 is its nonlinear analog tuning. When you get your unit, it will come with a custom frequency calibration chart depicting 11 frequencies and their corresponding dial settings for your particular unit. Thus, to tune the center of your 4 MHz wide filter to 825 MHz, you might in fact have to tune to 510 MHz on the dial. Needless to say, using this in a moving vehicle is akin to using the old frequency counters. And if you lose that paper chart out the open window you're out of luck, not that the chart is even remotely useful unless you happen to be interested in those particular frequencies. In a world in which digital tuning is no longer the exception but the rule, Opto should basically let the process of natural selection do its thing and retire this dinosaur. Again, as with all of Opto's products, the documentation for this unit is completely unreadable and unhelpful.

Universal M-400v2 Decoder

Not an Opto product but one which I thought I would mention just the same. As digital signals become more and more common across the radio spectrum, products such as the M-400, which is able to decode many types of signals including pagers, will gain in importance and popularity. Unfortunately, I was not able to acquire a unit for testing. I was, however, able to order an owner's manual from Universal, something I suggest everyone does with every expensive product before ordering the product itself. Just one glance at the manual was enough to confirm my suspicions that Universal is a lot like Opto when it comes to documenting their products. The manual does, however, clarify many of the questions I had concerning the M-400. For example, the unit can only store up to 8K of information, has extremely limited programming capabilities, and does not have a computer interface (although I am told that at least one company is working on such a product, and Universal does sell a similar model that plugs into a PC). So far as I can tell, the only reason that it is called the "M-400" is that it costs $400.

AOR's AR8000 Wide Range Receiver

As with the Scout, the AR8000 is enjoying immense popularity in the hacker world, and rightly so. The most important reason why you should own this $600-650 unit is that it receives 800 MHz cellular imaging loud and clear on its 1400 MHz band, with absolutely no modifications (tune from approximately 1419.9 to 1442.91 MHz in 10 kHz steps). Or, if you prefer, you can interface the AR8000 to a computer and reprogram its EEPROM to unblock cellular, a service which some people are now offering. If you're wondering how AOR can accomplish this with our current laws in place, so am I! In any case, even without these undocumented features, the AR8000 is a great little unit, capable of receiving from 100 kHz to 1900 MHz continuous (less cellular until you reprogram the EEPROM) and in the following modes: AM, USB, LSB, CW, NFM, WFM. Another

noteworthy feature is its ability to store frequencies in non-volatile memory along with eight-character alphanumeric text tags for each frequency. Lastly, the AR8000 does not use costly internal or external NiCads, but four AAs.

APS104 Frequency Calibration

Frequency	Dial Setting
10Mhz	004
27Mhz	013
50Mhz	026
100Mhz	057
150Mhz	076
220Mhz	111
450Mhz	222
600Mhz	325
825Mhz	510
870Mhz	570
1000Mhz	860

The frequencies above were chosen to represent typical communications bands. To tune the center of the 40khz wide filter to the desired frequency, tune the dial to the three digit number shown.

Any device that requires a sheet of paper in order to tune is not worth your time, especially when that device costs $995.

war dialing

by VOM

Living in small towns most of my life it has been hard to find any information on phreaking and related topics. So most, if not all, of what I have learned has been through trial and error and from a select few of other people I have met who share the same interests as I do - namely computers and phone systems.

Also, the town where I live owns the phone company. It is a rare situation and not many other cities own a telco. And up until about 1989 they hardly had any computerization at all and were still using very old equipment.

I had one telco person say there were still some mechanical switches in the CO. I don't know if that was true or not but with Citytel I would not discount it. They completely upgraded their system in 1990 and *everything* is computerized now.

Years ago when I was still in high school I read about a program that would dial numbers sequentially for some mundane purpose. At the time I had just bought a 300 bps modem for an Atari computer I had and was intensely interested in finding computers that I could connect with. Being in a small town in 1983 (under 3000 people), there was no BBS or anything local that I could dial into so everything was long distance. Not knowing a thing about phreaking I figured I could write my own program like the one I read about to dial everything in my prefix area and have it look for computers.

After about a week I had a program in Basic that worked and did what I wanted. I could only dial at night since it was on my parents' line. In about two days the program found a number that answered with a modem.

All I got was a prompt ("login>") when I connected to my mystery number. I tried to get in for a few days but I had no clue as to what it was asking for. I was in the local library and looking at some computer books when I saw the same prompt in a book. It was a Unix machine apparently. Well, after that I started to look for anything that was about Unix. I finally found an ID that got me in - UUCP I think it was. I must say after that little hack I was hooked. I wandered around that system for a few days and read anything I could on Unix. Eventually I found that the computer belonged to the local school board. I told a friend in my computer lab at school what I had found and he went and blabbed it around and the next thing I know I was having a little chat with the principal and a few others from the school board. Needless to say the powers that be freaked when they found what I had done. They did a little audit on their system and found that I had logged in quite a few times over a few weeks.

I knew nothing about hacker ethics at the time but all I wanted to do was learn about computers and other systems so I was careful not to damage their system. I can say all the books and mags that I read helped out quite a bit. I tried to explain that to them but they didn't listen and I was given one month's suspension and my parents were shocked that I could even do such a thing. All my computer stuff was carted away in a box and I was not let near it for about two months. Needless to say I was kinda famous when I got back to school.

I moved away to a larger town of about 16,000 when I finished school and I did not really think about doing any hacking again until I read about the famous Clifford Stoll and his hunt for the German hacker. By then I had an old XT and a 286 and was using a comm program called Qmodem. I

wrote a script in Qmodem's script language that did what my old dialer program did for my Atari.

I found lots of computers over a period of about a week. Lots were open systems with absolutely no security at all. I guess no one thought about hackers and how unprotected their systems are. Also I had learned more about computer systems and networks. Some of the Unix machines I was able to log into and gain root access almost right from the start.

As fate would have it, the first system I found was the local school board and I got system administrator access first try with sysadmin. No password on it at all. I attempted to cover my tracks but did not do a very good job of it and they eventually took the system off line and changed the number. I found it again about a month later and they had upgraded the machine quite a lot. But I didn't do much with it as they were savvy to intruders. But not enough... they still left the system wide open and I got root access almost right away. That really amazed me. After being hacked, they still left the system wide open.

I did find one interesting thing that to this day I don't know what exactly it was for. I found a number that I could connect with and I was trying to get a prompt and suddenly some phone numbers appeared on the screen. I decided to let it run for a while and see what else happened. Over a period of about half an hour new phone numbers would suddenly show up on the screen. One column always had one of four numbers in it and the second column was always a different one. Eventually I figured out that it was something that the phone company had set up that recorded who was calling the police department, fire department, a shelter for battered women, and a small RCMP substation. Nothing spectacular but interesting nonetheless.

I found a computer that controlled a gas cardlock system where you had to use a punch coded card to pump gas. I wondered how to get into it as the prompt was "Password:". The town is not that big so I drove around until I found the one I figured was the one. I looked over the system where you inserted your card and saw a little plate on the side with a serial number. Seeing that, I wrote down the five numbers and went home and called the system. Not really thinking that the serial number was the password, I entered the five digit serial number at the prompt and bingo! I was in. I think it was mostly a fluke that I got in but hey... a fluke is better than not getting in at all. I found I could shut the pump down or give myself free gas if I wanted to but was always afraid of getting caught.

After about three months of getting into every computer I could, I found I got kind of bored of it. Also, this time I told only one other person about what I was doing but it was a fellow who approached me with a number that he had found. I thought of telling others but no one would have really understood anyway what motivated me to get into systems. Mostly curiosity about other systems, how they work, and I guess the challenge of just doing it.

Another reason I stopped was the phone company upgraded their switch so people could have caller ID and all the bells and whistles. I'd still like to do it but I don't know how much of an eye the phone company has on lines these days. Before it was almost nil with the mechanical switches but now their switch is pretty good.

However a few days ago I accidentally dialed a wrong number and got a computer tone. My old hacker curiosity got the better of me and I dialed it again with my modem. To my surprise it was the CityTel switching computer! I got the prompt "Username>" with a banner saying city telephones so I'm assuming it's a Vax but I'm not sure as I hung up fairly quickly and I don't know what they have for security. Too bad... I'd like to see what they've got in there!

I've kind of grown out of it but still think about doing it now and again. But to the point of why I'm mostly writing this. I still have the old Qmodem script that scans prefixes and thought that others might want to use it as they see fit. It's short but it works well. I don't know how any other scanners work but this is the one I made. The only thing is you have to have Qmodem for it to work but it is available in a test drive version probably on most BBS's.

The script is as follows:

```
;Autodialer Script for Qmodem.

clrscr
assign 1 ATDT
assign 9 0

display 'Autodialer Script for Qmodem.'
writeln ' '
writeln ' '
write 'Enter the three digit prefix: '
getn 2 4
writeln ' '
write 'Now enter the four digit starting
    number: '
getn 3 4
writeln ' '
write 'Enter filename to save numbers
    to: '
get 6 20
writeln ' '
write 'Do you want to stop dialing at a
    certain number? (Y/N): '
inkey 4 1
writeln ' '
if '$4' = 'n' go_dial
writeln ' '
write 'Enter the number you wish to
    stop at: '
getn 5 4

turnon online

go_dial:
    displayln 'Now dialing $2-$3'
    pause 2000
    send '$1$2$3^M'

pause 25000; timing for how many
    rings. 25000 is for 20 seconds or
    about three or 4 rings.
if $offline add

gosub save
goto go_dial

add:
    displayln 'No connection made with
        $2-$3'
    hangup
    flush
    incr 3
    if '$3' > '$5' bye
goto go_dial

save:
    displayln 'CONNECTED with $2-
        $3'
    incr 9
    writeln 'Hanging up modem.'
    hangup
    clrscr
    writeln 'Writing number to disk.....'
    pause 3000
    openfile c:\$6 append
    writefile $2$3
    closefile
    writeln 'Done.'
    pause 1000
    clrscr
    flush
    incr 3
return

bye:
    writeln ' '
    writeln 'You connected with $9
        computers.'
    writeln ' '
    writeln 'Terminating Program.'
    exit
```

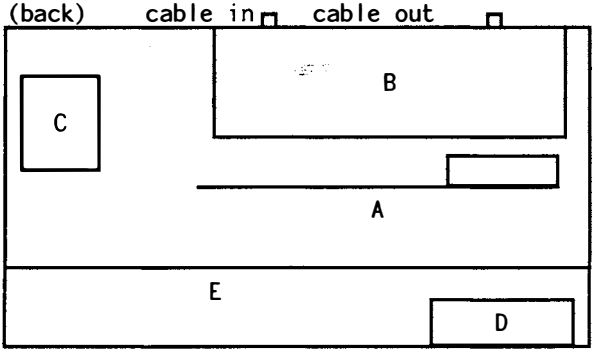
Coping with Cable Denial 2:
The Jerrold 450 Hack

by Prowler

I must commend Cap'n Dave on his excellent review of cable TV operation and equipment in the Spring 94 issue. In this article I hope to provide some methods for coping with cable denial at a low cost. Given the price of cable TV these days, one should be motivated to explore some do-it-yourself methods for receiving cable. You must however be willing to endure the cost of basic cable service.

Basic cable (everything except pay channels) can be received at your house without using a converter box if you have a "cable-ready" TV. If your TV is old or if you order the pay channels, a converter box will be issued for an additional monthly rental charge. You do not, however, have to rent your cable equipment from the company if you purchase your own box. This is actually a cheaper alternative since it will usually pay for itself within a year's subscription of cable. Also, you do not always have to own the most up to date converter box to get the job done. Typically, the boxes issued are the newer type converters which are addressable and descrambling. These are becoming the norm due to the widespread use of newer protection schemes and for access to pay-per-view type channels. It is, however, usually possible to get the same cable access using the older non-addressable and descrambling boxes. Since these boxes are not used much anymore, they can be purchased for a relatively low cost (around $30 to $50).

The difference between the addressable and non-addressable boxes is as follows: Addressable boxes have a unique number and can be programmed by the cable company remotely to control operation. This includes enabling and disabling the descrambling on the converter box. Non-addressable boxes require a chip that determines what channels will be descrambled. This chip is obtained from the cable company with the box when you order your channels. This is a pain for the cable company since the box must be opened and modified to facilitate changes in your cable service. The newer addressable boxes fixed this problem since they never need to be opened to handle any class of cable service. You have probably heard stories about people who order all the pay channels to have their addressable boxes enabled, then unplugging the unit to prevent the box from disabling when they cancel the service. This will leave your box settings on "descramble all" until the cable company turns it off. This is only a temporary fix because most cable companies send out a periodic signal to prevent this sort of thing from happening. This can be once a month or once a day, you can never tell. Basically the computer at the central office looks through the customer database and sends the message "all paying box numbers enable, all other numbers disable." So much for your free cable service. To avoid this, you can always purchase your own addressable box and get the "technician's kit" that is usually labeled "for testing purposes only". What you will get will be a ROM chip that replaces the EEPROM found in the box that stores the cable settings. This ROM of course has all the channels enabled and cannot be reset by the cable company no matter what they do. An ideal solution if you have the money and know what you're doing. An addressable box usually costs about $150 and the kit is around $60. You also must have some experience with electronics and soldering since there are a number of modifications to be made inside the box. This is simply too much of an expense



considering the low cost of non-addressable boxes that can have their descrambling enabled without a costly kit. Not to mention the fact that ordering these kits is suspicious if you don't own some kind of cable service company. The manufactures don't ask but someone could be watching, you never know.

To get yourself started here's what I suggest you do: First, find out what type of boxes that your cable company uses. Check the sticker on the bottom of the box for manufacturer and model. One of the most common manufacturers is General Instrument (GI) and I will be covering these types of boxes. A newer type of GI addressable box is the Impulse model. If your cable company uses these of other types of GI converters you are in good shape. GI also manufactures compatible non-addressable boxes with the model name Jerrold. This is the model you want to obtain. These older boxes are very common and can be ordered from fine publications like *Nuts and Volts.* You can also find these at electronics shows, HAM fests, and other such gatherings. Also, since these boxes are on the way out, you can sometimes find them in a dumpster behind your local cable office. It is not cost effective to keep and repair these boxes when the cable company can rent newer addressable type boxes that provide hassle-free service. So, as cheaply as you can, get yourself a General Instrument Jerrold 450 model. They are identified on the front next to the LED display and have a keypad on the top right.

Once you get a Jerrold 450, hook it up and make sure it works with your cable system. Put your TV on channel 2, 3, or 4 and you should be able to tune in all the cable stations. The pay channels will appear scrambled unless you got lucky and have a "fixed" box. Pay close attention to the scrambled channels. Do you get sound on these channels but a scrambled picture? If so, you will probably be able to get these channels. If the picture and sound is fuzzy (not just scrambled) there is probably a negative trap in use and you will not be able to get these channels without modifying the trap (not recommended). Now that you have your box you must get it open. More often than not, security screws are used to make it a hassle to open the box. What you can do is use a small file to cut a notch in the head of the screw then use a standard flathead to get it off. Or you can just drill out the screws and replace them with normal ones. Incidentally, the screws for common PC cases will fit and are perfect for this job.

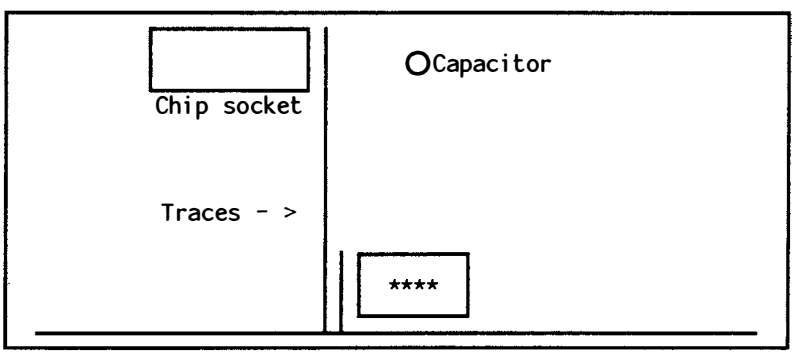
Once you have gotten it open, the inside should look like the above diagram (top view). Obviously, the only component we are interested in is the unscrambler (part

A). It is a circuit board with a small metal box attached to the back. The circuit board is attached with tabs that are inserted through the bottom of the case and then twisted to hold it in place. There are several wires connected to the circuit board, but usually with enough slack to move the board around once freed from the bottom. Use a pair of pliers to twist the tabs back and free the board from the bottom carefully. You do not have to cut wires to get it loose. Once you have it loose, take a look at the front of the board (the component side):

The area with the asterisks (****) is the area of interest. Do not be surprised if the whole board except for the chip socket is covered in blue epoxy. This is done to prevent someone from viewing or modifying the circuit. This, however, does very little once you know where the key point for modification is. In this case, we will be removing components from the circuit board from the spot indicated.

Right next to where the bottom wire connects are four vertically mounted diodes. They start approximately three inches from the left of the board. This will not be evident due to the epoxy coating but you can use the traces shown as a reference. Removing these diodes is the key to permanently enabling descrambling on the box. What you will need to do is carefully use a drill with a grinding bit to remove the epoxy in this area. You will notice that the diodes are covered in a small piece of white cloth. Once you see this, you will know that you are in the right area. If you expose a piece of this, you can sometimes pull the cloth and crack away the epoxy covering the diodes. You could also just grind right through the diodes as long as you do not cut any traces or cut through the whole board! You must be careful, there are traces next to and underneath the diodes. The diodes are right next to one another so once you expose one, the remaining three are easy to find. Once found, use pliers to cut them from the board or simply grind them away. If you accidentally cut through a trace, scratch up either side of it and put a drop of solder in to fix it. Once this is done, you are ready to complete the modification. Obtain a 1N914 diode (very common). You will need to insert this in two of the holes of the chip socket, specifically pins 7 and 8 which are the bottom right holes in the socket. The anode goes into the far bottom right hole (8) and the cathode (side with the black stripe) goes into the hole next to it on the left (7).

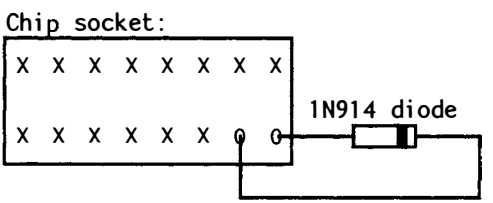
And that's it! Your box is now hardwired into descrambling mode. Put the circuit board back in place and hook up your box. Check to see what channels you are now pulling in. You should be getting one new channel at the very least. Most cable companies use different protection schemes for the different pay channels. Your modified



box may or may not handle all the different protection in use. One problem with the older boxes is that new protection schemes have been created since the time the boxes were designed. This again can be overcome without incurring significant expense.

One feature that the newer addressable boxes have is the ability to handle 12 dB cable signals. The older boxes only handle the 6 dB mode that was standard during their time of manufacture. A new protection scheme was developed that uses an alternating 6 and 12 dB signal and is commonly known as Tri-mode. You may notice this effect when trying to view the pay-per-view channel in your area. It may be unscrambled for one minute and then scrambled the next when the signal goes to 12 dB. What can you do to remedy this situation? Well, it just so happens that a subbox was developed for companies that still used the older boxes but wanted to use Tri-mode signals. This unit is called the Starbase and is also manufactured by General Instrument. These too can be ordered from electronics magazines and are much cheaper than the old converter boxes. This is because they are nothing more than a descrambling unit designed for 12 dB signals. They typically have an AC adapter to power the unit and come in a small flat case designed to sit underneath your converter box. The circuit inside is very similar in design to the one in the box. They also rely on a chip to enable channel descrambling. So, as you can imagine, the Starbase can be modified just like the box. Fortunately the Starbase circuit boards are usually not covered in epoxy. You should be able to immediately see the row of four diodes that need to be cut. Then by putting a 1N914 diode into the chip socket you will have completed the modification. You will then be able to see all cable channels not hindered by an outdoor negative trap, including pay-per-view which will now be on 24 hours a day! Depending on your cable company, a Starbase unit may not be required. In any case, it is a small expense for almost total access to cable.

I feel it prudent to mention that use of a modified cable box is of course illegal and should be taken into consideration. If you're caught using this equipment, the cable company will definitely prosecute. This is due to the fact that they really have no method of determining whether or not you are stealing cable. Most people are caught out of sheer stupidity. I will give you a few examples. One day the cable company decides to unscramble all the pay channels for about 2 minutes. During this time they broadcast a scrambled signal with an advertisement for free merchandise or a contest, etc. Since your box descrambles all signals sent down the line, it will descramble the ad. Lots of stupid people grab the phone and call in to get the merchandise. "Come on down and get your free stuff," says the operator. When you get there what you find is a warrant for your arrest. As a rule, never call in about things you have seen on channels you don't subscribe to. Sounds pretty straightforward right? It's amazing how many people the cable companies bust using this ploy. Another problem is that cable companies have trucks that they send out from time to time to scan



neighborhoods for signal leakage. If you have run another extension in your house and used cheap splitters and connectors, there will be leakage that the trick will detect. Your account will be checked and you could be busted. This could really suck if you're also using a modified box. As a rule, always spend the extra dollar for decent equipment and do the job right. Buying a decent cable signal amplifier is also highly recommended. This prevents the company from accurately determining what you are running inside the house. Even if they check your signal out at the pole, everything will appear normal. Connect one of these first on the line inside your house. Everything beyond it will not be detected. The better the amplifier, the better the protection. Lastly, never leave you cable equipment visible from outside your house. Your neighbors or a passing technician may notice it through a window. This can obviously lead to an uncool situation.

In conclusion, given the wide open structure of cable TV service and the availability of inexpensive equipment, you should be able to come up with a working system regardless of area or cable company. Do some experimenting in your area. Start at the bottom with the cheapest equipment you can get your hands on and see what works. It will usually be determined by the brand the local cable company uses. Anything this company manufactures should be fair game. Your entry level box should be non-addressable with descrambling capabilities. Add-on products for the box will usually be much cheaper than the box itself.

With all this in mind, be careful and happy hacking!

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used towards back issues as well).

A 2600 t-shirt for every article we print.

A voice mail account for regular writers (2 or more articles).

An account on 2600.com for regular writers. (2600.com uses encryption for login sessions and for files so that your privacy is greatly increased.)

2600 Marketplace

Conferences

DEF CON III COMPUTER "UNDERGROUND" CONVENTION. What's this? This is an initial announcement and invitation to DEF CON III, a convention for the "underground" elements of the computer culture. We try to target the (fill in your favorite word here): Hackers, Phreaks, Hammies, Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, Artists, Criminally Insane, Hearing Impaired. WHO: You know who you are, you shady characters. WHAT: A convention for you to meet, party, and listen to some speeches that you would normally never get to hear from some krad people. WHEN: August 4, 5, 6 - 1995 (Speaking on the 5th and 6th). WHERE: Las Vegas, Nevada at the Tropicana Hotel. SPECIAL EVENTS: Hacker Jeopardy, Spot the Fed Contest, Voice bridge, Giveaways, Red Box Creation Contest, Video Room, Cool Video Shit, Scavenger Contest, Who knows? For more information and complete convention details contact the following: World Wide Web: http://underground.org/defcon; FTP Site: ftp.fc.net /pub/defcon; mailing lists: mail majordomo@fc.net with the following statement in the body of your message: subscribe dc-announce; voice or voice mail: 0-700-826-4368 from a phone with AT&T LD, or 10288 it; e-mail: dtangent@defcon.org (The Dark Tangent); snail mail: 2709 E. Madison #102, Seattle, WA, 98112; BBS system to call for info if you don't have net access: 612-251-2511; new DEF CON Voice Bridge: 801-855-3326.

For Sale

DMV DATABASE - 1995 EDITION for the state of Texas. Look up license plates, generate mailing lists, search for missing persons, do demographic research, trace debtors, many other uses! Texas $495, Florida $495, Oregon $219. Mike Beketic, Bootleg Software, 9520 SE Mt. Scott, Portland, OR 97266 (503) 777-2910.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs, or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual .SYS/.COM program. 100% tested on PC, XT, AT, 286, 386, 486 & all DOS's. Only $29 US. Incl: disks, manual. Also: PC background keypress recorder. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to DISK or RAM. Also stores key-press timings, & key-hold duration. Can identify what's typed, when, & by *whom* (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite, GPO Box 343, Sydney NSW 2001 Australia.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector: ANSICHK9.ZIP. Send $3 to cover shipping and handling to Patrick Harvey, 710 Peachtree St. NE #430, Atlanta, GA 30308.

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes selected shareware catalog and restricted book catalog. Send $1 ($1.50 for 3.5) and 2 stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

LOOKING FOR A LINEMAN'S HANDSET? We have rotary for $65 (US). Great for use with your tone dialer. Send your order to Durham Technical Products - P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@sdf.lonestar.org). We also carry 6.5000 mhz crystals for $4 apiece; three or more crystals only $3 each. Also available: 8870 or SSI-202 DTMF decoder IC's or M957 receiver IC $4; 556 timer IC's for $1.50; 555 timers for $1.00. Cash, check, or money order accepted. (There is a short delay for checks to clear.) A current parts flyer is available by snail mail or e-mail.

VIDEO "HOW TO BUILD A RED BOX". VHS 72 min. Complete step by step instruction on how to convert a Radio Shack tone dialer into a red box. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! Best investment you'll ever make! Only $29 US. $5 for shipping & handling. DIGITAL RECORDING KEYCHAIN. Records ANY tone you generate onto chip. Very small. Fits in pocket for easy access. 20 second capacity. Includes 3 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300, 156 Sherwood Place, Englewood, NJ 07631.

LOWEST PRICES on underground information including: phreaking, hacking, cellular, anarchy, and too many other subjects to list. Send $1 (cash) for current catalog. Byte Bandits, PO Box 861, No. Branford, CT 06471.

"THE MAGICAL TONE BOX" - FULLY ASSEMBLED version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size & only 1/4 inch thin!. Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. Only $29, 2 for $55, 4 for $102. Send money order for 2nd-day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & insurance. "THE QUARTER" DEVICE - complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 volt battery &

wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S., add $12 per order in U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

INFORMATION IS POWER! Arm yourself for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supplement you with files, programs, manuals, and membership from our elite organization. Legit and recognized world-wide, our information resources will elevate you to a higher plane of consciousness. Send $1 for a catalog to: SotMESC, Box 573, Long Beach, MS 39560.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

UNAUTHORIZED ACCESS. The hacker documentary by Annaliza Savage, as reviewed in 2600 Winter 93-94 issue now available from Savage Productions, Suite One, 281 City Road, London EC1V 1LA, U.K. with a cheque or money order for $25.00 or 15 UK Pounds. NTSC VHS unless otherwise requested.

Info Exchange

DATA INTELLIGENCE CORE (503) 697-7694. An information exchange for intelligence matters. Handles H/P/A subjects as well as espionage. Need information on Russian Intelligence. Send e-mail to idres6e7@pcc.edu.

INFO EXCHANGE. Please send any hack/phreak/scam/controversial info. Especially looking for info that is relevant to the United Kingdom. Need info to start UK hack mag. Send info and return address (not compulsory) to: London Underground c/o Terry Boone, 120 Chesterfield Rd., Ashford, Middlesex, TW15 2ND, England.

WANTED: Any information on cable hacking or ANSI bombs. I need to know what exactly an ANSI bomb does, where I can get one, and how it works. Also need any other BBS or cable hacking info. Will exchange knowledge with anyone. Send info to The Dominus, 4302 West Azeele St., Tampa, FL 33609-3824. Will exchange knowledge!

NEW ENGLISH HACKER requires contacts in order to learn and explore the arts of hacking and phreaking, will provide a 100% reply to any other hackers who will take the time to reply and supply information. Send all correspondences to: The Net_Jester, 16 Frida Cres, Castle, Northwich, Cheshire, CW8 1DJ, England.

Help Wanted

MINNEAPOLIS/ST. PAUL BUSINESSMAN would like to discuss a business venture with "top gun" hacker and/or surveillance expert on a consulting fee basis. In confidence please forward a note profile to: Robert, P.O. Box 27401, Golden Valley, MN 55427-0401

NEED HELP WITH COLLEGE TRANSCRIPTS. Please respond telephonically (334) 887-8946.

WANTED: Articles for a NEW newsletter. Hopefully one by-line will be "Darker Shades of Gray" written only by citizens convicted of at least a misdemeanor. Then maybe a back page closer by an incarcerated felon entitled something like "Definite Black" or "In The Dark". Need manual so I can learn to use a telephone lineman's test set. Small blue metal box. Western Electric 145A Test Set. Send all submissions to: PO Box 30286, Memphis, TN 38130.

NEED HELP TO CLEAR MY CREDIT REPORTS. Please respond to: PO Box 32086, Panama City, FL 32407-8086.

Hacker Boards

ANARCHY ONLINE - A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Telnet: anarchy-online.com. Modem: (214) 289-8328.

TOG DOG, Evil Clown of Pork BBS, you saw us at HOPE - now call us and experience a professional, freedom-based BBS! H/P texts, PC demos, coding, free Internet newsgroups, and e-mail. No charges/ratios! 28.8, 24hrs (313) TOG-1-DOG, automated info from info@togdog.com.

UNPHAMILIAR TERRITORY WANTS YOU! We are a bulletin board system running out of Phoenix, AZ and have been in operation since 1989. We serve as a system in which security flaws, system exploits, and electronic freedom are discussed. There is no illegal information contained on the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those wily computer hackers. We call this "neutral territory" and we have been doing this for 4 years. Since 1991, we've had security officers from Sprint, MCI, Tymnet, various universities and branches of the government participate. We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested, please send mail to: imedia@tdn.net.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 8/15/95.

YOU DON'T NEED ENCRYPTION TO BLOW UP A bomb. That's the lesson the Clinton administration seems to be having trouble learning. Almost immediately after the Oklahoma City bombing, there were cries on Capitol Hill for "broad new powers" to combat terrorism. According to FBI Director Louis Freeh, one of the biggest problems facing us today is that of criminals communicating on the Internet using encryption. "This problem must be resolved," they say. According to White House aides, Clinton will seek new FBI powers to monitor phone lines of suspected terrorists as well as more access to credit and travel records. Under the proposal, authorities will be able to do this without evidence of a criminal act underway or in the planning stages. Under the current situation, a lot of people are supporting this kind of a move without considering the consequences. Once such measures are undertaken, they have a history of being abused. In a land where tabloid television describes hackers as "computer terrorists", we wonder if the government is that far behind. After all, our own Bernie S. (see page 4) was denied bail, at least in part because he owned books that explained how explosives worked. With this kind of hysteria dictating enforcement, we shudder at the results of these proposals. In the case of Oklahoma City, one fact remains very clear. None of this would have helped. The suspects weren't significant enough to be noticed. And they didn't use encryption or the net at all. And yet, the tabloids are screaming about the shocking speech that can be found on the Internet and how something has to be done to stop it. But curtailing speech and liberty never advances the cause of freedom and once begun is very difficult to reverse. Considering that it had no difficulty speaking out against the recent Communications Decency Act which seeks to outlaw objectionable material over computer networks, the Clinton administration really should know better.

ENCRYPTION HAS ALREADY BEEN EFFECTIVELY outlawed in Russia. An edict entitled "On Measures to Observe the Law in Development, Production, Sale, and Use of Encryption Devices and on Provision of Services in Encrypting Information" restricts the use of encryption technologies by government agencies as well as private entities. The edict bans the development, import, sale, and use of unlicensed encryption devices, as well as "protected technological means of storage, processing, and transmission of information". It's widely believed that this came about because of FBI influence abroad.

IT'S NOW ILLEGAL TO OWN A SATELLITE TV DISH in Iran. Saying the dishes are the equivalent of waving American flags, the government hopes this move will "immunize the people against the cultural invasion of the West." We think that same cultural invasion inspired this short-sighted overly hysterical reaction. It's not quite as stupid as outlawing listening to the radio. But it's close.

HERE'S ONE YOU WON'T SEE IN A PHONE COMPAny ad: Caller ID used successfully *by* a criminal *against* a victim. That's right! A San Antonio woman was allegedly shot to death by her exboyfriend earlier this year after he used a Caller ID box to track her down. It seems she called him to talk from a male friend's house and that in addition to the phone number being sent out, the caller's name was as well. All that was needed at that point was a phone book. Since we've done such a good job teaching our children and society the importance of 911, maybe it's time we started teaching them about *67.

IN ENGLAND, HOWEVER, BRITISH TELECOM IS reporting a 21 percent drop in "malicious" calls due to their version of Caller ID known as Caller Display. Says BT, "Our technology not only helps create a more efficient and convenient world but is helping our customers feel safer." Customers are also using the British Call Return feature at a rate of three million calls a day. Callers dial 1471 and hear the number of the person who called them last for no charge.

THE CALL RETURN FEATURE IN CANADA HAS sparked some controversy. The CRTC (the regulatory commission governing phone companies) has ordered all of Canada's local phone companies (BC Tel, AGT, Bell Canada, MT&T, NB Tel, and Newfoundland Tel) to stop Call Return from functioning on calls that have been blocked.

LAST ISSUE WE REPORTED ON THE DIFFICULTY NYNEX was having with its All-Call Restrict feature. Some phones that were supposed to have it didn't. (We were one of those.) Now it seems that NYNEX can't even handle a simple call trace without causing a major incident. Within hours of the Oklahoma City bombing, someone called in a bomb threat to a Boston hospital. NYNEX traced the call to the wrong number, thanks to an employee error and a pol-

icy of not doublechecking. Now NYNEX is offering to pay the college tuition of the innocent kid who spent two days in jail as a result.

IT COULD HAPPEN AS SOON AS EARLY 1996. Residential customers in New York City and Long Island will have a choice between NYNEX and Cablevision's Lightpath. Consumers would be able to switch services without switching numbers. Lightpath has been providing phone service to business customers on Long Island. Of course, the flipside of this is that NYNEX will now enter the cable TV business, something we're not sure the world is ready for.

THE PRESS RELEASE GOES SOMETHING LIKE THIS: "You no longer need to carry a pocketful of quarters. With NYNEX's new European-style payphones, all you'll need is a phone card." Trouble is, these phones are beginning to pop up everywhere in New York City streets, replacing existing "real" payphones. This wouldn't be a problem in itself except the phones have three strikes against them: they don't allow calls to 800 numbers, they don't allow calls to 950 numbers, and they don't take incoming calls. One thing that isn't lacking is the NYNEX greed factor: if they aren't making money every minute the receiver is off the hook, they'll make the phone completely unusable.

AT&T'S NEW 500 NUMBER SERVICE HAS ITS pluses and minuses. While you can make calls from anywhere using your master PIN, you will be stuck with a hefty 80 cent surcharge. If the number you're calling is your home number, you can avoid this surcharge by using one of the non-master PINs that you're supposed to give out to your friends and family. Hopefully you won't be committing a federal crime by engaging in this practice.

U.S. WEST HAS TAKEN A BIG STEP TOWARDS MAKing phone rates a bit more realistic. For one dollar, payphone callers in Northern Oregon can make a call within the region and stay on the phone for as long as they like. The same rate applies for calling card and collect calls. The calls are made by dialing 1+503 or 0+503 before the number. Local calls are still a quarter.

IN A DISTURBING LITTLE BIT OF REVISIONISM, we've noticed that scanners with 800 mhz capability, while still illegal to buy, are now defined as "for government use only" in advertisements. Anyone working for a governmental agency who files the proper paperwork is entitled to buy one of these devices and presumably listen to the frequencies that have been denied to the rest of us.

GOVERNMENT RAIDS ON 24 SPY SHOPS AROUND the country were designed to keep certain pieces of technology out of the hands of private citizens. Advanced surveillance equipment such as transmitters hidden in pens are illegal for average citizens to own. Only law enforcement agencies are allowed to have those kind of devices. In fact, the federal agents who made the busts were using those very devices to gather evidence.

IT'S OFFICIAL. THE TRIAL OF KEVIN MITNICK begins July 10 in Raleigh, North Carolina. He will be facing a 23-count indictment, allegedly for making cellular phone calls on a cloned phone. Each of the federal counts carries a sentence of 20 years. Assuming Mitnick doesn't receive a 460 year sentence, the feds have indicated that they will bring him up on charges in other locations as well (San Francisco, San Diego, Denver, Colorado, and Seattle). Every single one of these charges is directly related to the fact that Mitnick was trying not to be captured. So why was he running in the first place? We may finally have an answer. In 1992, Mitnick was employed by Teltec Investigations, a company that was being investigated by Pacific Bell. According to a source, when the company was contacted, they agreed to testify against Mitnick in exchange for leniency. The focal point of the entire investigation was the unauthorized accessing of Pacific Bell voice mail. Since Mitnick was on probation at the time and since any probation violation could easily result in prison time, he chose to leave. And that's really the whole reason why this wild chase happened in the first place. Either he accessed a voice mail system without permission or someone else in the company did and decided to make him the fall guy. Either way, the punishment far outweighs the crime, if, in fact, there ever was a crime. And in Mitnick's case, the punishment has already been handed down - he lived a fugitive's life for years, never knowing when or if his freedom would suddenly expire. We can only hope this side of the story is told at the trial.

ANYONE WISHING TO SEND MAIL TO KEVIN MITnick can do so by emailing kmitnick@2600.com. We will forward the mail to him on a regular basis. Please remember that prison authorities read all incoming mail.

THE COMPLETE NPA LIST

We thought it was about time somebody put together an updated area code list complete with all of the new, weird area codes that have been announced so far. Some of these are so new that they don't even work yet. In the case of area code splits, we listed the originating area code next to the newer one. If the area code wasn't formed from a split, the year of its creation is listed. This information is accurate to the best of our knowledge. Please let us know if you spot any errors or omissions.

NPA	ORIGIN	LOCATION
201	(1952)	NEW JERSEY
202	(1952)	WASHINGTON DC
203	(1952)	CONNECTICUT
204	(1952)	MANITOBA
205	(1952)	ALABAMA
206	(1952)	WASHINGTON
207	(1952)	MAINE
208	(1952)	IDAHO
209	916	CALIFORNIA
210	512	TEXAS
212	(1952)	NEW YORK
213	(1952)	CALIFORNIA
214	(1952)	TEXAS
215	(1952)	PENNSYLVANIA
216	(1952)	OHIO
217	(1952)	ILLINOIS
218	(1952)	MINNESOTA
219	(1952)	INDIANA
250	604	BRITISH COLUMBIA
281	713	TEXAS
301	(1952)	MARYLAND
302	(1952)	DELAWARE
303	(1952)	COLORADO
304	(1952)	WEST VIRGINIA
305	(1952)	FLORIDA
306	(1952)	SASKATCHEWAN
307	(1952)	WYOMING
308	402	NEBRASKA
309	217	ILLINOIS
310	213	CALIFORNIA
312	(1952)	ILLINOIS
313	(1952)	MICHIGAN
314	(1952)	MISSOURI
315	(1952)	NEW YORK
316	(1952)	KANSAS
317	(1952)	INDIANA
318	504	LOUISIANA
319	(1952)	IOWA
330	216	OHIO
334	205	ALABAMA
340	809	PUERTO RICO
360	206	WASHINGTON
401	(1952)	RHODE ISLAND
402	(1952)	NEBRASKA
403	(1952)	ALBERTA
404	(1952)	GEORGIA
405	(1952)	OKLAHOMA
406	(1952)	MONTANA
407	305	FLORIDA
408	415	CALIFORNIA
409	713	TEXAS
410	301	MARYLAND
412	(1952)	PENNSYLVANIA
413	(1952)	MASSACHUSETTS
414	(1952)	WISCONSIN
415	(1952)	CALIFORNIA
416	(1952)	ONTARIO
417	(1952)	MISSOURI
418	(1952)	QUEBEC
419	(1952)	OHIO
423	615	TENNESSEE
441	809	BERMUDA
456	(1995)	INTERNATIONAL INBOUND
500	(1994)	PERSONAL COMMUNICATIONS
501	(1952)	ARKANSAS
502	(1952)	KENTUCKY
503	(1952)	OREGON
504	(1952)	LOUISIANA
505	(1952)	NEW MEXICO
506	902	NEW BRUNSWICK
507	612	MINNESOTA
508	617	MASSACHUSETTS
509	206	WASHINGTON
510	415	CALIFORNIA
512	(1952)	TEXAS
513	(1952)	OHIO
514	(1952)	QUEBEC
515	(1952)	IOWA
516	(1952)	NEW YORK
517	(1952)	MICHIGAN
518	(1952)	NEW YORK
519	416	ONTARIO
520	602	ARIZONA
522	500	PERSONAL COMMUNICATIONS
533	500	PERSONAL

		COMMUNICATIONS
540	703	VIRGINIA
541	503	OREGON
544	500	PERSONAL COMMUNICATIONS
562	310	CALIFORNIA
566	500	PERSONAL COMMUNICATIONS
577	500	PERSONAL COMMUNICATIONS
588	500	PERSONAL COMMUNICATIONS
600	--	CANADA (TWX)
601	(1952)	MISSISSIPPI
602	(1952)	ARIZONA
603	(1952)	NEW HAMPSHIRE
604	(1952)	BRITISH COLUMBIA
605	(1952)	SOUTH DAKOTA
606	502	KENTUCKY
607	315	NEW YORK
608	414	WISCONSIN
609	201	NEW JERSEY
610	215	PENNSYLVANIA
612	(1952)	MINNESOTA
613	(1952)	ONTARIO
614	(1952)	OHIO
615	901	TENNESSEE
616	(1952)	MICHIGAN
617	(1952)	MASSACHUSETTS
618	(1952)	ILLINOIS
619	714	CALIFORNIA
630	708	ILLINOIS
700	--	IC SERVICES
701	(1952)	NORTH DAKOTA
702	(1952)	NEVADA
703	(1952)	VIRGINIA
704	(1952)	NORTH CAROLINA
705	613	ONTARIO
706	404	GEORGIA
707	415	CALIFORNIA
708	312	ILLINOIS
709	902	NEWFOUNDLAND
710	--	U.S. GOVERNMENT
712	(1952)	IOWA
713	(1952)	TEXAS
714	(1952)	CALIFORNIA
715	(1952)	WISCONSIN
716	(1952)	NEW YORK
717	(1952)	PENNSYLVANIA
718	212	NEW YORK
719	303	COLORADO
760	619	CALIFORNIA
770	404	GEORGIA
800	--	TOLL FREE SERVICES
801	(1952)	UTAH
802	(1952)	VERMONT
803	(1952)	SOUTH CAROLINA
804	703	VIRGINIA
805	213	CALIFORNIA
806	915	TEXAS
807	613	ONTARIO
808	(1957)	HAWAII
809	(1958)	CARIBBEAN ISLANDS
810	313	MICHIGAN
812	(1952)	INDIANA
813	305	FLORIDA
814	(1952)	PENNSYLVANIA
815	(1952)	ILLINOIS
816	(1952)	MISSOURI
817	214	TEXAS
818	213	CALIFORNIA
819	514	QUEBEC
822	800	TOLL FREE SERVICES
833	800	TOLL FREE SERVICES
844	800	TOLL FREE SERVICES
847	708	ILLINOIS
850	904	FLORIDA
860	203	CONNECTICUT
864	803	SOUTH CAROLINA
866	800	TOLL FREE SERVICES
877	800	TOLL FREE SERVICES
888	800	TOLL FREE SERVICES
900	--	PAY SERVICES
901	(1952)	TENNESSEE
902	(1952)	NOVA SCOTIA/ P.E.I.
903	214	TEXAS
904	305	FLORIDA
905	416	ONTARIO
906	616	MICHIGAN
907	(1957)	ALASKA
908	201	NEW JERSEY
909	714	CALIFORNIA
910	919	NORTH CAROLINA
912	404	GEORGIA
913	(1952)	KANSAS
914	(1952)	NEW YORK
915	(1952)	TEXAS
916	(1952)	CALIFORNIA
917	212/718	NEW YORK
918	405	OKLAHOMA
919	704	NORTH CAROLINA
941	813	FLORIDA
954	305	FLORIDA
970	303	COLORADO
972	214	TEXAS

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

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

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

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

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

University Circle Arabica.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Nashville

Bellevue Mall in Bellevue, in the food court. (615) 646-9020, 9027, 9050, 9089.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Ottawa, ONT (Canada)

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

Philadelphia

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

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644.

San Francisco

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

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

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 and phone number at (516) 751-2600 or send email to meetings@2600.com.

LAST CHANCE

NO, WE'RE NOT RAISING OUR PRICES. (WE'LL LET YOU KNOW.) THIS IS A DIFFERENT KIND OF LAST CHANCE. WE HAVE DECIDED, AFTER MUCH DEBATE, TO CHANGE THE DESIGN OF OUR T-SHIRTS. THIS MEANS THAT ONCE WE GET RID OF THE CURRENT BATCH, THERE WON'T BE ANY MORE. IF YOU'RE ONE OF THE LUCKY FEW WHO MANAGE TO SAVE ONE OF THESE, WE'RE CERTAIN YOU'LL BE ABLE TO RESELL IT IN THE FUTURE FOR THOUSANDS OF DOLLARS. SO DON'T BE A FOOL. ORDER YOUR SHIRT TODAY BEFORE IT'S TOO LATE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND, BLUE BOX SCHEMATIC ON THE FRONT, CLIPPINGS ON THE BACK.

YES! I'D BE A MORON NOT TO TAKE:
❑ 1 shirt/$15 ❑ 2 shirts/$26 SIZE: ____

NO! LEAVE ME ALONE. BUT SIGN ME UP FOR:

INDIVIDUAL SUBSCRIPTION
❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION
❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION
❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION
❑ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)
❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25
(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)
(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953
(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED:

Payphones of the Planet

CUBA

Here's the scene straight from Havana. If you're up to it, the "bubble" phone has some exposed wires for the international boxer in us all.

Photos by Arclight

RUSSIA

Somehow this one works to this day.

Photo by Warlock

ETHIOPIA

This shiny red beacon is used by people standing outside the Accident Investigation Department.

Photo by G.T.