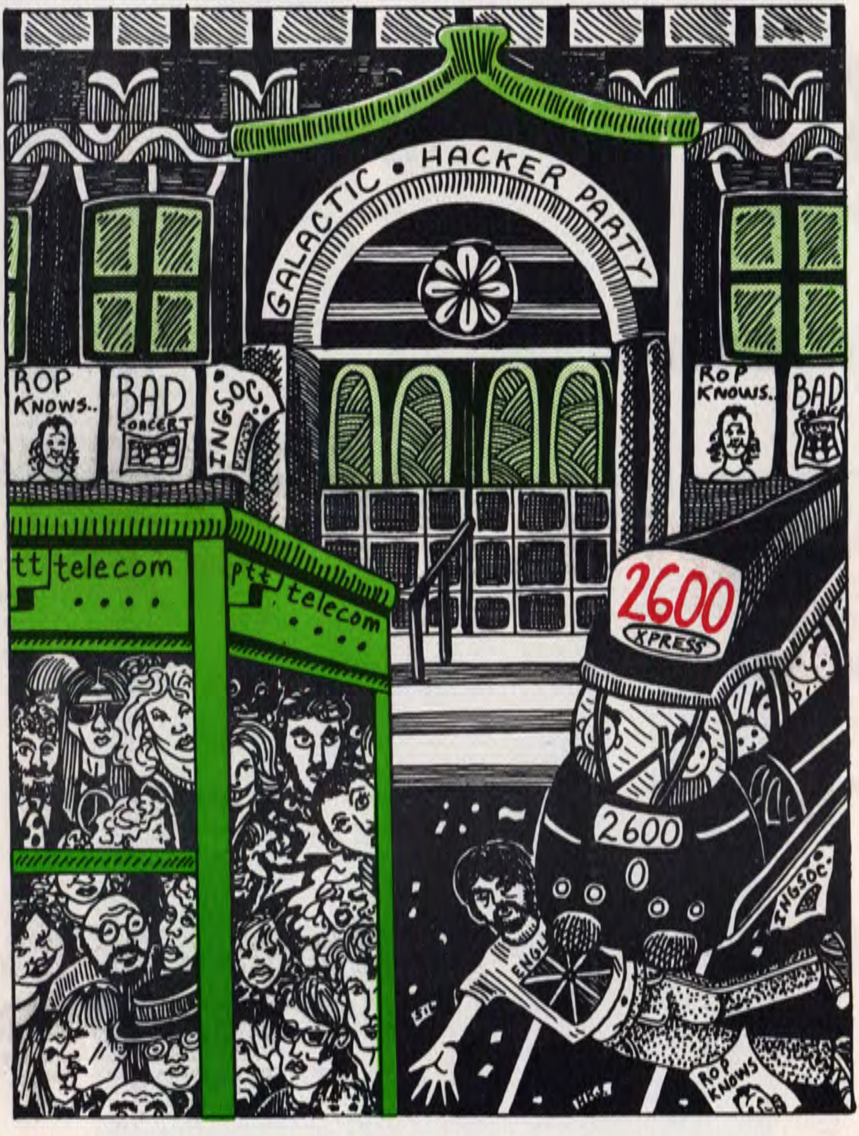
2600

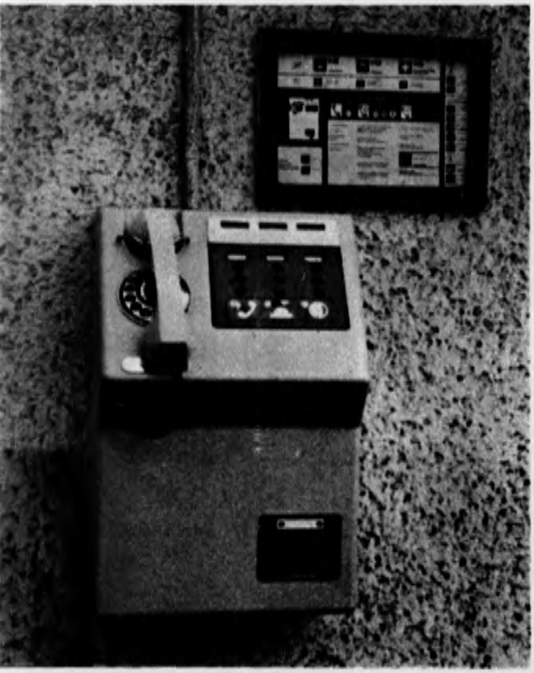
The Hacker Quarterly

VOLUME SIX, NUMBER THREE
AUTUMN, 1989



COMMUNIST PAYPHONES

Seen in the streets of East Berlin



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

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988
at $25 per year, $30 per year overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.

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

Competition... It's the next best thing to being there.

We've just about had it with this NYNEX/New York Telephone strike. Since early August we in the New York region have been living with substandard service, long delays getting through to information, non-responsive repair service, a suspension of new orders, 50 minute waits for service reps after interminable busy signals, and payphones that never seem to work.

Here's an exchange one of us had while trying to reach a service rep. One hour before closing, busy signal. Three phones were set to redial mode, each trying the same number. After half an hour, success! A ring, then a recording. "Due to the work stoppage, there will be a slight delay answering your call. Please hold on, etc." The announcement repeated every minute. Finally, at one minute before closing, a human being came on the line. "Hello I can't hear you," they said. "What?!" we asked incredulously. "I said I can't hear you." Click. We redialed. Sure enough, we were connected to their after-hours recording. Please call back when we're open. Right.

It gets worse. After going through about a dozen payphones in the streets of New York without a single one working properly, after losing 75 cents trying to make a local call, the New York Telephone operator suggests we place the call using a calling card. "I can't access the billing information because of the strike," she said. "But I do know the surcharge is only 45 cents."

New York Telephone has this incredible habit of fixing their own faults by charging you extra. Another example centers on our fax machine, which, according to our AT&T bill, was calling people in Delaware and staying on for 15 minutes. When we started hearing from people who were trying to send us faxes but were instead

continued on page 9

Grade "A"

by The Plague

What Is UAPC?

UAPC stands for University Applications Processing Center. This is a computing and data processing facility that deals with academic record keeping and processing. One of their jobs is to process student applications for CUNY (City University of New York) schools. Another job, and this is the part that interests us most, is to process student records for the New York City public high schools.

Nearly all New York City public high schools are connected to UAPC. There are 116 public high schools in New York City (with several hundred thousand students). The reasons for interconnection are obvious. If every school had its own student data storage computer, its own proprietary software, and its own staff trained on that particular system, the cost would be too great. Not only that, but data transfer and statisical analysis would be impossible for the school system as a whole. As an example, there would be much paperwork, chaos, and confusion just to transfer a student from one school to another. Computing the drop-out rate and other valuable statistics like standardized test scores would involve every school sending in reports generated by its own computer system, and hence more paperwork, more bureaucrats, and more confusion.

So now you understand why all NYC high schools are linked by modem to this one computer. All grades, attendance, course records, and schedules for every New York City high school student are stored and processed at UAPC.

Where is UAPC?

UAPC is located in Brooklyn at Kingsborough Community College (across from Sheepshead Bay at the far end of Manhattan Beach). The actual computers and personnel are in Building T-1 (or simply building ONE). If you happen to go trashing there sometime, building T-1 is a one-story tan colored aluminum shed. It looks sort of like a gigantic tool shed. Above the entry door is written "ONE" in large black plastic lettering. By the way, you're allowed to go in. Nobody is going to check ID or anything like that. If you look like a student, no problem. The reason for this is that T-1 connects to T-2, another shed (blue in color) which has many classrooms. The actual UAPC office is directly to your right as you enter T-1.

In each New York City high school, there is something called a "program office". This room usually contains terminals and big printers and it's where each school creates class schedules for teachers and students, among other things. The staff that work in these offices are trained at UAPC.

> ***"If you go to a New York City public high school, the chances are 95 percent that your school is on UAPC."***

Technical Information about UAPC

Enough background; here's the scoop. UAPC computers run on IBM mainframes (IBM 370 and 3090). The virtual operating system that is used is MVS (which is much like the familiar VM/CMS). On top of MVS runs Wylbur (pronounced will-burr, not while-birr), which is sort of like a command shell plus a batch language plus an editor all rolled into one. On top of Wylbur, run the actual applications (jobs) for processing of grade files.

There are several applications for various tasks (entering grades, entering attendance, class scheduling, generating transcripts, and various other reports). These applications are written in a batch-like language and are stored on disk in source code format. The reason for this is that each school has its own way of doing things (i.e., naming conventions for classes and sections), and the batch programs can be modified by either UAPC or qualified people who work in each high school's program office. These applications are submitted to run on the IBM machines with the JCL code appended at the top of each application.

Each school connects to UAPC via a terminal and modem and each school is allocated its own directory (or library as the batch-heads call them) on the system. This directory contains the applications (jobs) that the school uses each day for various activities. Data files are also contained in these directories. The data files are in a pretty-much IBM standard format (although stored in EBCDIC instead of ASCII). Input records for each application are usually fed in using punch-cards or scan-tron type readers at the local school. If you've ever gone to a New York City high school you'll know what I mean: the attendance punch-cards are brought down each day from each homeroom to the program office. Also, each teacher would fill in attendance forms (used to detect class-cutting) using a number 2 pencil. These forms look like the test forms for the SAT's.

Sometimes, however, input is entered manually at the terminal in the program office, usually for query type jobs. For instance, if one student lost his class schedule and wanted a replacement, he would have to go to the program office and ask for one. They would run that application on the terminal, print up a schedule for that student, and give it to him.

How do you know if your school is on UAPC?

If you go to a New York City public high school, then the chances are 95 percent that your school is on UAPC. If you are not sure, look for the telltale signs at your school. Does your homeroom teacher use punch-cards? Is your transcript laser-printed on white paper and divided into nice columns grouped by academic subject? Does your school's program office contain terminals and printers? Is your class schedule (a.k.a. program card) printed on 5.5" x 7" paper (either heavy-bond white or thin-bond blue)? Is your grade report (a.k.a. report card) printed on computer paper, about 5.5" high (regular width) with a blue Board of Ed logo in the middle, with explanation of grades (in blue) on the back? Do you get little yellow or white laser-printed cards in the mail when you play hookey or cut classes? Any of these sound familiar, boys and girls? They should, because almost every New York City public high school fits all these categories. If your school fits any of these (especially the punched cards and terminals in the program office), then you can be sure that your grades are lurking somewhere in the bowels of UAPC.

Logging on to UAPC

To get on, you're going to need a dial-up. It's not too much work getting the dial-up, if you do a little snooping and trashing around the program office at your school, you should find it written down somewhere. However, I will save you some time and tell you that there are at least 12 dial-ups for UAPC in the 718-332-51XX number range and several in the 718-332-55XX range. There are many more elsewhere (usually exchanges local to Kingsborough Community College).

You should only connect to UAPC on school days during valid school hours. You can connect to UAPC at either 300 or 1200 baud. However, in an effort to thwart people for finding their dial-ups, UAPC will not print anything to the screen unless you connect at the right format and hit a few of the right keys. Therefore, you should use the following procedure in order to connect: Call at 300 or 1200 baud, using 7 data bits, even parity and 1 stop bit (7E1), and local echo (or half duplex). Once connected, hit the RUBOUT/DELETE key (ASCII code 127 or 255 [hex $7F or $FF]) three times, and then hit return twice. You will be greeted with the

Grade "A"

following:

```
UAPC MVS390A LINE — 10-TEN 11:59:02
03/22/89

11:59 Wednesday 89-03-22
You are signed on to U.A.P.C. Have a
good day.

TERMINAL?
```

When you are prompted for the terminal, just enter a letter-two-digit combination (A99 works just fine).

You will then be prompted for "USER?", which is your school's login ID. The format for the username is $HSxxn, where xx is a two-letter abbreviation for your school's name, and n is a digit from 1 through 9, indicating the particular account used by the school. N is usually 1, 2, or 3. An example of a user ID is $HSST1 or $HSST2 which are the user ID's for Stuyvesant High School in Manhattan.

You can guess at your school's user ID (it's easy enough, for instance Sheepshead Bay High School would be $HSSB1 or South Shore High School would be $HSSS1, etc.), but a better way is to pick up the trash from the program office. You should find stacks of green and white printer paper that is 132 columns in width. The user ID will be almost everywhere throughout most printouts generated. Remember to look for the $HSxxn format.

After entering a valid user ID, what you will see next depends on several things. Normally you should see the "PASSWORD?" prompt, but on some accounts you may also see a "JOB?" or "KEYWORD?" prompt. This simply depends on the school, however 90 percent of the accounts only ask for the PASSWORD. The JOB and KEYWORD are simply additional passwords. However, every user ID has a PASSWORD on it. Usually only $HSxx1 accounts have JOB or KEYWORD passwords. However most schools have several accounts (usually 2 or 3), and the $HSxx2 and $HSxx3 will usually have only the "PASSWORD?" prompt. There is no difference in access privilege between the various accounts at each school. They are simply there so that more than one terminal at each school can be logged in at the same time.

Getting The Password

Naturally, you're going to need the password if you are serious about doing anything with UAPC. There are several options here. However, one option that I would not recommend is that you attempt to hack the password by brute force. UAPC has a nasty habit of allowing you 4 attempts at the password before it disables that account and notifies the security dudes at UAPC. If you disable your school's account, your school's program office must call UAPC by voice in order to reactivate it. There is a way around this, if you really want to brute-hack the account. After three password attempts, you should hang up and redial, and then do another three attempts, and so on. This will keep the counter from ever reaching 4 and disabling the account. Although it's a pain in the neck, there isn't much we can do about it. However, if you have no plans of ever getting into UAPC and just want to annoy your school, simply log on as them early each morning and disable their password. This will give them a headache to say the least, having to call up UAPC each day to reactivate their password.

Other ways of getting the password include our old favorite, social engineering. Here there are two options. You can attempt to engineer UAPC by voice, thus saying that you are the school and that you need the password. Conversely you can attempt to engineer the school by calling the program office by voice and saying that you are from UAPC and that you need them to change their password to a diagnostic password which you will so kindly provide. If you're going to do social engineering, make sure you get some valid people's names at either UAPC or at your school.

Yet another way to get the password is to do what was done in Wargames, snooping around the program office. They usually do not have the password written down. But, and this is important, you can get the password if you can somehow manage to look over the shoulder of the terminal operator when he/she is logging in. Remember, they connect to UAPC at half duplex, and thus keys are echoed locally, meaning that you will see the password on the screen as it is typed. I know this for a fact.

If you're hardware inclined, you can tap the line that connects to the modem and terminal. These lines are usually not connected to the schools switchboard, and can even be exposed outside the building itself. Use a tape recorder and a Radio Shack auto-pickup device to tape the transmission (which is usually 300 baud anyway). Play the tape into your own modem (set it on answer) and you'll be able to see the originate data (including the password) on your screen. If you haven't tapped modem lines before, I do not suggest using this method.

Note that UAPC requires each school to change their password once a month, so make sure you get the password right after they change it. This will give you plenty of time to learn how to use UAPC before you attempt any stunts with modifying data.

All About Wylbur

Okay, you're in UAPC, what now? Well, once in you will be dealing with Wylbur. Like I said before, Wylbur is sort of like a command shell plus batch language and editor all built into one. You will know you're in Wylbur when you are given a "COMMAND?" prompt.

There are some misconceptions about Wylbur that I would like to clear up right now. When most New York City hackers talk about the "grades computer" they simply refer to it as Wylbur. This is misleading because they are referring to UAPC. Wylbur is not synonymous with UAPC; the Wylbur shell is used at many different computing sites which use MVS and IBM mainframes. It's sort of like equating VAX/VMS to the computers at DEC. VMS is an operating system and has very little to do with the machines at DEC headquarters. The same holds true for Wylbur and UAPC.

Wylbur also runs on the other IBM machines at Kingsborough (which have different dial-ups, seperate from UAPC), these machines have no affiliation with the UAPC machines. Therefore students using these other machines at Kingsborough must know Wylbur as well. Lucky for us, you or any student can purchase (no ID required) a Wylbur manual at the Kingsborough bookstore (Building U) for $4. Just ask the nice lady for the "Wylbur User's Guide", written by Ganesh Nankoo, and tell 'em I sent ya. If you do get into UAPC, I strongly suggest that you buy this manual. It is very informative and can keep your ass out of hot water.

Some useful commands under Wylbur:

RUN PRINT: run the exec program in your active area and print the output.
RUN FETCH: same as above, but place output in fetch queue.
FETCH *: fetch the last output and place into your active area.
LIST: list current active area to screen.
LIST OFF: list current active area to printer.
LOCATE: locate all jobs submitted.
LOCATE *: locate last job submitted.
LOCATE 056: locate job 056.
PURGE 056: purge job 056 which is on the output queue.
COLLECT: input/enter data into your active area.
CLEAR ACTIVE: clear your active file in memory
USE #name: load the file "name" from disk into your active area.
SAVE #name: save your active area.
SET PSW: change your password.
SET KEY: change your keyword.
SHOW DIR: show current files in your directory.
SHOW USERS: show current users on UAPC.

(Note: your active file is a buffer used by the editor. You can list it, save it, clear it, load into it, run exec jobs from it, etc.)

You can also get help on UAPC by typing HELP HELP (yes, twice. One HELP will not do the trick).

Applications That Run on UAPC.

Once inside UAPC, you may have very little contact with Wylbur itself, and you will see a "WHICH JOB?" prompt instead of the "COMMAND?" prompt. The reason for this is because most of the time the applications are all automated and accessed from menus that are run by batch files which execute when you log in.

Thus, the system is very friendly. You may see a menu that asks you if you want to view a transcript, view a schedule, admit a student, dismiss a student, transfer a student, add classes, delete classes, etc. You simply choose what you want to do. Via these menus you will be able to do anything that the school administrators can do, including changing grades. Sometimes, however, there are no menus, and you will have to execute commands yourself. A list of these commands can be gotten using one of the HELP menus. Here are some of the jobs you can execute: ABSCOR, ABSINFO, ABSREP, ACADROP, ACAINFO, ACAMSTR, ADDSECT, ADDROP, ADRPLST, BATINFO, ABSINQ, CLASSLST, CODELIST, CUTINFO, CUTDEL, FIXCODES, FIXOFCL, HITRAN, GRDUPDT, LATCOR, LATINQ, MAIL, NGRUPDT, OFCLLIST, PUNRQST, REGISTER, REQADRP, REQINFO, REQUPDTE, SCAN, SCHEDULE, SKED, TRAN, TRANUPDT.

You can drop straight into Wylbur by sending a <BREAK>. This will cause your menu shell program to stop executing. If you happen to leave the menu system and do drop into Wylbur (with its "COMMAND?" prompt) you can get back to the menu system by typing RUN. This will execute the menu shell program that is currently in your active area.

Remember that each time you or your menu program submits a job (i.e., to change a grade), the job will be executed and the output will be placed on the fetch queue. If you don't want to leave a trail, then you must use one of the above Wylbur commands to find and PURGE the output of your completed jobs. If you do not PURGE the output, it has a good chance of being printed out at the program office when they print the output of all the jobs that they submitted.

Changing Grades

Clearly, this thought has crossed your mind in the past few minutes, so let me begin by saying that I do not recommend changing any records on UAPC. You can use UAPC to get all kinds of useful information on people and never get in trouble.

If you do hope to change grades and get away with it, there are several things to consider. You must remember that your guidance counselor has physical backups of all your grades in his/her little notebook. If you've gone to your counselor for advice on which classes to take, you'll recognize the book of which I speak. The grades in this book are not generated by UAPC but instead entered into the books at the end of each grading period by the counselors using a pen or pencil. This physical record is only used as backup in case UAPC gets wiped out or something like that. Comparisions between UAPC transcripts and the physical record are almost never done, unless there is some kind of disagreement between the student and the school regarding the transcript itself. If you do plan to make a clean run, you had better cover all the angles. This means bribing some stupid kid to borrow the book for a little while so that you can make some modifications, give the dude $20, and make sure he doesn't know who you are

Guinea Pigs

Before modifying either your physical record or your UAPC grades, I would strongly suggest using a guinea pig test subject. What this means is that you should pick some kid, any kid, who goes to your school and that you have never met and never plan to meet, change their grades, purge the output on the fetch queue, sit tight for a few days, and watch what happens

Hacking

Keep a close eye on your test subject. If you notice the kid getting suspended or federal agents running around your school or something like that, you know that you better not mess with UAPC, at least not in your school anyway. If nothing happens, then you should decide whether to take the risk of changing your own grades.

If you consider the use of innocent human guinea pigs to be distasteful, then you had better be prepared to risk your ass by using yourself instead. I do not consider it to be distasteful, but then again I am devoid of all ethics and morals anyway.

You can still bail out at this point and your life will proceed normally. However if you do change your grades (both physically and on UAPC) and nothing happens to you for several weeks, you can be almost 100 percent sure that you got away with it. Since both records (physical and UAPC) have been changed, there can be no discrepancies. Only your previous teachers will know what grades they gave you, and by now they will have forgotten who you are. Only your transcript speaks for them now. If you do get away with it, you can start mailing out those applications for Stanford and MIT.

Enough Already

(continued from page 3)

getting strange human beings in another location, we realized what had happened. Again. An incompetent repairman had routed our fax line into someone's house. They got our calls and we got their bill. Apparently, the problem was fixed without us ever being notified. New York Telephone says there's no way for us to get credit for the local calls these people must have made or for the service interruption because what happened to us simply wasn't possible. If we wanted more information, though, we could obtain a local usage list for only $1.50.

In 1984, we made reference to the AT&T strike of 1983. The strikers weren't paid, the customers were charged full price for poor service, and the company made lots of unearned money. The same is true today of NYNEX/New York Telephone. With all the confusion that divestiture brought, we now at least have options to AT&T. With New York Telephone, there is no choice. No competition. And it's high time there was.

Kabelsalat
ist gesund
Chaos Computer Club

THE GALACTIC

The Galactic Hacker Party could very well have been the strangest gathering of computer hackers ever to have assembled. It wasn't just a meeting of silicon-heads who talked binary for three days. It wasn't simply a group of rowdy individuals out to give the authorities a headache and cause general chaos wherever they ventured. Nor was it merely an ensemble of bizarre, crazy, and ultra-paranoid types, like the ones who make it to the 2600 monthly meetings in New York. The Galactic Hacker Party was *all three* of these put together, and a good bit more.

The conference took place at the Paradiso Cultural Center in Amsterdam on August 2nd, 3rd, and 4th. Hackers and techno-rats from all over the world converged on the scene, some remaining for quite some time afterwards. Information about computer systems, phone systems, famous hackers, governmental regulations, privacy abuses, and new toys flowed freely and openly. Since there are no laws against hacking in The Netherlands, there were virtually no restrictions placed on anybody.

Representatives from the Chaos Computer Club (West Germany), Hack-Tic (The Netherlands), and 2600 met for the first time, along with hackers from many other countries. We tried to figure out the best way to pool our resources, to share information, and to support one another's existence. It was most heartening to see other people in strange and distant lands who also had developed an infatuation with knowledge and a strong desire to share it. It was at the same time a bit disconcerting to see this enthusiastic spirit, and to wonder why it would seem so strange back home in America.

Like any good conference, the best things happened behind the scenes. That's where the contacts were made and the methods divulged. Press from all over the world showed up, as did people from all walks of life. It was a curiosity shop, a coming together of inquiring minds.

But enough poetics. What does this all mean? Well, for starters, it's injected us with some new enthusiasm and some brand new knowledge. We tend to forget that there's a world of diversity out there, different lifestyles, alternative ways of accomplishing things.

The Germans taught us the importance of organization. In Hamburg alone, there's at least one meeting of hackers a week. They play with computers, compare magazines (in West Germany there are several magazines that deal with hacking), and figure out their various strategies. Hacking is much more political in West Germany than any other country.

The Dutch showed us how, above all else, having fun is what really matters. Learning about the things that you're really interested in can be the most fun of all. In The Netherlands, what the authorities do or think is less than secondary.

HACKER PARTY

The openness of Dutch society helps to foster this healthy attitude.

We, the Americans, shared our beloved and practical hacking traditions, like the art of trashing. Almost as soon as we raided our first trash bin, the anti-authority Dutch figured that the dumpster of a police station would be the best place to get info! We must now live with the knowledge of what we have started.

We also helped to convey the importance of thorough scanning. It's easy to get discouraged in countries that don't have the wealth of services that we've grown accustomed to. But, regardless of how primitive or restrictive a phone system may appear, scanning almost always accomplishes something. There are now people scanning in both East and West Germany, as well as The Netherlands, England, Belgium, and France, discovering strange tones, dialing shortcuts, ringbacks, and other nice things.

Calling To The U.S.A.

One thing we'd like to advise those of you who travel abroad in the future. *Do not use USA direct to makecalls*! It may be cheaper than dialing direct from Europe, but it's still a great deal more expensive than most people seem to realize. While a three-minute call to New York may cost something like $8, so will a 10 second call, as the initial billing is for the first three minutes. After that, it's at least $1 per minute. It's extraordinarily easy to rack up a huge bill. By the way, here are the USA Direct numbers from various countries:

Australia: 0014-881-011; Austria: 022-903-011; Bahamas: 800-872-2881; Belgium: 11-0010; Bermuda: 800-872-2881; Brazil: 000-8010; British Virgin Islands: 800-872-2881; Cayman Islands: 1872; Denmark: 0430-0010; Dominica: 800-872-2881; Dominican Republic: 800-872-2881; Finland: 9800-100-10; France: 19-0011; Gambia: 001-199-220-0010; Grenada: 872; Greece: 00-800-1311; Guatamala: 199; Hong Kong: 008-1111; Hungary: 00-36-0111; Italy: 172-1011; Jamaica: 0-800-872-2881; Japan: 0039-111; New Zealand: 000-911; The Netherlands: 06-022-9111; Norway: 050-12-011; Singapore: 800-0011; St. Kitts: 800-872-2881; St. Martin: 800-1011; Sweden: 020-795-611; Switzerland: 046-05-0011; United Kingdom: 0800-89-0011; West Germany: 0130-0010.

Now you may be curious as to why we printed those numbers if they're such a rip-off. Because it doesn't have to be a rip-off if you're smart about it. You can use USA Direct to call person-to-person collect to someone who isn't there. The person who answers will then get your number and call you back. No matter what service they use, the cost will be substantially less. USA Direct is also a great way to get free directory assistance for anywhere in the U.S. That's right, they charge 60 cents per call over here, but from overseas it's free!

continued on page 45

British Telecom: Guilty

The following plea was sent by British Telecom to the British people.

British Telecom is asking customers to be patient - and to *listen* for the changes which are taking place as a result of its annual multi-million pound investment programme.

Many people dislike change. Others may feel changes are of questionable value. A lot of money is being spent - but on what?

That old familiar sight, the red telephone box, is disappearing from view. Some people see this as a change for the worse - yet the new tough, easy-clean booths, with clear telephone keypads make life a touch easier for thousands who would not or could not previously use a public telephone.

A few people even dislike having a push-button, digital 'phone in their home, instead of the old 'dial' variety - yet without the switch the vast potential of telecommunications technology could not be unleashed.

Questions are often raised about the high numbers of bright yellow vans spotted around the country, and the traffic problems they sometimes cause. But British Telecom engineers often have to park at inconvenient points temporarily, simply to carry out installation and repair work.

British Telecom is working hard to improve service to its customers, and to offer the best possible value for money. Most people will have heard about the network 'going digital', and ultimately this will revolutionise the way we communicate.

However, until all the cables and equipment are in place to link up the entire country, the customer down the road may not fully appreciate the changes which are taking place.

Once the actual telephone exchange where your line is connected 'goes digital', it can open up a whole new range of communications possibilities. Under an optional package of Star Services, calls can be forwarded to another number anywhere in the country under automatic call diversion - invaluable, for example, for the one-man business which needs to stay in touch 24 hours a day. A big advantage is that callers need only ring one number - wherever you happen to be.

All you need is an approved multi-frequency 'phone which plugs in to the usual socket.

Another option is a three-way calling conference facility, where business meetings can be held down the telephone line. It can also be used for family conferences. Think of the savings on telephone bills!

Other developments will be useful to the non-business user. Itemised billing is being progressively introduced, and another facility will enable you to ring a number and check immediately what a call has cost.

The all-talking, singing, dancing exchange is just around the corner, with everything geared towards helping the customer get the best possible use out of the 'phone.

The average digital exchange is capable of transmitting around 250 'messages', from helping you to find out what a call has cost to sending a polite message to remind you to replace your handset. If polite requests fail, it resorts to a Howler - a screech which will alert you even if you do happen to be at the bottom of the garden!

The inside of the exchange has been transformed, too. The old, conventional switching equipment has been replaced by rows of blue and grey cabinets housing printed circuit boards.

One floor of equipment replaces what used to take up two floors, and the technology is getting more compact all the time. The new equipment is cleaner, virtually maintenance free, and much quieter.

If a fault occurs, the card controlling that particular line is replaced with another, and the problem card is sent away for repair.

The size of the mainframe computer has also reduced, and the battery back-up units are clean and maintenance free.

It all heralds another world, but although the 'character' may have changed, the new hi-tech equipment is making everyone's life

(continued on page 30)

The death of COSMOS?

In the summer edition of COSMOS Currents, a newsletter put out by Pacific Bell/Pacific Telesis, the death of COSMOS is said to be on the way. "Tired of those old outdated dial-up COSMOS TTY43's?" one of the articles reads. "Well, get ready to kiss them goodbye. To better secure COSMOS, all dial-up machines are being replaced with Private Line terminals. Funds have been approved for their removal, to be replaced with new CITOH 326's (or some equivalent hardware). This project is being done to comply with the Pacific Bell Security Information Policies, and to prepare the way for the eventual replacement of COSMOS with the new SWITCH product."

All that we know about SWITCH is that it used to be called ASCOT and that there was an article about its future in the spring edition of COSMOS Currents. They go on to brilliantly deduct that "the main cause of hackers breaking into the COSMOS database has been access to the dial-up COSMOS network. This project will eliminate that threat. What remaining staff and Systems Technology personnel that must remain on dial-up circuits will be secured through other means (i.e., tokens)." Tokens? As in coins? Token minorities? What could they be referring to?

"More users [of COSMOS] also translates into more people that have access to the database, and hence the opportunity to degrade its integrity. The long range answer to many of these types of concerns will be forthcoming with the availability of SWITCH in the early to mid 1990s. Until then we are the stewards who must keep COSMOS running effeciently [sic]." And then a few rousing choruses of the company song.

A new telephone number has also been announced for the COSMOS Client Community that encompasses everything from simple repair to the COSMOS Hotline, MIZAR Hotline, the CCTACs, the DDTAC, placing an order, etc. That number (811-DATA) can only be reached from within California and is answered by a voice response unit that directs the call.

Has anyone else heard anything about SWITCH or its equivalent in other parts of the country? If so, forward the info here.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch
Ken Copel

Design
Zelda and the Right Thumb

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, The Plague, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Violence, and the growing anonymous bunch.

Technological Marvels

US Sprint swears that its billing problems are ending. They're introducing a new system meant to replace all the old systems that never quite agreed to forced integration. Does this mean that Sprint will stop sending us bills for six-month old calls? Stay tuned. (By the way, it's perfectly all right to pay those bills six months late. At least with us it is.)

☎

Get ready for the new Sprint Voicecards. Now in the testing stage, they may soon become commonplace. This is how they say it will work: "You begin by taking the first two steps you would take in using the US Sprint FON Card. You dial the 800 number and punch in the number you're calling. Then, instead of dialing your FON Card number, you dial an easy-to-remember number, such as your birth date, and give a two-second personal verbal password." If the technology is a thousand times better than Sprint's billing system, it just might work. Of course, then it will be subjected to another more sophisticated testing stage: us.

☎

Voiceprints of another sort are being tested in Suffolk County, New York. The authorities are experimenting with an "electronic barbed wire" system, similar to ones that seem to be popping up all over the nation. It works like this: the "system" calls a prisoner on probation at his home at any time of the day or night. When the person answers, the computer tells him to name ten states (thereby assuming he/she has had a college-level education). If the voice doesn't match the one in memory, a probation officer's beeper goes off and the prisoner gets a visit. It seems easy enough to fool for now. A series of tapes would be good enough to act as a substitute for the real voice and they could be played on demand by an accomplice while the prisoner is on his/her way to a new location. And once he/she gets there, call forwarding will take care of the rest. Naturally, the solution to the shortcomings will eventually be cameras. It's probably better than prison, but a giant step closer to Big Brother. Not to worry, it's for our own good, remember?

☎

And speaking of surveillance, guess what Nielsen Media Research has come up with? A brilliant new way of finding out what people are watching on television, that's what! You guessed it, cameras, no bigger than a breadbox, that would, according to the New York Times, identify members of a household and record, second by second, when they are watching television, when they leave the room, and even when they avert their eyes to read a newspaper. The Nielsen people think it'll be a big hit because people won't have to do anything. The device will focus on facial features, first deciding if a face is recognizable and then whether or not the face is directed toward the set. Twenty-four hours a day.

Hacker Spies

You may have heard of some computer hackers being indicted in Hannover, West Germany for KGB spying. While some media have reported a link between these people and the Chaos Computer Club, we find no such link at all. What many fail to realize is that Chaos reports hacking activity to the world, much like 2600. They are not themselves actively involved. Remember this the next time you read sensationalist reports in the papers.

Nynex Bigotry

One we somehow missed last year...it seems the Nynex Yellow Pages has problems with the twentieth century. Heritage of Pride Incorporated is a Manhattan-based gay and lesbian organization. When Nynex asked them what category they wanted to be listed under in the phone book, they responded with "Gay and Lesbian Organizations". That won't do, said Nynex. Try something like "Escort Services", "Nightclubs", or "Human Services Organizations". Heritage of Pride filed a complaint with the New York City Human Rights Commission, charging Nynex with violating the city's human rights ordinance which prohibits discrimination on the basis of sexual orientation. A category for homosexual groups in Manhattan could easily contain over 100 listings. We're not sure how it turned out because we can't get ahold of the new yellow pages (Nynex strike). Regardless, it will no doubt be replayed all over the country.

Dial-It News

Pacific Bell has a new 900 service classification. The 505 exchange will be used for chat services, 303 for sex talk, and 844 for everything else. Also, a recorded message at the beginning of the call must give the charges. And if charges for either 900 or 976 calls exceed $75 in one month, Pacific Bell will send you a letter telling you what a fool you are.

☎

A way to get sort of even with all of those ripoff phone numbers that charge absurd prices. Unlike just about everywhere else in the country, 976 numbers in parts of California are reachable from other parts of the country. This means that you'll only be charged the rate to California, which can be substantially less than a local call to a 976 number, especially at night. It seems that Pacific Bell lacks either the technology or the inclination to block these calls. But it's possible that your local company may have put a block on its end, in which case you'll be denied access. Also, only one long distance company seems to complete calls to 976 numbers: AT&T. All the rest will give you error messages of some sort. Some numbers that are reachable: 213-976-WAKE, a computerized wake-up service which is only good for waking people up in California, 415-976-4297 and 213-976-9769, a couple of "hot" conference lines, and 213-976-1010, a computerized matchmaker service. Even at "normal" prices, we think you'll feel ripped off.

Payphone Choices

Three-quarters of the owners of property where Bell payphones are located have chosen AT&T over other long distance companies for operator-assisted calls on those phones. MCI got 10 percent, Sprint 8 percent, and all of the little companies got the rest (around 7 percent). Some of those little companies are AOS companies, which often charge exhorbitant rates and try to make customers think they're using AT&T. These percentages are in line with the choices made by residential customers.

☎

The Missouri Public Service Commission has outlawed AOS companies in businesses (hotels, malls, etc.) and at public phones, saying that these services are not in the public interest. However, consumers are still free to be ripped off within their homes if they so choose.

Overseas Access

AT&T is reportedly trying to get permission to make calls to Vietnam, one of a few countries that are impossible to call from the United States. When dialing overseas, there are two possibilities: either you can dial the country direct, assuming you have direct overseas dialing capability or you have to go through an international (IOC) operator who places the call for you, sometimes after a lengthy delay. But then there are countries like Vietnam, where there is no access at all from the United States. Usually it's because of an argument or a war or something of that nature. But things are looking optimistic for a connection with Vietnam since the government there appears interested in having AT&T ring its phones. An agreement also appears imminent for direct-dial service to the Soviet Union (7), now reachable only through an operator. Some other countries that are currently unreachable are Cambodia (855), North Korea (850), and Albania (355). Numbers in parentheses are those countries' country codes. Vietnam's country code is 84. If anyone knows of other unreachables or has an alternative way of reaching these countries, let us know!

News From The U.K.

Waits for directory assistance in England are commonplace. To help alleviate this, the voice of actress Julie Berry will soon speak the desired phone number to customers. It's estimated that this will reduce operator time by one third. The automatic voice response (AVR) works like this: the operator searches for the number in the usual way by asking for name, locality, and street. The operator keys this information into the computer. The system then displays a list of possible numbers on the screen. The operator touches a button on the keyboard to identify the required number and switches over to AVR. The AVR equipment assembles the number message from its store of exchange names (a major difference from the U.S.) and numbers recorded by Julie Berry and then gives it to the caller. For example, "The number you require is Ipswich, 0473, 227848. I repeat, 0473, 227848. Please hold if you need to speak to an operator." Ms. Berry had to record all of British Telecom's 6,000 exchange names, plus the full set of numbers and number combinations, in the different inflections with which they are spoken depending on their position in the complete number. For example, the last four digits in the number 01-356 5366 are spoken "five three double six"; the inflection on the double six in that position is different from that used when the number "double six five three" is spoken. Recordings of exchange names of uncertain pronunciation were sent to British Telecom operators in the relevant localities for checking, and if necessary, re-recording. For some Welsh names, a Welsh operator sat with Ms. Berry during the recording to make sure the name was spoken correctly. Earlier this year, call handling time was also reduced by introducing a recorded message at the beginning of the call, much like the systems in use in the United States. Each of British Telecom's 10,000 directory assistance operators records an opening message of

"Directory enquiries; what name please?" that is heard by the caller as the call is being connected. All of these time-saving measures will bring the average human operator time down from 39 seconds to about 25 seconds.

☎

British Telecom is expected to buy Tymnet from McDonnell Douglas for $355 million. Tymnet is one of the world's largest data networks, with local access in 750 U.S. locations. It ought to be interesting having a British phone company running America's second largest public data network. Telenet is, of course, number one.

☎

Chatlines have been banned by British Telecom. They had been operating on two special exchanges: 0898 and 0077. BT cut off service to eight companies that didn't obey their order. A spokesperson says, "Reports from customers and our own enquiries suggest that some lines, not normally used for chatlines, may have been switched to that purpose. We are continuing to monitor the many thousands of telephone lines which have the capability to be used for chatline services and will cut them off as we track them down." They've also set up a snitch line (0272) 252801 for customers to call if they know of a chatline. By British Telecom's own definition, the ban effects any call in which more than two people take part in a live conversation. We all know how dangerous that can be.

One Less Choice

As of August 1, The Source Information Network no longer exists. Compuserve bought its main competitor and promptly shut it down.

Privacy? What's That?

According to Boardwatch Magazine, Representative George Gekas of Pennsylvania has introduced a bill that would require BBS operators and information services to provide names and addresses of persons suspected of using communications networks to commit crimes without requiring a search warrant. The bill (House Bill 2082) could also force phone companies to give this information, again without a search warrant. It's been a bad summer, folks.

☎

The Commissioner of Immigration and Naturalization, Alan C. Nelson, has proposed a nationwide computer system to verify the identities of all job applicants in order to halt the widespread use of fraudulent documents by illegal aliens seeking jobs. Similar nationwide computer databases are being suggested repeatedly by various governmental agencies. So far, Congress has been successful in preventing this because civil liberties can still be found in their dictionaries. How much longer do we have?

☎

Scotland Yard is busy storing information in electronic databases. Things like electronically processed fingerprints, suspects' photographs, and full criminal records. When the system is ready (by the end of 1990), police officers will be able to find out everything there is to know about a person within minutes. The fully digitized fingerprint records could allow a detective to send an image of a fingerprint found at the scene of a crime and receive within minutes the name and criminal record of the suspect. The system is known as PNC2. Another system, called HOLMES2, will be used to spot discrepancies in suspects' stories. The example they use says that if a suspect gives two separate police forces differing stories, the computer will instantly catch the discrepancy. Policemen just hate being lied to, don't they?

☎

The Christian Science Monitor reports that Americans are so concerned with getting tough on drugs and crime that they've become lax on privacy concerns. "Anybody with the intelligence of a turnip has to be concerned about the potential" for abuse, says Clifford S. Fishman, a law professor at the Columbus School of Law of Catholic University. According to James A. Ross, president of Ross Engineering Inc., some new phone systems have built-in monitoring capabilities, allowing a person to listen in on others' conversations. It's become much easier to "wiretap" a line. Often it can be done by computer. Experts are increasingly concerned about illegal wiretapping by private individuals. A growing number of private detectives and police forces appear to be engaging in this activity, with little chance of being detected. The current hysteria over drugs and crime make it all the more unlikely that Americans will be concerned about civil liberties.

☎

In a related story, Bell of Pennsylvania has acknowledged widespread wrongdoing by company employees, including giving outsiders the private phone records of its customers. A Bell employee gave information about a phone customer's long distance calls to a private investigator, according to a report from the company. Bell also routinely let police have information about long distance records without search warrants. The company said it was disciplining 13 employees, but it refused to identify them or describe their punishment.

☎

The Justice Department has a neat idea to keep guns out of the hands of felons. Every citizen will be required to carry a "personal smart card". This card would contain your life story, including any criminal activity. Gun dealers would never let a criminal buy a gun, right? And if you're not a criminal, you've got absolutely nothing to hide. So everyone will be safe. And happy. And brain-dead, given time.

Hackers In Trouble

Kevin Mitnick, the computer hacker featured in our spring '89 issue, will have served a year in jail this December. At that point, he is to be transferred to an addiction clinic for six months, in order to help cure him of his "disease". After separating the Mitnick myth from the reality, the authorities backed away from many of their original allegations. "A lot of the stories we originally heard just didn't pan out, so we had to give him the benefit of the doubt," said James R. Asperger, the assistant U.S. attorney who handled Mitnick's case.

☎

And Robert Morris, the writer of the Internet Worm, is facing 5 years in prison and a $250,000 fine for that bit of mischief. The 24-year-old was indicted on a single felony count under the 1986 Computer Fraud and Abuse Act. Nobody was hurt, no valuable data was lost, and we all learned an important lesson. Why the government is wasting everyone's time on this is beyond us. They must prove that Morris intended to cripple the Internet by releasing the worm that wound up disabling thousands of machines on November 2, 1988. We've obtained a copy of the source code to the worm. If you want to judge for yourself, send $10 to 2600 Worm, PO Box 752, Middle Island, NY 11953.

Hacker Fun

2600 received many calls from the media in the days before the dreaded "Friday The 13th Virus" was supposed to strike. We tried to tell them not to panic but it didn't work. Some people actually were given the day off because their employers didn't want the computer to power up on that day. Once again, the media fueled a nonexistent fire. We'll repeat here what we told them. Viruses can occur at any time. The odds of being infected are relatively small. The odds of being adversely effected are next to nothing if you take some basic precautions: know the source of your software, keep backups religiously, don't let fools tell you what to do, etc. The viruses set to go off on the 12th and 13th are no different from any other in that relatively few people will ever see them.

The only difference is that we know about it beforehand and have plenty of time to let our imaginations run wild. We suggested that users who were concerned could simply change the date on their computer to the virus date to see if anything unusual happened.

After all, the computer doesn't really "know" the date, right? The media didn't go for that, saying it was too technical.

☎

Recently an unknown hacker got into the computer that controls the speed limit on the Burlington-Bristol Bridge near Philadelphia. He proceeded to change the speed limit from 45 m.p.h. to 75 m.p.h. Judges refused to listen to appeals of those ticketed, saying, "The public should know better than that no matter what the sign says."

☎

Persons attempting to call the probation office in Delray Beach, FL early in June were connected to a phone sex hotline operated by a woman named 'Tina' instead. According to Southern Bell, someone accessed the central office with a modem and reprogrammed their computer in such a way that calls intended for the probation office were instead routed to a New York-based phone sex line. "People are calling the Department of Corrections and getting some kind of sex palace," said Thomas Slingluff, a spokesman for the Palm Beach County Probation Department. Southern Bell officials said it was the first time their switching equipment had been maliciously reprogrammed by an outside computer intruder. Southern Bell provides the local phone service for Florida, Georgia, North Carolina and South Carolina.

Telco Literature

What kind of people are the phone companies hiring as writers? This blurb was spotted in the July/August issue of the MCI customer newsletter, MCI Connections: "The sun begins to set over the Golden Gate. The grill's been lit. The cicadas sing. A sizzling steak brings back memories of the summer of '82...that rooftop cookout with Doug. Even though

continued on page 38

4TEL

4TEL is a loop testing system mainly used by General Telephone (GTE) that consists of a Voice Response System and a Craft Dispatch Section as well as the facilities and equipment used for testing functions. The following text will attempt to dispel many of the 4TEL myths that have been created in the past years, such as the idea that it can be used to eavesdrop on lines within its serving area. The information provided has been gained from company publications and from personal experience. A 4TEL is not the same thing as a REMOBS, which stands for Remote Observation.

The portion of the system that much of the phreak/hack population is familiar with is the Voice Response System, which has normal POTS dialups. This system greets the user with an announcement message and then asks for a password, which is entered in DTMF tones. The legitimate use of these dialups is for outside craft personnel (linemen) to call in, perform tests, and receive the results for subscribers' lines. The VRS is provided so craft personnel can access the 4TEL system at times when no one is at the testboard (at nights or weekends). Through the VRS, up to eight craft technicians can access 4TEL at the same time, enabling them to get more done in a smaller amount of time.

After a password has been accepted by the system, the electronic voice will ask for the line number that the user wishes to be tested. The number entered will be read back to ensure correct entry. The system will then ask for the user to enter the mode. The modes are:

1: Calling on other line.
2: Calling on test line.
3: Line test results.

It is possible on some VRS's to get a listing of the modes by dialing 0 when the voice prompts. Line tests are possible from both modes 1 and 2 by dialing the octothorpe (#) key. The results of the test will be announced along with the length of the cable in miles. Bridged ringers, if any, will also be noted. Mode 3, the line test results section, will tell the user there are no test results available unless they have been previously entered. The 7 key is the monitor command from both test modes. If there is speech on the line, it will be detected electronically but will *not* be heard by the user. The monitor command is not 'REMOBS' (Remote Observation) but a method of determining if the line is busy due to normal means (conversation) or due to some trouble condition at the switch. When the system asks for the ID code for a monitor command, the system will accept the line number as well as the initial password, and even a secondary password before dialing, but it has not been determined by the author if this is a standard for every 4TEL. Not just anything will work for the monitor password however, as it will announce if the ID code entered is invalid or not.

If mode 1 is entered, these commands are available:

1: Fault location.
2: Other Testing.
7: Test OK, monitor.
8: Hang up.
9: Enter next line number.

If option 7 is chosen, another menu will be available if the line tests busy.

2: Monitor test.
3: Overide and test.
4: Wait for idle.

If suboption one (fault location), mode one, is chosen, these commands are available:

1: Open location.
3: Short location.
4: Cross location.
5: Ground location.
8: Hang up.

If suboption two (other testing), mode one, is chosen, these commands are available:

2: Loop ground ohms.
3: Dial tone test.
4: Pair ID.
8: Hang up.

Mode Two Commands

2: Other testing.
7: Test OK, monitor.
8: Hang up.
9: Enter next line number.

If suboption two (other testing), mode two, is selected, these commands are available:

2: Loop ground ohms.
8: Hang up.

The 4TEL system's main use is for standard testing, which is done nightly upon every line in an exchange. This locates faults and problems before they have to be reported by customers. All lines that have trouble detected upon them are printed out in a report at the repair center the next morning where the proper fault location and dispatching can be done. The measurement and test unit of the 4TEL system is called a COLT, Central Office Line Tester, which performs all nightly and on-demand tests upon the exchange through local test trunks.

There are a few different types of COLTs. The standard version will serve any CO for up to 10,000 subscribers. The COLT RS is used in rural step-by-step offices (referred to as "steppers" also) for up to 1,300 lines. The Digital COLT is used for digital central offices. These can have remote Colt Measurement Units (CMU's) for remote switches which are controlled by the Colt Computer Unit (CCU) at the host switch. The CMU speed calls the CCU at night to start the testing and direct the operations. The CMUs in regular end offices have digital links (over the normal telephone network) with the SAC, which is how the line test results are distributed to the repair center.

The 4TEL system can also test lines upon command by a human operator at the SAC (Service Area Computer). The CRT operator enters the line number in the proper field and 4TEL runs a full series of tests as well as displaying past line history, fault summary, volts and current information, and the cable length. The results of the testing are displayed in plain English, as opposed to decimal or other format, on the screen. A dispatch decision is also displayed after every line test to determine if a dispatch is needed.

SAC's

The SAC is the centralized focal point for 4TEL control and reporting. This computer is located in the repair center and distributes test/work information between CRT's and COLT's. The SAC formats the results of routine testing into a daily advisory report as mentioned earlier.

There are several types of 4TEL reports that are worth noting. The DISPATCH report lists troubles that can have an immediate dispatch for them. These also tell the location of the fault (cable, CO, station, etc.) and are classified into two types, moderate and severe, relating to how service affecting the problem may be. The CABLE report lists all new cable faults. A plant status report summarizes the condition of the outside plant and totals them per individual exchange. In these reports, trouble conditions can be listed in a variety of ways. CROSSES and WETS refer to line insulation faults and may indicate water penetration of the cable. SHORTS and GROUNDS are insulation faults at the station set. OPENS refer to a broken, or "open" ring or tip lead in a cable pair. BACKGROUND refers to electrical noise caused by power lines being nearby. ABNORMAL VOLTAGE indicates high voltage conditions. There are others, but the reader will hopefully get the idea from the ones listed above.

CDS

Another major part of the 4TEL system is the Craft Dispatch System, which is a DTMF and speech response setup used to exchange report and schedule information between the repair center staff and outside craftspersons. Linemen call in to get dispatch information that has been previously entered by the dispatcher. CDS plays back the info one field at a time. When the craft personnel is ready to receive the next field of information, he simply says 'Go' and the system continues. A printer at the repair center informs the dispatcher when a craftsperson has received a report. When the trouble is taken care of, a completion report is done on the CDS in which it asks for the closeout and schedule, one field at a time, to be entered in DTMF and in speech. The clerk at the repair center then closes the trouble on the SAC/4TEL system after the line is tested a final time to ensure proper operation.

CDS may also have audit trails of every transaction for a certain time period. So to summarize the work flow for involving the CDS: irate customer calls the clerk at the repair center. The information is forwarded to the dispatcher who enters it into CDS. Craft personnel call in and receive the messages, do the required work, then file a completion report. The clerk then closes out the trouble in SAC/4TEL.

The Digital Concentrator Measurement Unit is another component of the 4TEL testing equipment that is used to test lines in digital concentrators such as the GTE MXU and the NTI-OPM. They are located inside Digital Loop Carrier System remote terminals or huts and consist of a circuit board and measuring system. It provides AC and DC measurements of subscriber loops, as well as all the normal test/measurement functions such as fault description and location, dispatch messages, and special tests. The DCMU can test the lines of an individual DLC remote terminal, or a group of terminals that are located together. The capacity of terminals that the DCMU can test is determined by analysis of test traffic and economic factors as well. Both the CRT at the SAC and the VRS are compatible with the DCMU. These units are self calibrating, unlike the PMU's of an LMOS supported Loop Testing System. The 4TEL CCU is linked to the DCMU via either a 1200 baud dialup or a dedicated link, depending upon the size of the exchange.

Some of the tests that 4TEL performs are loop and ground resistance (which detects resistance faults and sheath ground problems), dial tone test (in which the number of times dial tone can be drawn during a certain period is recorded), busy line monitoring (not BLV or REMOBS), coin station tests (totalizer, coin relay, etc.), as well as all the standard tests which were covered above. A pair identification can also be done, in which a tone is placed on the pair to help those at terminal cabinets locate that specific one, similar to the LMOS/MLT tone applique function.

Miscellaneous Notes

If a user enters the number of the 4TEL system they have dialed in upon, the system will announce an intercept. A user cannot monitor/test Directory Assistance through 4TEL. Lines that are out of the system's NPA can be tested also, but a 1 has to be dialed before the number just like an ordinary toll call. The 4TEL VRS will give the user a "beep" tone after a few seconds of waiting for input. If the user doesn't enter anything, the VRS will disconnect. A version of the 4TEL system is also used by Rochester Tel in New York, and there may be other independent companies that use the system. Try to find out what system you're served by. If you're in a Bell area, it will most likely not be 4TEL, but LMOS.

I hope that this article has helped readers to better understand the way the 4TEL system operates. Again, there may be some differences depending upon the area and the company.

Thanks to the small group of people who contributed additional information to the contents of this article.

words from

Mobile Telephone Info

Dear 2600:

The article "Scanning for Calls" appearing in the Summer 1989 issue mistakenly identifies the phone service using 451-459 mhz as cellular phone service. IMTS/MTS, old style mobile telephone service, service is found between 454-455 mhz, 152-153 mhz, and 35.26-35.66 mhz. This service can be provided by either the phone company or an RCC (Radio Common Carrier). RCC's can also provide paging services. While these frequencies are not locked out of most scanners, they are illegal to intercept due to the passage of the ECPA just like cellular.

Since the IMTS/MTS service providers were not the major force behind the passage of the ECPA, unlike the cellular industry, and scanners capable of intercepting their frequencies have been on the market since the epoch; the services on these frequencies have been left unprotected by scanner manufacturers. The media's focus on cellular service may also have been a factor.

For informational purposes here are the Mobile Telephone Channel Assignments for the above ranges:

ZO: 35.26	ZF: 35.30	ZH: 35.34
ZM: 35.38	ZA: 35.42	ZY: 35.46
ZR: 35.50	ZB: 35.54	ZW: 35.62
ZL: 35.66	11: 150.180	13: 150.210
JL: 150.510	1: 152.030	3: 152.060
5: 152.090	7: 152.120	9: 152.150
YL: 152.540	JP: 152.570	YP: 152.600
YJ: 152.630	YK: 152.660	JS: 152.690
YS: 152.720	YR: 152.750	YK: 152.780
JR: 152.810	28: 252.200	21: 454.025
22: 454.050	23: 454.075	24: 454.100
25: 454.125	26: 454.150	27: 454.175
29: 454.225	30: 454.250	31: 454.275
32: 454.300	33: 454.325	34: 454.350
QC: 454.375	QJ: 454.400	QD: 454.425
QA: 454.450	QE: 454.475	QP: 454.500
QK: 454.525	QB: 454.550	QO: 454.575
QR: 454.600	QY: 454.625	QF: 454.650.

Koo Iyo Do

A Southern ANI

Dear 2600:

That number in Atlanta (yes, this is a weird one) is 940-222-2222. (Nothing happens until the 10th digit is entered.) You get a computer voice telling you your number.

John

ROLM Horrors

Dear 2600:

Columbia University has recently installed a new digital ROLM system to replace the old centrex. This change has angered many students for the following reasons:

The system is incompatible with modems and answering machines and the university charges "rental fees" for data-comm equipped telephones as well as for space on the Phonemail voice message system.

They've blocked all access to 976 and 540 numbers simply because the billing software on their "state of the art" system is not able to track them.

They slap a $5 surcharge on every collect call received.

You have to dial 9 digits (91+Personal Security Code) just to get an off-campus dialtone.

They impose a $100 limit on the Personal Security Code (PSC). If your account runs over $100, they turn your PSC off, even if it's in the middle of a billing cycle, and even if they didn't bother to let you know that your account was nearing $100.

The system bills you for a call 45 seconds after you stop dialing regardless of whether or not the call goes through. If you call long distance and let the phone ring more than a few times, you're billed for it even if the person doesn't answer.

The local calls are now timed as opposed to the untimed trunks we used to have.

There are only 400 trunks for over

8,000 phones. Re-orders are not uncommon.

The phone-mail answering machine type service does not have enough channels. You could find the message-waiting light flashing on your station, but you might have to dial the message retrieve code 15 or 20 times because you can't get a circuit.

Is there any FCC ruling that the university is violating by imposing these restrictions on us? Their attitude is more one of, "Well, that's just the way it is. If you don't like it, pay New York Telephone to draw wires into your room." Indeed, I have put in a private line. But there are a lot of people who just cannot afford to do that, and are beirig shafted right up to their tonsils. Any advice?

gmw

If you haven't already, read our Spring 1988 issue where we describe how such a system was installed at the State University of New York at Stony Brook with a lot of the same problems. Not much has changed there; in fact many things have gotten worse. Frequently every phone on campus appears to be busy because the university refuses to buy enough incoming trunks. Outgoing calls are often just as hard. A recent test revealed a wait of 25 minutes just to get an outside operator (it had nothing to do with the NYNEX strike). Outside operators refuse to bill to the originating number because the exchange isn't recognized as an actual telephone company exchange and they have no way to verify your identity. And ROLM can't handle call supervision so everything bills after 45 seconds, even international calls, where it can easily take that long just to get a busy signal. For a corporate setting where individual preference really doesn't matter, ROLM may be bearable. But for a university setting, no system could be worse, that is for the students. We happen to know that Stony Brook makes money from the phone system now because the bills they send to students are much higher than the bills that come from the phone companies. In other words, New York Telephone doesn't charge the university for uncompleted calls. Yet the university charges the students. Where does the money go? It's getting to the point where some universities are as sleazy as AOS companies.

At least Columbia offers you the choice of putting in your own lines. Stony Brook offers no such freedom. The wimpy student government thinks they accomplished something by winning the right for a student not to have a phone at all, rather than winning the right to choose one system over the other.

A company called BITEK has moved in to handle billing. They developed a notorious reputation for ignoring student complaints about bills. Finally, someone broke into their Phonemail account (which they never changed from the default password), and changed the outgoing message to: "Hello. This is BITEK and we don't care about your problems!" You can hear their current message by calling (516) 632-9050. They've also just installed a "state-of-the-art" automated billing computer that sounds like it belongs on Lost In Space. Call (516) 632-9055 to hear that.

As far as we know, there's nothing illegal about what Columbia and Stony Brook are doing. But it's damn immoral to rip people off and make already chaotic lives even worse. There are ways of getting even, like scanning out the entire Phonemail system and clogging up the system with junk mail (not using your own extension, of course). Or calling someone on campus and sending a symphony of touch tones. The ROLM switch will dutifully keep the line open until the concert is over, rendering the recipient's phone useless. But the most effective way is to complain until *you're blue in the face and to let those responsible know what's being said about them.*

Good luck.

A Nagging Question

Dear 2600:

How many subscribers do you have anyway?

The Apple Worm

Next to "Whatever happened to TAP?" that's the question we get asked the most. It's harder to answer than it might seem because 2600 isn't like most other magazines. We have around 1,000 people who get the magazine sent directly to them. But don't be deceived by that rather small number. Many others (random polls indicate at least four times that number) get what is known as a "secondary" copy, that is, one that has been copied by a friend or even electronically transcribed. Naturally, we prefer it when people subscribe directly because it helps keep us going. The most important thing, though, is to get the information out. Close to 1,000 more copies go to various newsstands and bookstores around the world. And whatever else is left goes to all of the people that order back issues in the future. So, to answer your question, we don't really know. The numbers just don't tell the whole story in our case.

A Request

Dear 2600:

Thank you for publishing such an informative well-written magazine.

I only have one complaint. Please try to deal more with phone phreaking than hacking. Anyone can get access to a phone, but not all of us have computers and modems to participate in computer hacking.

Thank you.

Grand Rapids, MI

Another Request

Dear 2600:

You mean I'm paying $18 a year to read such stupid, boastful lies such as those of The Disk Jockey that you printed in the Letters section in the Spring '89 issue?? C'mon, you didn't really believe that crap of the $150,000 *cash only*, did you?? I mean *four* pages of your good magazine were wasted because of this letter! Anyway, the reason I am writing is this: Up until a little while ago, I was able to use my computer to blue-box. I would simply call up *any* 800 number (I could even dial 1-800 and make up the last 7 digits), and whenever the 800 number was ringing, answered, busy, or even the recording of "We're sorry, the number you've dialed is not in service," I could whistle 2600 hertz and box on. Anyway, one day the 2600 hertz would not work anymore. There is still an exchange in my area that I assume is on step-by-step. That exchange does not even have touch tone, call waiting, forwarding, etc. (Mine does.) I assume that exchange can be blue-boxed off of. In the spring '89 issue, you answered a letter that said that blue-boxes can still work from an ESS line.

Can you *please* tell me how I can perhaps blue-box from an ESS area? Is it all in the 800 number that I call? (The 800 number never seemed to matter before.) I do *not* want to *red-box*. I want to use a *blue-box*.

I am sure that if you will print some *valid* information concerning ESS and *blue-boxing* that your readers (and me) will greatly appreciate it. If you could devote half as much space to this question as you did to The Disk Jockey's letter, I'm sure your readers would gain more from it than what they did from his letter. Thank you. One more thing: has anyone had any complaints on the *red-box* circuit that you printed last summer? Does it work?

THOR

just like you

First off, in a country where a computer hacker is locked up in solitary confinement while sadistic murderers aren't, you'll forgive us if we believe someone who claims their bail is unreasonably high. Even if it was a blatant lie, it certainly is conceivable and we chose to treat it as such. If you have information to the contrary, please share it.

Now, about your blue-box problems: you need facts, not assumptions. Obviously, something has changed in your area since not all 800 numbers would change their characteristics on the same day. Find out what happened. Did you get a new switching system? Did the routing somehow get changed? You must go to this office that you believe to be a step and see if your old method works there. If it does, then you know where the restrictions are being applied, mainly in your own exchange. If it doesn't work in the step exchange, then restrictions are in effect further up the line somewhere. Once you understand what these restrictions are, you can attempt to find a way around them, like routing through a remote part of Canada, perhaps through an 800 number that terminates there. It all depends on what has changed. It sounds as if you were able to box off your outgoing trunks in the past which is why it didn't matter what number you dialed. If these have changed, it will now only work if the remote trunk is still boxable. Keep in mind that blue-boxing is dangerous, particularly in an ESS area.

The only complaint we've had about the red box circuit in the Summer '88 issue is that the schematic is too small. For a bigger copy, send us a stamp or an SASE.

The Call-Waiting Phone Tap

Dear 2600:

Can you please tell me if this really works?

From Alternative Inphormation, PO Box 4, Carthage, TX 75633: "So, you think your best friend may be running around with your girlfriend, eh?? Or is he just a plain back-stabber? Whatever the case, if you have two phone lines and the call-waiting feature on *one* of the lines, you can tap his phone line and listen to his conversations if he has call-waiting also!! 1) Call up your friend with the phone you wish to listen to his conversation with. When he answers call-waiting (he's already on the phone and you are the second caller), then you either just sit there quietly or say, "I'm sorry. I have the wrong number." 2) Next, you wait until he returns to his original call (the one you interrupted) and he puts you on hold. 3) Now, pick up *your other* phone line and call *your* call-waiting. 4) Answer *your* call-waiting. 5) Now go back to him. (Answer, then click back. Click two times, answer, and go back.) 6) Hang up your *second* line. 7) You are now on the line! 8) Listen and remain silent!!! He can hear you!!"

We'll be honest. We asked quite a few people to test it out and nobody was able to make it work. But nobody said such a thing was impossible. If it does work, it probably only works within the same central office, maybe even the same exchange. If you can get two lines in the same central office that each have call waiting, by all means try it out. If it works, let us know what your exchange is. If this capability does exist, it's probably a flaw in a particular type of switch. We'll let you know what we find out.

Interesting Numbers

Dear 2600:

You may have seen the bumper stickers about that say:

DON'T LIKE MY DRIVING?
CALL 1-800-EAT-SHIT

One day I got inspired and dialed it. Amazingly enough, there was a recording there promising to explain the bumper sticker if I only dialed a 900 number somewhere. How much money he would extract from my wallet in the process was unclear. But the idea of advertising a 900 number via an 800 number is certainly a new one, at least to me.

You think that's sleazy? Maybe, but we can top it. A baseball player in California offered to tell the real story behind his drug arrest, but only if you call a special 900 number. Still another has you call a 900 number which tells you to call another 900 number.

Dear 2600:

Could you say something about the number 900-xxx-0000? By changing the prefix and adding the 0000 to the end you get a recording that identifies the 900 exchange provider. Maybe someone can give some insight to this. It's almost like the 700-555-4141 long distance service.

LK

There's not much we can add to what you said, except to be careful when dialing a 900 number as it may turn around and bill you for a special call. If you look in our Spring '89 issue, you'll see a complete list of prefixes and their corresponding companies for both 800 and 900 exchanges. By the way, 800-xxx-0000 gives you that information as well. Also, if you want to hear what other companies' messages sound like, simply prefix the 700-555-4141 verification number with the carrier access prefix. For example, 10222-700-555-4141 will get you MCI's verification message, 10288-700-555-4141 will get you AT&T, etc. Look in this issue somewhere for a complete list of carrier access prefixes.

UNIX Hacking

Dear 2600:

As a long-time UNIX systems program and security officer, I found the two-part series (A Hacker's Guide to UNIX) quite interesting. I commend Red Knight on his or her following the true spirit of hacking: learning about something through experimentation. I would like to make a few remarks which may prove useful to people who will follow in Red's footsteps.

First, there are two major versions of UNIX: AT&T and Berkeley. Minor variations on these major versions abound. The AT&T version is used mainly in the "commercial" world and for all practical purposes, it doesn't support computer networking. The Berkeley version differs in many subtle ways (most of which make it friendlier to programmers and users), but a primary difference is its thorough support of TCP/IP networking. (Hacking computer networks is a topic worthy of a separate article.) The Berkeley version is used by many universities, and it also forms the basis for the version of UNIX supported by Sun Microsystems.

Second, login names may include any characters and may be any length up to and including 8 characters. Administrators discourage upper case login names, due to UNIX's attempt to determine whether you are logging in from an upper-case only terminal (a now obsolete feature).

Third, different UNIX versions differ in the password requirements, although all have a maximum of 8 characters. The standard way for UNIX to handle passwords is to use the password as the key to a modified DES encryption routine, and encrypt the value zero. The resulting 64 bit value is translated to a printable form and stored as the encrypted password. The DES encryption accounts for the 64 bit (8 character) limit. The DES encryption algorithm is "broken" in one of 4,096 ways to prevent searching the encryption space and to keep hardware DES encryption devices from being used in attacks.

Fourth, there are three different

shells available:

Bourne shell: /bin/sh - all systems

C shell: /bin/csh - Berkeley systems

Korn shell: /bin/ksh - recent AT&T systems

They all differ in detail, but achieve the same goal. Look in the last field in /etc/password to determine which shell a user prefers (others can be invoked as desired).

Fifth, the directory lost+ found is not where all removed files go, but rather where all files go when recovered after a system crash.

Sixth, the sysadm command is AT&T UNIX-specific.

I would also like to mention that there is a wide range of books available on UNIX operation and programming. (I know, that's cheating.) However, there is one book that I highly recommend: UNIX System Security by Patrick H. Wood and Stephen G. Kochan, Hayden Books UNIX System Library, 1987, ISBN 0-8104-6267-2.

It only covers AT&T UNIX (and hence misses out on real networking) but does an excellent job.

fin

Intelligent Payphones

Dear 2600:

"Any person having the phone number and password of a specific intelligent payphone can do such things as program the calling rates, check the amount of coin in the box or even check to see if the phone has been vandalized. An FCC approved data access arrangement must be used to connect the system to telephone lines with an automatic ring detect circuit answering incoming calls. Upon receiving an incoming call, the software could be set up such that the payphone issues a false ringback tone or busy tone to discourage unauthorized users. Personnel with the password, however, could simply enter DTMF codes over the false call progress tones to gain access. Once the password has been correctly entered (from any DTMF phone) commands can then be entered."

Upon reading this information (from the California Micro Devices Data Applications for the G8880 DTMF Transceiver), I promptly went down to the local mall where I knew there would be some "intelligent payphones". For some reason, the numbers of the two payphones I found were printed on the outside of the phone. Armed with this information, I went home and proceeded to dial up the payphones. During the ringback, I tried beeping in a few DTMF tones, but to no avail. But after a few rings, a computerized voice came on which advised the operator that this was a public phone (and therefore collect calls should not be directed to it). When the voice stopped, I tried some DTMF tones once again. The phone beeped some tones back and then eventually hung up. After calling back a few times, I stumbled into something remarkable. I began to hear the sounds of cars starting and people talking. I had somehow caused the payphone to monitor the area near the payphone and transmit these sounds back to me at the other end of the line. Needless to say, I was quite surprised. I began to ponder several questions: is this legal? What legitimate purpose is there for a function like this on a payphone? Should the general public know? It seems to me that we should experiment more with these private payphones and see what other hidden features they may have.

Mr. Upsetter

By all means, experiment. We'd like to know what formats exist for the security phones, i.e., how many digits, when are they entered, etc. In answer to your other question, it's probably legal, although for what purpose it's intended we're hard pressed to say.

Retarded Payphones

Dear 2600:

In the Spring '89 edition, I read your article on How Payphones Really Work and enjoyed it immensely. I thought that

post-script

it was a very accurate and informative piece. Continue the excellent work.

Now that I have given your ego a boost, I will ask for a favor. Could you please include in one of the next articles a piece on "collect only phones" as I am incarcerated at the present time and all that is available to use from this crowbar hotel are those damnable gadgets. They are the most exasperating items ever invented, as you are unable to call 800 numbers or to bill to a third party or even be able to use a telephone credit card with them. The party you are calling must pay the exhorbitant prices which they charge for collect calls, and who the hell wants to try to convince individuals to accept collect calls? There has to be a way around these mechanized monsters, and any info which you could possibly print about them would be greatly appreciated.

Incarcerated

It's hard to experiment with something without having access to it. That's why people who find themselves locked up with these hell-phones have to try everything possible. It is entirely possible there are no holes, considering what the purpose of these phones is. In that case, there are still options. For instance, just suppose you called a voice mail system or an answering machine that answers the phone with the message: "Hello? (pause) Why of course I'll accept charges." If you're lucky enough to gain access to a voice mail system that allows you to dial out, you'll be able to make phone calls (and rack up two bills at the same time). Unless your DTMF pad gets cut off after a connection is made, in which case you'll need a white box (portable DTMF generator) to hold up to the mouthpiece. And that's probably illegal to possess in prison. Readers, any ways out?

British Telecom: Guilty

(contiuned from page 12)

easier.

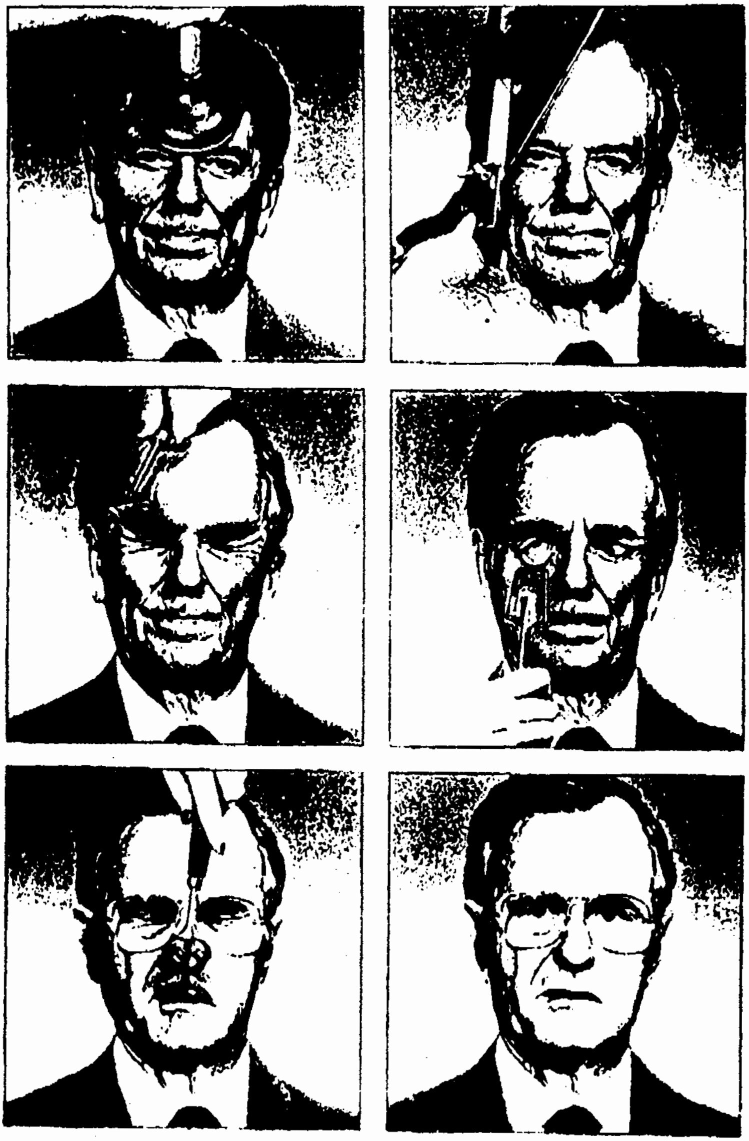
Some people may not want the complete new range of features offered by a fully digital system, but most will approve the changes which give them fast, clear communication, with fewer breakdowns and less maintenance needed. That is where British Telecom is heading.

As the old saying goes - a chain is only as strong as its weakest link. Hence, until every connection end to end of a telephone call is fully digital, you may not notice any difference in the clarity of the line.

Once it *is* all digital, calls will be connected in split seconds, and the line will be sharp and clear.

In the meantime, if you see a British Telecom engineer up a telephone pole or down a manhole - please remember he is trying to bring you the best possible service, wherever you may live.

Did you get the feeling that perhaps the public isn't too happy with old BT? Of all the phone companies we've ever come across, these folks seem to have the guiltiest consciences.



THIS IS THE BEST FAX WE'VE GOTTEN SO FAR, NOT COUNTING ARTICLES. YOURS COULD MAKE IT TO THE WINTER ISSUE. KEEP THEM COMING IN.

(516) 751-2608!!!

REMOBS

by The Infidel

Technically, REMOBS stands for REMote Service OBservation System. But in plain, everyday English, it's Ma Bell's way of watching what you do on the phone.

This is far more dangerous to the phreak than the DNR (Dialed Number Recorder), which begins recording as soon as you pick up the phone in order to catch the numbers you dial.

The REMOBS allows anyone to tap into your line, without clicks, beeps, noises, volume or voltage drop (sorry guys, but those voltage meters on the line won't cut it here), and most importantly of all, it can be done *without* the need of a hard-line tap. That's what makes the REMOBS so dangerous - it's done from remote. In other words, from any touch tone phone.

The REMOBS was meant for observational purposes. When designed, it was devised so linemen and fellow telco employees couldn't indiscriminately access anyone's line and make calls off of it, while providing the person monitoring the line safety from detection. The signal coming out of the mouthpiece and keypad of the observer's phone will not make it to the target number's end. So, your victim cannot hear you when you lock onto his line, nor can he hear when you drop off. This isn't a gizmo like the diverter or the gold box; it's totally different.

When you call up the REMOBS unit, you will hear a tone which lasts for about 2 seconds. You then have about 5 seconds to key in the access code or the REMOBS will hang up. The access code is different, depending on the unit, ranging from two digits up to five, but most commonly being four. When entering the code from the touch tone keypad, each digit must be held down for about a second for the unit to receive it. When you key in the correct code, you'll hear another tone and the unit will wait for the 7-digit target telephone number.

But here's the catch: due to the volume of exchanges present within an NPA, the unit itself is limited to covering only a small region, usually within the confines of a central office. In large cities, many units may be needed to cover an entire NPA, and so, your REMOBS may not be able to reach every number you try. That means that you'll most likely need more that one REMOBS to cover one area or city. This also means that it will not be able to access out-of-LATA numbers.

After dialing the target number, if that line is being used, you'll instantly be connected with the conversation, and they, as I've said before, will never know you're there. If you should lock into the target number when it's not in use, you won't hear anything - just line noise and maybe some crosstalk, rather than hearing the actual dial tone, as you would if you had made a direct line tap. With the REMOBS, you don't actually "connect" with the customer's line; you simply monitor it. When the customer picks up the phone, you'll hear their dial tone, the person dialing the number and the conversation, and then the person hanging up again. You could stay there all day, but that's not too smart.

Though your keypad may not be heard by the line you're monitoring, the REMOBS itself does recognize the tones. To disconnect the unit from the current tap, enter a digit, most often the last digit of the access code. After you disconnect, you'll get the second tone again, prompting you for another seven digit number; you don't have to reenter the access code. When you're done with the REMOBS altogether, instead of hitting the last digit of your access code to reset the unit for another number, you must enter another digit, which varies from unit to unit, to disconnect totally so the unit can be used again.

It's important not to just hang up from the REMOBS, or it will stay connected to the line you set it for, and will not accept other calls until it's reset manually, which will draw attention to it, your target, and most important of all, you.

Keep in mind that REMOBSs vary from network to network, and perhaps even state to state, so you will have to experiment with it to see what keys perform what function. Have phun....

Gee...GTE Telcos

In this issue we printed an article about 4TEL, a testing system used by GTE. What quite a few people don't realize is that GTE hasn't been involved only with Sprint, a long distance company. For many years, GTE has been operating local phone companies in areas known as non-Bell regions.

Their equipment is made by a company called Automatic Electric, located in Illinois. (We've heard reports that AT&T has bought them, to make things even more confusing.) This company only made step, electronic, and digital switches, completely skipping over crossbar. One of their early electronic switches was known as the EAX #1 and was introduced in the early seventies. It had very few custom calling features. An annoying trait of their call waiting feature was that it signalled you after each and every ring, making it very hard to ignore.

Eventually, the EAX #1 was scrapped and replaced by the EAX #2 in the mid seventies. You could distinguish this switch by the loud 1100 cyle tone between rings that indicated a number wasn't in service. Also, GTE's busy signals would time out after about 18 cycles. Another characteristic: if you came in on someone else's call waiting, you could hear a short bit of the conversation you were interrupting right before the ring, which was about 50 percent longer than a normal ring.

The EAX #5 was introduced around 1980. It was soon renamed the GTD #5 (General Telephone Digital #5). It was more sophisticated, with no clicks at any point in the connection.

As we mentioned, Automatic Electric skipped the crossbar phase of evolution. But GTE wanted to install a crossbar switch at one point. So they contracted a French company to make a crossbar switch for a Texas location. Instead, they received this horrible piece of junk that got numbers wrong, connected people together who didn't want to be connected together, among other things. One day, the machine that played the non-working number announcement broke down. GTE couldn't get parts for it. So an enterprising switchman took a Code-A-Phone 700 answering machine, recorded a "number out of service" message, put the machine in play mode, hooked it through a push-to-talk handset, and held the button down with a piece of tape. Everyone who called a non-working number in that exchange would get connected together after the recording cut off. But one day the motor in the answering machine burned out; it was running 24 hours a day after all. For a while anyone who called a non-working number in the 214-423 exchange would instantly get connected together. Today, that exchange is served by a GTD #5.

The GTD #5 has different custom calling packages, known as smart call, smarter call, and smartest call. The smartest package offers call forwarding, call waiting, three way, speed dialing (8 and 30 entries), cancel call waiting, one number redial, save call (like a redial but with a special code), and call camping (calls you when person you're trying to reach isn't busy). A person who has call waiting will hear call waiting beeps if a call comes in while the first call is on hold and they're talking to the second call. Whether this is a design flaw or a feature is unclear. All custom calling features can be accessed on the second line, unlike Bell companies, who only offer cancel call waiting on the second line.

Many of those who live in GTE land do not sing a happy tune, particularly those who don't have digital switches. Here are some observations:

"The telephone 'service', if I may use the term lightly, was abominable. I personally experienced all of the horrors (lousy call completion rate, wildly wrong numbers, noisy-and-not-just-white-noise lines), and then some."

"I know a fair number of people for whom Pacific Telephone vs. GTE was a factor in choosing a place to live — and not the least important factor by far."

"For year after year here in Durham, North Carolina I put up with wild buzzes on the line; picking up the phone to dial, only to find other people on the line in the middle of a conversation; not getting important calls because my phone wouldn't ring properly; touch tones that weren't buffered well enough and were converted to pulse anyway (if you dialed too fast, you had to start all over); dropped connections in the middle of a conversation; frequent wrong numbers not even remotely similar to my number. These were not isolated things every couple of months — it was *all the time*."

GTE payphones don't get very good reviews either:

"I once spent a miserable two days looking for an apartment in the west/southwest Los Angeles area (almost all covered by GTE), driving around with a car full of newspapers and a pocketful of dimes. It got so I wouldn't even bother stopping at a GTE payphone unless there were at least two of them together, as only then was it likely that I'd find a single working phone. The defective phones were in nice areas and had no signs of exterior damage — they just didn't work. Often they'd be sitting there emitting strange clicking and thunking noises, as if they couldn't quite digest that fast coin. Others would appear to be fine until you put a dime in."

Then there was this observation:

"One of the interesting operations that GTE participates in when you have not paid your phone bill is to *not* disconnect your line, but rather to block *outgoing* calls... except 800's. When they did this to me, I didn't care because I almost never made any local calls. One call to the Sprint 800 number and I could make all the long distance calls I wanted."

Naturally, we'd like to hear of any experiences from our readers in GTE land.

This article was written with the help of Silent Switchman and Mr. Ed. Angry comments were extracted from The Telecom Digest, a newsletter distributed on the computer networks.

Nowadays, we fix a problem before there is a problem.

The basic approach of quality management couldn't be simpler.

Working in teams, we anticipate the potential problems. Then we work out how to solve them before they occur.

One of the first successes of using a quality approach was payphones. We used it to develop more than twenty ways to solve the payphone problem.

As a result, today all our payphones work nearly all the time.

Thus, in turn, earning us much more money.

Some of the solutions were obvious. Kids set fire to the blue buttons (remember those blue buttons?) because they liked to sniff the solvents these released.

So we changed the keys to something better suited to kids. Heavy metal.

Some of the other things we had to do were not so obvious.

We had, for instance, to take a completely new look at training, documentation, and maintenance.

Alan Whicker finds out more in the latest '*Whicker's Telecom World*.'

And because it is 'Telecom World' he takes a look at how payphones abroad match up to ours.

With some surprising differences in France, Germany and the USA.

As you will discover, when the film comes to your team meeting.

№1

We're working on a new number.

AN INTERNAL BRITISH TELECOM ADVERTISEMENT.
YOU WON'T GET A BETTER PICTURE OF A BT PAYPHONE.
AT LEAST, NOT FROM US.

Voice Mail Hacking...

by Aristotle

There are four models of the Genesis Voice Mailbox Systems (VMS). They all have the good VMS features, like voice data compression, ability to send messages to other users, user definable passwords (I believe up to 10 digits), user definable opening message, ability to review message when recording, and a separate phone number for each box.

How To Hack The VMS

The first step is to find the voice mail system. The easiest way to find a system is to look in the yellow pages under telephone answering services and/or equipment companies. I found a system in Louisville, Kentucky that was listed with the name Voicelink. Its number is 502-429-9200.

After finding the VMS, you must find out what type of system it is. There are many different types, each with their own unique characteristics. If you find that the system is a Genesis system, look into it. Chances are you will be able to get on easily.

A Genesis system has the following distinguishable characteristics: 1) If you hit "0" during the announcement, it will prompt you for the password. 2) If you hit "#", it will go to a phonebook system. The phonebook is used to look up users' boxes by spelling out their names.

When the target Genesis system is found, do the following: 1) Find a mailbox with an announcement that says, "I am taking a message for mailbox number XXX." 2) During this announcement, press the "0" key and wait for the password prompt. 3) At this prompt, press "0" again. This is almost always the password for the unused box. If it is not "0", then go to the next open box. 4) Now that you have control, change your password and follow the friendly directions. It is extremely user-friendly so you should have fun.

...NYNEX Style

In mid-August the NYNEX Business Centers' nationwide voice mail information system was penetrated by unauthorized individuals. According to Randy Hareford, voice mail administrator at NYNEX, numerous "kids, maybe twelve or thirteen years old", who "didn't know what they were doing" took over 38 of approximately 1900 voice mailboxes on the system.

Dialup modem numbers used to manage the system were posted on at least two bulletin boards and sent to other interlopers via the voice mail system, but most of the encroachment was blamed on the use of "easy passwords" chosen by legitimate users. The callers identified themselves with aliases such as Flight Commander, Knight Caller, Blackbeard, Chris Columbus, Photo Bug, Easy E, Ray Gun, Mr. Upright, Teenage Warrior, and Mr. Six.

According to Hereford, at least one message passed between purloined mailboxes contained information detailing stolen credit card numbers and expiration dates. The FBI was reportedly notified, but was only interested in the credit fraud issue; not in security problems with the system. Interestingly, NYNEX has always maintained that messages on the system were not retrievable by anyone other than the addressee.

The security breach allegedly brought the system down one evening and later resulted in a system broadcast to all users warning them not to convey sensitive information on the system, instead suggesting "more secure" methods such as the U.S. Mail, IBM PROFS, and the direct-dial telephone network. While most of the abused mailbox passwords were deleted and reassigned after two weeks, the system administrator received one message offering information about other compromised mailboxes and the security loopholes used in exchange for legitimate voice mail privileges. The offer was neither accepted nor replied to.

PUNCHING PAY PHONES

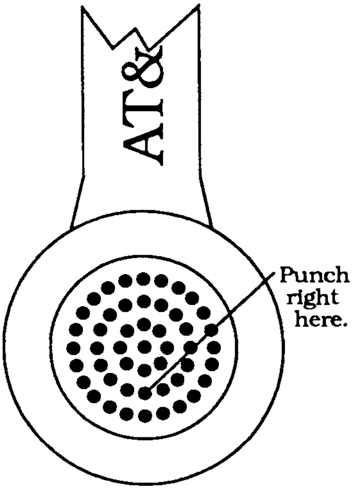
By Micro Surgeon/West Coast Phreaks

Remember in the movie *Wargames* when David needed to make a call, and had no money. He did so by opening the mouthpiece and touching a piece of metal from the inside of mouthpiece to the plate of the pay phone. Believe it or not this archaic technique still works in the most sophisticated areas, including all BOC'S (Bell Operating Companies) DTF (dial tone first) pay phones. This technique does not, however, work on private pay phones.

To make a local call, without using coins (or slugs), first punch a small hole (see diagram) with something sharp (ie. a nail) through the existing outer plastic holes into the inner (metal) mouthpiece. This gives access to the inner magnetic coil. Next dial the first six digits of the local number and **before** dialing the last digit, touch the nail to the face plate, holding it there as you press the last digit. This whole process of touching the nail to the face plate, pressing the seventh digit, and simultaneously releasing it from face plate as the button is let go, should all be done within one second. Timing can be critical. Essentially the phone is being grounded, and as a result BOC's are fooled into thinking that sufficient funds have been deposited for local calls.

As with any ploy there are limitations and problems. Long distance calls cannot be made, because a different method is used to verify the deposited coins. One of the main problems is that a mild shock (not to death of course) may be experienced. A less serious problem can be that the mouthpiece may be damaged, by punching to hard or in the wrong place, rendering the phone useless.

Punching pay phones is nothing new, and I certainly didn't discover this art. Of course a Red Box will work much better, but it could have inadvertently been left at home. What one should understand is that this technique will work and that it's not just a bit of telephone history.



A Pay Phone Handset Receiver

continued from page 19

it's only 7:30 pm, Lynn reaches for the phone call to call him in New York. Introducing the new MCI Prime-Time Plan...." Or how about this from Sprint's FON Line Newsletter: "On average, most Americans will move 11 times during their lives, coping with a process that can be exhilarating, exhausting, and expensive. Although moving can often be stressful, planning ahead can ease the transition and save wear and tear on your nerves and your wallet...." Five more paragraphs elapse before the first mention is made of US Sprint and how it wouldn't be a bad idea to have a Sprint calling card. We suspect this kind of cagey sales pitch won't exactly go over big but at least it's giving those writers from the slush pile a place to go.

Calling Card Tutorials

For those who feel like wasting a bit of time, give a call to the AT&T "calling card tutorial" line. By dialing 1-800-255-3439, you can experience the excitement of using an AT&T calling card by making a simulated telephone call! A narrator guides you through this exciting process. MCI has a "test drive" number that takes you through the adventure of using an MCI card. They can be reached at 1-800-950-TEST. In both cases, valid calling card numbers are not necessary.

Another Telco Ripoff

C&P Telephone is said to be scamming the public in the Washington DC area. It seems that local calls in Washington DC are 20 cents, while in neighboring Maryland and Virginia they're 25 cents. In Washington DC, none of the phones are marked for price and many people are fooled into depositing 25 cents instead of 20. The phones don't even give any extra time to callers who put in too much.

Technology Marches Back

A French computer system fouled up big-time when it misread some data. 41,000 Parisians who were supposed to have been fined for fairly minor offenses found themselves receiving computerized letters accusing them of all sorts of bizarre crimes.

Apparently the coding used in the system got mixed up, meaning that people who were supposed to have been fined for speeding were instead fined for pimping. "There were a lot of cases of living off immoral earnings, racketeering, and murder," said a City Hall official. "The accused persons will be receiving latters of apology. Instead of receiving summonses on criminal charges, they should have been sent reminders of unpaid motoring fines." Motorists ticketed for failing to stop at a red light were fined for "importing unauthorized vetinary medications", while those whose only offense was crossing a solid white line on the road were charged with "night fishing in a place reserved for fish breeding".

☎

New York Telephone repairmen are being sent on wild goose chases. This is thanks to a new computerized repair service introduced in the midst of the Nynex strike. Now you no longer have to talk to a service representative, unless you don't have a touch tone phone. Customers key in their phone number and then go through a menu. "Are you having trouble getting a dial tone?" the computer asks. "Press 1 for yes, 2 for no." Other categories include trouble making calls, static on the line, trouble receiving calls, or trouble with custom calling features. If you answer yes to any of these, you dive into another menu where the computer attempts to isolate the problem by asking more yes/no questions. The whole process takes about three times longer than talking to a human being but it saves New York Telephone the expense of human employees. And as for the wild goose chases, it is possible to completely foul up the system by making lots and lots of calls, each time entering a different number. A repairman will be dispatched for each and every call. Hackers will have fun because they don't have to use their voices and the system is accessible from payphones. It's also possible to dispatch a repairman by accident since there's no way to abort. The system confirms the date the repairman will be out but never asks the customer to verify in case they've changed their mind. People who want to bypass all of this garbage can call 890-6611 toll-free and reach a human at repair service. New York Telephone does not give out this number. They've also introduced an automated credit operator which is reachable by dialing 211. You can either hang up at the tone for a local credit or touch tone the number you dialed. Again, it takes longer than the equivalent with a human being.

And if you don't have a touch tone phone, you get connected with a recording that tells you to wait until after the strike is over.

And Finally

Some words from the Beijing youth daily: "In recent days, people in Beijing who normally love to make phone calls have suddenly become cautious, and many of them say on the phone 'Let's write or chat face to face instead, otherwise we might get into trouble.'"

Lair of the INTERNET Worm

by Dark Overlord

These days worms & viruses seem the in thing to do. Most hackers (and crackers) have a friend who has a friend who is a "super genius" and wrote one that did amazing things, did wonders, scrambled eggs, etc.... Any programer worth half the ram in their system can write a worm and/or virus without much difficulty. The information provided in most magazines and newspapers on the subject is utter crap.

The decompiled source code to the "Internet Worm" is now available from *2600* magazine. The code is based on an effort of reverse engineering. This source, when compiled, will generate the same executable that the "Great" Internet Worm was made out of. I can't say where I got this code because s/he does not wish to have their name (handle) echoing around these circles.

The personality/attack strategy of this worm was to reach as many hosts as possible rather then attempting to access higher privileges on an infected host.

Please note that all of the attacks used by the Internet Worm have been fixed on almost all systems that use the Internet. If there is sufficient interest I may do a detailed write-up on how the attacks used by the Internet Worm worked. There are still many more holes in UNIX to be abused. Thus it is possible that, with a weekend's worth of work, this worm could ride again. (But I would not do that, would I?)

If you want a copy of the source code (with comments), send $10 to 2600 Worm, PO Box 752, Middle Island, NY 11953.

Touch-Tone Frequencies

	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Each touch tone is a combination of two tones. For instance, 3 is 697 hertz and 1477 hertz. This diagram also contains the four extra tones that every touch tone phone is capable of producing. These tones are used in the U.S. military phone network (Autovon) for establishing the importance of the call. We'd like to hear specifics of any further uses for them.

Special Information Tones (S.I.T.)

We've all heard these. They're the special tones you get right before you hear a recording telling you the number you've reached is out of service. They're also used for a multitude of other conditions. The purpose of these tones is to permit an automatic Call Disposition Analyzer (CDA) to differentiate between a human voice and a recorded announcement, and to categorize the type of recorded announcement.

Special Information Tones are a series of three tones at the beginning of an intercepted call.

SIT Tone type and usages

Period	Frequency	Designation
SSL	LLL	IC - Intercept - Vacant # or AIS, etc.
LLL	LLL	NC - No Circuit (Inter-LATA carrier)
LSL	HLL	VC - Vacant Code
SLL	HLL	RO - Reorder Announcement (Inter-LATA Carrier)
LSS	LHL	#1 - Additional Reserved Code
SLL	LHL	RO - Reorder Announcement
SSL	HHL	#2 - Additional Reserved Code
LLL	LLL	NC - No Circuit, Emergency, or Trunk Blockage

Period duration: S=Short (274 msec), L=Long (380 msec)
Frequency: L=Low (913.8 hz 1370.6 hz 1776.7 hz)
H=High (985.2 hz 1428.5 hz)

This information was taken from a central office recorder/announcer installation manual circa 1983.

2600 MARKETPLACE

HACKING AND PHREAKING SOFTWARE for the IBM and Hayes compatible modems. The best war dialers, extender scanners, and hacking programs. $8.00, including shipping and handling. Make payable to Tim S., P.O. Box 2511, Bellingham, WA 98227-2511.

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. FOR SALE: Genuine Bell phone handset. Orange w/tone, pulse, mute, listen-talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

WANTED: Information or documentation on Natural Microsystems' WATSON VIS Option. Will be used for upcoming 2600 voice mail board. Urgent need! Contact the 2600 office (516) 751-2600.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market, 153 E 53rd St., NY. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info or to request a meeting in your city.

WANTED: Technical/operations manual or any technical data on North-east Electronics Corp's TTS-2762R MF & Loop Signaling Display. Will gladly pay for copying and mailing costs, or reasonable price for genuine manual. Does anyone know anything about this machine? Bernie S., 144 W. Eagle Rd., Suite 108, Havertown, PA 19083.

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

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

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

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

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

**Do you have something to sell?
Are you looking for something
to buy? Or trade? This is the place!
The 2600 Marketplace is free to
subscribers! Send your ad to:
2600 Marketplace, P.O. Box 99,
Middle Island, NY 11953.
Include your address label.**

**Deadline for Winter Marketplace:
12/1/89.**

CARRIER....

10001-MidAmerican LD (Republic Telecom)
10002-AmeriCall LDC
10003-RCI Corporation
10007-Tel America
10011-Metromedia Long Distance
10012-Charter Corporation (Tri-J)
10013-Access Services
10021-Mercury
10022-MCI Telecommunications
10023-Texnet
10024-Petricca Communications Systems
10028-Texnet
10030-Valu-Line of Wichita Falls
10031-Teltec Saving Communications
10033-US Sprint
10036-Long Distance Savers
10039-Electronic Office Centers of America (EO/Tech)
10042-First Phone
10044-Allnet Communication Services (LDX, Lexitel)
10053-American Network (Starnet)
10056-American Satellite
10057-Long Distance Satellite
10059-COMNET
10060-Valu-Line of West Texas
10063-COMNET
10069-V/COM
10070-National Telephone Exchange
10080-AMTEL Systems
10084-Long Distance Service (LDS)
10085-WesTel
10088-Satellite Business Systems (MCI)
10089-Telephone Systems
10090-WesTel
10093-Rainbow Communications
10095-Southwest Communications
10099-AmeriCall
10122-RCA Global Communications
10137-All America Cables and Radio (ITT)
10142-First Phone
10146-ARGO Communications
10188-Satellite Business Systems (MCI)
10201-PhoneNet
10202-ExecuLines
10203-Cypress Telecommunications (Cytel)
10204-United Telephone Long Distance
10206-United Telephone Long Distance
10211-RCI
10212-Call US
10213-Long Distance Telephone Savers
10214-Tyler Telecom
10215-Star Tel of Abilene
10217-Call US
10219-Call USA
10220-Western Union Telegraph
10222-MCI Telecommunications
10223-Cable & Wireless Communication (TDX)
10224-American Communications
10227-ATH Communications (Call America)
10229-Bay Communications
10232-Superior Telecom
10233-Delta Communications
10234-AC Teleconnect (Alternative Communication)
10237-Inter-Comm Telephone
10239-Woof Communications (ACT)
10241-American Long Lines
10242-Choice Information Systems
10244-Automated Communications
10245-Taconic Long Distance Service
10250-Dial-Net
10252-Long Distance/USA
10253-Litel Telecommunications
10255-All-State Communications
10256-American Sharecom
10260-Advanced Communications Systems
10263-Com Systems (Sun Dial Communications)
10268-Compute-A-Call
10276-CP National (American Network, Starnet)
10284-American Telenet
10286-Clark Telecommunications
10287-ATS Communications
10288-AT&T Communications
10298-Thriftline
10302-Austin Bestline
10303-MidAmerican LD (Republic Telecom)
10311-SaveNet (American Network, Starnet)
10318-Long Distance Savers
10321-Southland Systems
10322-American Sharecom
10324-First Communication
10331-Texustel
10333-US Sprint
10336-Florida Digital Network
10338-Midco Communications
10339-Communication Cable Laying
10343-Communication Cable Laying
10345-AC Teleconnect (Alternative Communication)
10350-Dial-Net
10355-US Link
10357-Manitowoc Long Distance Service
10362-Electronic Office Centers of America (EO/Tech)
10363-Tel-Toll (Econ-O-Dial of Bishop)
10369-American Satellite
10373-Econo-Line Waco
10375-Western Union Telegraph
10385-The Switchboard
10393-Execulines of Florida
10400-American Sharecom
10404-MidAmerican LD (Republic Telecom)
10412-Penn Telecom
10428-Inter-Comm Telephone
10432-Lightcall
10435-Call-USA
10436-Indiana Switch
10440-Tex-Net
10441-Escondido Telephone
10442-First Phone
10444-Allnet Communication Services (LDX, Lexitel)
10455-Telecom Long Distance
10456-ARGO Communications
10462-American Network Services
10464-Houston Network
10465-Intelco

....ACCESS...... CODES......

10466-International Office Networks
10469-GMW
10472-Hal-Rad Communications
10480-Chico Telecom (Call America)
10488-United States Transmission Systems (ITT)
10505-San Marcos Long Distance
10515-Burlington Telephone
10529-Southern Oregon Long Distance
10532-Long Distance America
10533-Long Distance Discount
10536-Long Distance Management
10550-Valu-Line of Alexandria
10551-Pittsburg Communication Systems
10552-First Phone
10555-TeleSphere Networks
10566-Cable & Wireless Communication (TDX)
10567-Advanced Marketing Services (Dial Anywhere)
10579-Lintel System (Lincoln Telephone LD)
10590-Wisconsin Telecommunications Tech
10599-Texas Long Distance Conroe
10601-Discount Communications Services
10606-Biz Tel Long Distance Telephone
10622-Metro America Communications
10634-Econo-Line Midland
10646-Contact America
10652-New Jersey Bell
10654-Cincinnati Bell Long Distance
10655-Ken-Tel Service
10660-Tex-Net
10666-Southwest Communications
10675-Network Services
10680-Midwest Telephone Service
10682-Ashland Call America
10684-Nacogdoches Telecommunications
10687-NTS Communications
10698-New York Telephone
10700-Tel-America
10704-Inter-Exchange Communications
10707-Telvue
10709-el-America
10717-Pass Word
10726-Procom
10727-Conroe-Comtel
10735-Marinette-Menominee Lds
10737-National Telecommunications
10741-ClayDesta
10742-Phone America of Carolina
10743-Peninsula Long Distance Service
10747-Standard Information Services
10755-Sears Communication
10757-Pace Long Distance Service
10759-Telenet Communication (US Sprint)
10760-American Satellite
10766-Yavapai Telephone Exchange
10771-Telesystems
10777-US Sprint
10785-Olympia Telecom
10786-Shared Use Network Service
10787-Star Tel of Abilene
10788-ASCI's Telephone Express Network
10789-Microtel
10792-Southwest Communications
10800-Satelco
10801-MidAmerican LD (Republic)
10827-TCS Network Services
10833-Business Telecom
10835-RCI/Teleconnect
10839-Cable & Wireless Communication (TDX)
10847-VIP Connections
10850-TK Communications
10852-Telecommunications Systems
10859-Valu-Line of Longview
10866-Alascom
10872-Telecommunications Services
10874-Tri-Tel Communications
10879-Thriftycall (Lintel Systems)
10881-Coastal Telephone
10882-Tuck Data Communications
10883-TTI Midland-Odessa
10884-TTI Midland-Odessa
10885-The CommuniGroup
10888-Satellite Business Systems (MCI)
10895-Texas on Line
10897-Leslie Hammond (Phone America)
10898-Satellite Business Systems (MCI)
10910-Montgomery Telemarketing Communication
10915-Tele Tech
10933-North American Communications
10936-Rainbow Communications
10937-Access Long Distance
10938-Access Long Distance
10951-Transamerica Telecommunications
10955-United Communications
10960-Access Plus
10963-Tenex Communications
10969-Dial-Net
10985-America Calling
10986-MCI Telecommunications
10987-ClayDesta Communications
10988-Western Union Telegraph
10991-Access Long Distance
10999-United States Transmission Systems (ITT)

Only a few codes are likely to work in any one area. The easiest way to find a working code is to dial the code followed by 700-555-4141 and listen for a verification message from the company. A few of these companies don't offer verification messages and only work in a few locations. 10698, for example, is used to route local calls via New York Telephone. But since all local calls are routed through New York Telephone anyway, it doesn't really serve much purpose except to occasionally get around PBX restrictions.

Timely TELEPHONE Tips

WHEN YOU RECEIVE A TELEPHONE CALL

Always Remember to

1. ANSWER AS PROMPTLY AS POSSIBLE.

   Try to answer before second ring.

2. IDENTIFY YOURSELF WHEN ANSWERING.

   "Mr. Brown's office, Miss Andrews."

   "Personnel, Mason."

3. SPEAK DISTINCTLY AND PLEASANTLY.

   Hold mouthpiece well up in front of lips.

4. AVOID TRITE OR ABRUPT PHRASES.

   "Who's calling?" . . . "Just a moment."

   "He's busy." . . . "He's in conference."

   "He's tied up." . . . "He isn't in."

5. VOLUNTEER THE "WHEREABOUTS AND WHENABOUTS" OF AN ABSENT PERSON.

   "He can be reached in Mr. Jones' office. . . . Extension 2094."

   "He is out of the building until 3 o'clock."

   "May I locate him and ask him to call you?"

6. VOLUNTEER YOUR OWN ASSISTANCE.

   "Is there something I could do?"

   "Could I help you?" . . . "or anyone else?"

7. REQUEST IDENTITY OF CALLER ONLY WHEN NECESSARY, AND IN A TACTFUL MANNER.

   "May I have your name?"

   "May I ask who this is, please?"

8. EXPLAIN OFF-THE-LINE DELAYS.

   "It's in the files—Can you wait a moment?"

9. TAKE MESSAGES WILLINGLY.

   Write essential details on a suitable message form; deliver promptly.

10. TRANSFER ELSEWHERE ONLY WHEN YOU KNOW DEFINITELY THE CORRECT PERSON OR NUMBER.

    Give caller these facts before transferring.

WHEN YOU MAKE A TELEPHONE CALL

Always Remember to

1. PLAN AN EFFECTIVE CONVERSATION.

   Get your thoughts in order before calling.

2. PLACE THE CALL YOURSELF, EXCEPT IN SPECIAL CIRCUMSTANCES.

   Make sure you are on the line ready to talk when the called person is reached.

3. HAVE THE CORRECT NUMBER (OR EXTENSION) IN MIND.

   Consult your directory, or personal number list.

4. LISTEN FOR DIAL TONE . . . DIAL CAREFULLY.

   See general information page in your directory.

5. IDENTIFY YOURSELF IMMEDIATELY TO THE FIRST PERSON ANSWERING THE CALLED TELEPHONE.

   "This is Mr. Johnson. . . . May I speak to Mr. Hodges, please?"

6. IDENTIFY ALSO, WHEN HELPFUL, YOUR OFFICE AND PURPOSE IN CALLING.

   "Mr. Brown, in Accounts . . . returning Mr. Green's call."

7. ASK WHETHER CALLED PERSON HAS "TIME TO TALK NOW' IF CALL IS LIKELY TO BE LENGTHY.

8. TRY TO COMPLETE YOUR BUSINESS ON ONE CALL BY SECURING INFORMATION OR LEAVING A MESSAGE.

9. VOLUNTEER YOUR EXTENSION AND THE BEST TIME TO REACH YOU IN CASE YOU REQUEST A "CALL-BACK."

10. KEEP YOUR CONVERSATION BRIEF AND BUSINESSLIKE.

FROM A DEFENSE DEPARTMENT PHONE BOOK

THE GALACTIC HACKER PARTY

continued from page 11

While we're at it, we might as well pass along the toll-free numbers to get the equivalent services in other countries. Calling these will connect you to an operator in the following countries. They will expect you to provide a means of billing and to know who you're calling:

Australia: 800-682-2878; France: 800-537-2623; Hong Kong: 800-992-2323; Italy: 800-543-7662; Japan: 800-543-0051; The Netherlands: 800-432-0031; Panama: 800-872-6106; Singapore: 800-822-6588; South Korea: 800-822-8256; United Kingdom: 800-445-5667; West Germany: 800-292-0049.

A Problem

Not all went smoothly, as is the case sometimes. Apparently, some low-life memorized a 2600 AT&T Calling Card number, which, fortunately, was unused by us. It was very easy to isolate the $3,000 worth of fraudulent calls billed to it. We should emphasize that such an occurence is very much the exception. In hacker circles, there's an unwritten rule: don't screw each other (we're speaking metaphorically for the moment). Whoever did this is not a hacker in the true sense, but a lowly, deceitful criminal. Unfortunately, many people judge hackers by the actions of such criminals. It's just not true; hackers have a very high code of ethics for the most part.

We think it's also important to throw some of the blame on AT&T, for continuing to be incredibly stupid. Why is it necessary to print these credit cards with all 14 digits screaming for attention? They could be much more inconspicuous. Or better still, the phone number portion (which is usually what the first ten digits comprise) can be eliminated entirely, since most people are capable of remembering this. Right now, a simple glance at the numbers is all it takes.

Since this was, in fact, our phone bill, we thought we'd share some of it with you. Feel free to find out who these people are and who they know overseas that may have placed the calls. AT&T may have already figured it out since they've had two months to do it.

415-422-3772 (Lawrence Livermore Labs)

301-345-5053

617-868-5765

718-768-7431 (Brooklyn, was called most frequently)

413-637-2870

There are many more, but these appeared most frequently. We suspect the person who did this didn't realize that American phone bills come with complete itemization, that is, the day and time of the call, the number called, and the location the call came from. In a surprising amount of countries, this information still isn't provided. Based on the information given to us, it appears obvious that the person lives in England, made a visit to Amsterdam for the convention, and then went to West Germany for a week before returning home. It's also obvious that they kept the code to themselves, as no two calls overlap.

We'd like to know what the hackers of the world think we should do about this. Suppose we find out who it is? Do we tell AT&T? Do we tell the world? Do we forget it ever happened? What is the proper response in your eyes?

What's Next

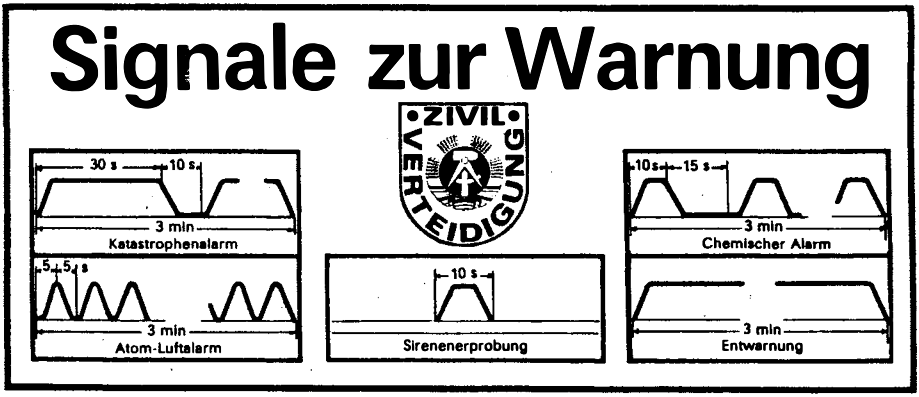
We must emphasize that this was the only truly negative thing that happened as a result of the Galactic Hacker Party. We hope that what came out of this conference will strengthen the spirit of hackers everywhere. In America, we need that strength desperately.

You may have noticed that our bulletin board network has pretty much collapsed, for varying reasons. Unfortunately, it seems to reflect a growing inertia, a lack of spirit. When we started operating BBS's, we expected them to grow and flourish. Why hasn't this happened?

In Europe, the hackers are continually expanding their grasp on technology, from pirate radio to voice mail systems to videotex to well-organized computer networks. Here, we seem to be reverting to one-upmanship and conformity when we should be finding new toys of technology to play with and shape to our needs. What happened to the huge conference calls, the hundreds of hacker bulletin boards, the clever pranks, the legendary phone phreaks? Are we afraid? Are we losing our spirit? Or are we just getting comfortably dumb?

A look through these pages will tell you that there are plenty of entities just aching to gain control of technology and in due time, the individual. This magazine is only one voice. We need more.

If you think you can do something, then you can. People all over the world know and understand the spirit of the hackers. It's up to all of us to keep it going.



NOW HEAR THIS

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

INDIVIDUAL SUBSCRIPTION

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

CORPORATE SUBSCRIPTION

□ 1 year/$45 □ 2 years/$85 □ 3 years/$125

OVERSEAS SUBSCRIPTION

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

LIFETIME SUBSCRIPTION

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

BACK ISSUES (never out of date)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25

TOTAL AMOUNT ENCLOSED: □

Contained Within...

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

we
are
the
dead