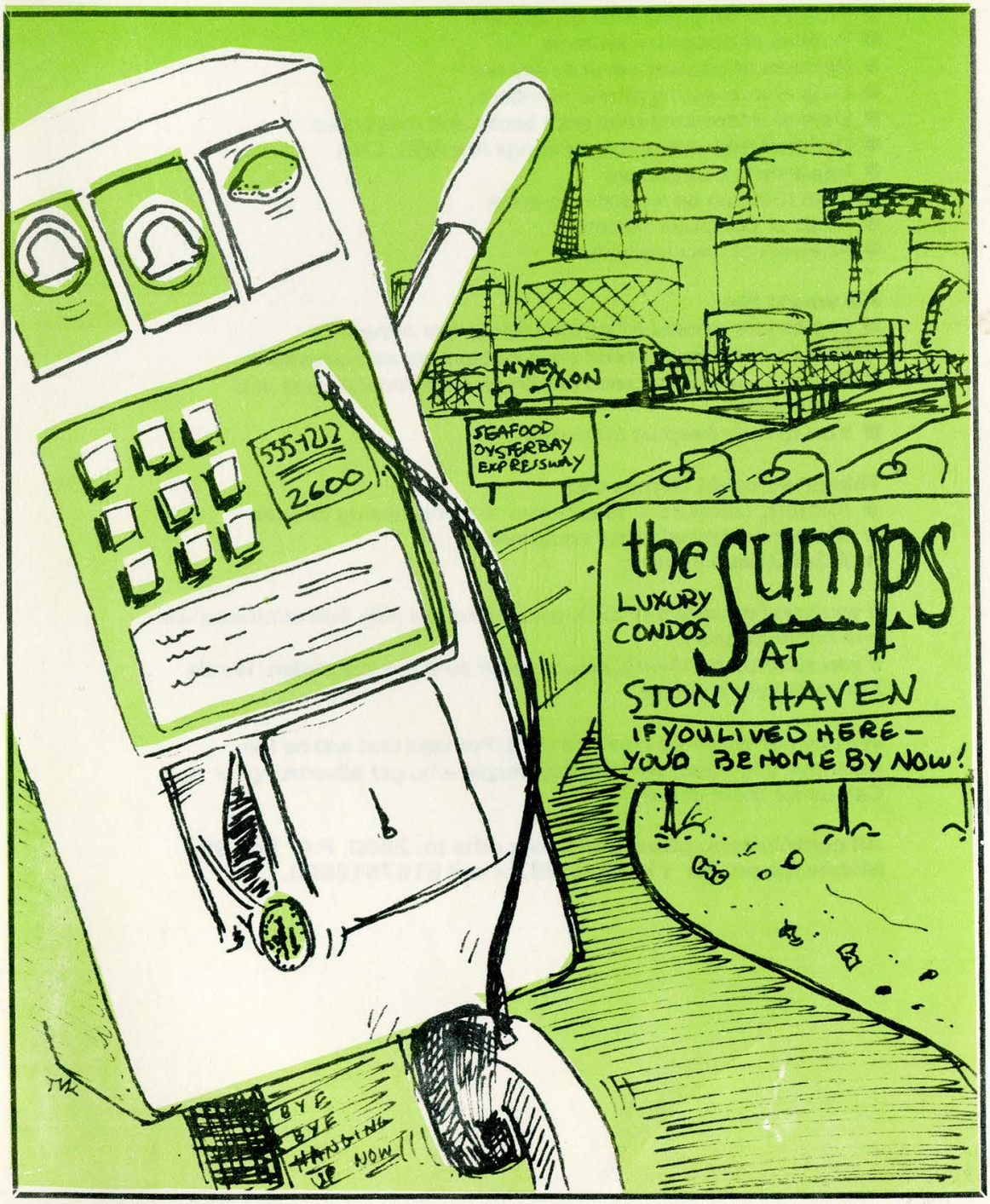
2600

The Monthly Journal of the American Hacker

Volume 4, Number 9 September, 1987 $2



2600 WANTS YOU!

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

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

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

Things we could always use:
- ★ Printers, computers, telephones, and interesting devices
- ★ More modernized office equipment
- ★ A 2400 baud modem

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

We pay our writers a small amount. Perhaps that will be the incentive you need. We also pay people who get advertising for us. Call us for more details.

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

As you thumb through this issue, you may notice that we've used a few more graphics and displays than we have in the past. Ever since we started publishing in 1984, people have been sending us interesting artifacts, copies of their phone bills, nasty letters from phone companies, stupid letters from phone companies, pictures, bits of data, drawings of all sorts—the list goes on. And the pile gets bigger. Well, our pile has been mounting and we figured it was time to do something about it; namely, to print some of these fascinating treasures.

In the past, some of our readers have said that there are too many pages of straight text in 2600—they need a break now and then. That's why we've decided to give you an idea of the kinds of things we can use in the future.

There's no reason why we can't have pictures of strange telephones or large computers in every issue. We have the ability to print them, something we didn't have a year ago. All we need are the people to find interesting shots, get them on film, and send them in. Odds

(continued on page 16)

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Peter Kang

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Bernie S., Mike Salerno, Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

Production: Mike DeVoursney.
Cartoonists: Dan Holder, Mike Marshall.
Editor Emeritus: TSH.

2600 *(ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending 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 –$15 individual, $40 corporate.
Overseas –$25 individual, $55 corporate.
Back issues available 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 11953-0752.
Telephone: (516) 751-2600

Worldnet: Getting

by Hank@Taunivm.Bitnet

First off, let me say that I am on the other side of the fence. My job is to make sure the system I work for is secure and that there are no hackers or crackers trying to do damage to the system I am employed to defend. In one instance, I assisted the police in collecting all the necessary information to create a court case against a cracker. The kid in question (a high school student) ended up getting a year of civil work. I subscribe to this magazine not to learn how to do something illegal but rather to learn what others are trying to do to me. Knowledge is a tool and by hiding a tool you gain nothing. Therefore, I have decided to explain how international computer networks work, how they are tied together and what services you can hope to receive from them.

There are dozens of computer networks—all of them spawning off the grandfather of all networks: Arpanet. Today, it has grown so large that it is known as The Internet. As more and more networks begin to interconnect, the concept of a Worldnet becomes feasible.

Basic concepts

All users are known by three variables: userid, nodename, and network. A userid can be the person's initials, or the person's last name, or anything else the person decided upon when he opened his computer account. A nodename is also known as a hostname. It designates the computer the user is using. The network indicates which of the two dozen or so networks the computer is connected to. If you look at my name at the top of this article, you will see that my userid is Hank, my nodename is Taunivm (that is in Israel, in case you were wondering), and my network is called Bitnet. The nodename and network section of a user's "handle" has been undergoing a transformation in the past few years and this will be explained later.

The one common protocol that all networks talk is something called RFC822 standard mail. Within individual networks there are other protocols which will be covered where necessary.

Arpanet

This network is based on a protocol called Tcp/Ip. (I know there are people out there reading this and saying, "What does Tcp/Ip stand for?" But I do not think it is important to know what the letters stand for. When it is important, I will explain it.) It allows for three major applications: FTP, SMTP, and Telnet. FTP stands for File Transfer Protocol and allows a user on one machine to extract a file from any other machine on the network (assuming you know the read password) or allows a user to write a file onto any other machine assuming you know the write password for the destination user and machine. SMTP stands for Simple Mail Transfer Protocol and allows users to send electronic mail almost anywhere in the world. Telnet is a remote-login application. It is not Telenet. But it does basically the same thing. You specify the machine you want to login to, and Telnet makes the connection from your machine to the one you specified.

Most links within Arpanet are 56kb leased lines although there are cases where it may be higher or lower. There are other networks that are modelled after Arpanet: Csnet (Computer Science network), Nsfnet (National Science Foundation Network—which interconnects all supercomputers in the United States), and a few smaller ones. Csnet, up until recently, used primarily X.25 connections via Telenet to establish a connection. They are now switching more and more links over to leased telephone lines. Nsfnet uses primarily T1 lines which run at 1Mb per second. In case you were wondering, Arpanet stands for Advanced Research Projects Agency and is owned by the U.S. government. All of these networks use the Tcp/Ip protocol and are therefore part of an evergrowing Internet.

Bitnet

This network spans 27 countries (U.S.A., Canada, West Germany, France, Italy, The Netherlands, Finland, Denmark, Spain, Turkey, Israel, Japan, Mexico, Taiwan, to name a few) and has over 1800 computers interconnected. It uses a protocol different than Arpanet but the one common language they talk is electronic mail (RFC822). The European segment of the network is called EARN (European Academic Research Network) and the Canadian section is called NetNorth. All links within Bitnet/EARN/-NetNorth are 9600 baud leased lines. Bitnet stands for Because It's There or Because It's Time. It all depends on who you ask. Bitnet is not

Closer Every Day

the largest network by computer hosts, but is the largest by number of connected countries. If you are an academic institution or a research lab, all you need to do is pay a membership fee per year to Bitnet, Inc. (varies between $1,000-$10,000) and order a leased line from Telco to your nearest neighbor that has a connection to Bitnet.

UUCP

Unix to Unix Copy Program Network is a freewheeling, anarchy-type network. It is unknown how many computers are connected to this network but estimates vary from 4,000 to 10,000. Lately, some organizers are trying to put some order into UUCP. It is a slow and grueling process but one that I hope they will succeed at. It has the worst reputation for mail delivery, where delays can be sometimes a week and it is not infrequent that the system loses the mail.

"There are dozens of computer networks...as more and more begin to interconnect, the concept of a Worldnet becomes feasible."

Others

Here is a brief list of some of the other networks that share RFC822 mail:

MFENET: Magnetic Fusion Energy Network
SPAN: Space Physics Analysis Network
JANET: England's National Academic Network
VNET: IBM's corporate internal network
Easynet: DEC's corporate internal network
EUnet: European section of UUCP

There are many other smaller networks that are starting to get off the ground, but as you will see later on, the world of networking is moving away from the concept of a "xxxxNet" to one that imposes a hierarchical structure on all networks.

When you add up all the networks and all the machines that can exchange RFC822 mail, the number of machines (from a VAX 730 up to a Cray X/MP) approaches 20,000. Some of the larger systems have 50,000 registered users on their systems while more typically it is around 2,000 users. That means that as a rough estimate, there are about 40 million users that are accessible via RFC822 mail. This grows even larger when you consider that there are experimental gateways that allow networks like Dialcom and MCI Mail to pass RFC822 mail into the Internet and vice versa (no, I will not tell you where they are or how to use them). Most of the users are students, professors, academics, researchers, and school administration personnel. The number of corporate users, like IBM's 200,000 Vnet users, only make up about 10 percent of the network. What makes this Worldnet system so attractive is that for a large part it is free to use. The university or the company pays Telco for a leased line and connects to the network of their choice. The users of the newly connected computer are then given free access to the network (certain universities impose access restrictions on their users). European sites will soon be undergoing a severe hardship. Their PTTs will require volume charging, so each site will have to restrict usage by their users. At present charging by European PTTs is still on a leased line monthly cost.

Since it is a free system, abuse is closely monitored. For example, it is considered bad manners to start a chain letter in the network, since it can quickly grow to saturate the network. Users are caught and in general they understand that disrupting the network will only cause their "free" and genuine mail to be delayed also.

Addresses

Now for a brief tutorial on how to read network addresses. All RFC822 mail addresses are composed of a LHS and a RHS (Left Hand Side and Right Hand Side). You look at the address and scan for an @-sign. This is the separator between the LHS and the RHS. The LHS is considered the local part of the address. Examples:

Hank
John Smith
steve%hbo.HAIRNET
philco!sun!munarri!john

These are all samples of LHS addresses. The first two are simple userids. The third one is a gateway. It says that there is an indirect network called HAIRNET that has a machine on it called hbo and you wish to contact the user named

(continued on page 11)

operating with difficulty

by Wintermute

New York Telephone recently introduced a new service to its customers. It's called operator service. Other telephone companies around the nation are doing the same thing. When customers in New York dial 0, they get connected to a New York Telephone (NYT) operator. When they dial 00, they get connected to an AT&T operator (assuming they've chosen AT&T as their long distance company).

The equipment used for the NYT operators consists of a Northern Telecom DMS-200 switch running TOPS (Toll Operator Position System) software. This change, while refreshing, has brought about many problems—not to mention my pet peeve: when an operator answers, there is no longer a beep.

The most important problems can be grouped into two major categories: routing and hardware.

Routing Problems

• From coin phones you cannot dial 00 to get an AT&T operator. Instead you are routed to an intercept recording.

• As an alternative to dialing 0, you're supposed to be able to dial 10xxx0# to get an operator, where xxx is the three-digit number of the long distance company. This is assuming that the long distance company offers operator services in the first place. But from a pay phone, dialing 102880# (288 is the three-digit number for AT&T) gets you an NYT operator! Dialing 107770# or 103330# is supposed to get you a Sprint operator. But instead you get an NYT operator again.

• New York Telephone "coin craftsmen", those guys who fix our pay phones, will be in for a nice surprise. There is a coin test number which checks to see if a pay phone's "negative start package" or red box is working. From the 212 area code you dial 0-212-959-1230 and from 718 you dial 0-718-959-1230. (Other areas may allow you to dial 0-959-1230.) The way NYT is routing traffic, a 0+ (zero plus) call within New York State (and the small part of Connecticut served by NYT) gets sent to the TOPS DMS. The 959-1230 is handled out of an AT&T TSPS. When the TOPS receives the 212-959-1230, it searches its database of exchanges and sees that 959 is not a va16, 212) as well as "invalid" NPA's (710, 200, 210, 700, 999, etc.). This presents a problem when trying to call Alliance Teleconferencing (0-700-456-1000). The TOPS receives 700-456-1000 and sees that 700 is not a valid New York area code. It then routes you to an announcement: "Your call cannot be completed as dialed. Please check the number or ask your operator to help you."

• NYT operators can't dial 959, 800, 900, 976, 950, 970, 540, and 550 calls. I can understand not being able to connect you to most 800 numbers, but the 800-698 exchange is a new one that's *owned* by New York Telephone. Yet the operator cannot dial it.

• There is one trick which comes in handy. To get free directory assistance (DA) from a Customer Owned Coin Operated Telephone (COCOT), you dial 0-NPA-555-1212. If the NPA is within the New York City area (212, 516, 718), the call speeds straight through to DA. (Note: the caller must also be within that area.) Most COCOTs let you dial 0+ without asking for money, so your DA call would be free. Similar variations of this trick probably work in other parts of the country.

Hardware Problems

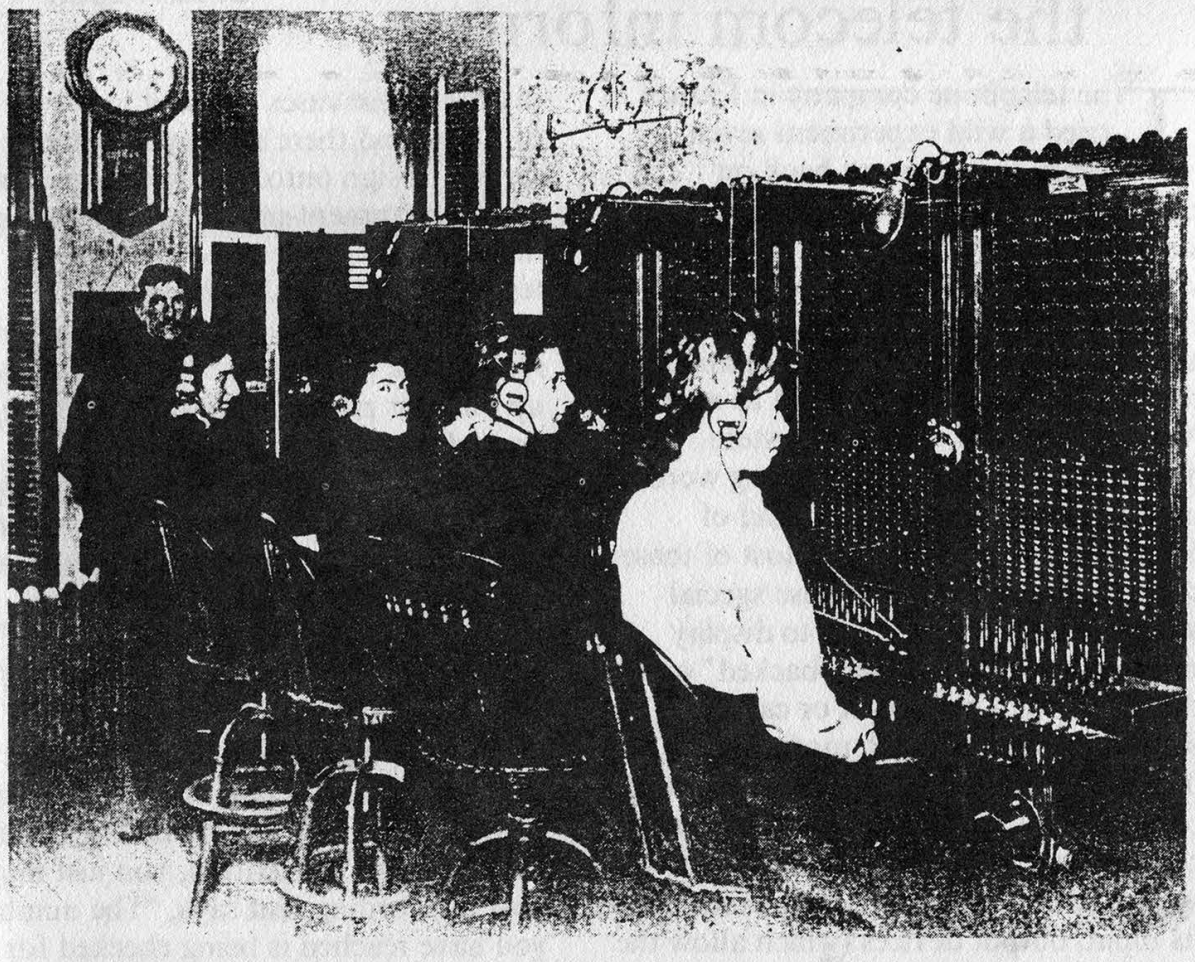
• As I mentioned before, the operator does not beep when she answers a call.

• When you dial a 0+ call, you are given a choice of dialing 0 at the tone or entering your calling card number at the tone. If you call from a pulse or rotary phone and don't respond with touch tone after the tone, an operator will arrive to assist you. Sometimes, right before the "enter calling card" tone (sounds like a # tone melting into a quick dialtone) you hear a quick second of distorted noise, like a fragment of speech. When this happens, if you are on a pulse phone and can't dial a 0 in touch tone, the calling card tone will repeat every couple of seconds *forever!!* This seems to be happening less now than when they put the first TOPS in Manhattan sometime last year.

• There seems to be an overwhelming problem with intelligible crosstalk. Many times right after the operator answers you hear a loud click and then a burst of 12 multi-frequency (MF) digits, followed by "Operator, may I help you?" Both operators will then say there is a "crossed line" and hang up.

• This problem is by far one of the worst. It's been reported that when emergency interrupts

(continued on page 18)



Traffic Department Toll Board Circa 1896 at offices located in the Lowe Building at the corner of Orchard and North Streets. Left to right, John Ayres, Edna Ferris, Jenny Finch, Mina Brown and Della Rogers. Equipment installed 1896. Picture taken in 1902.

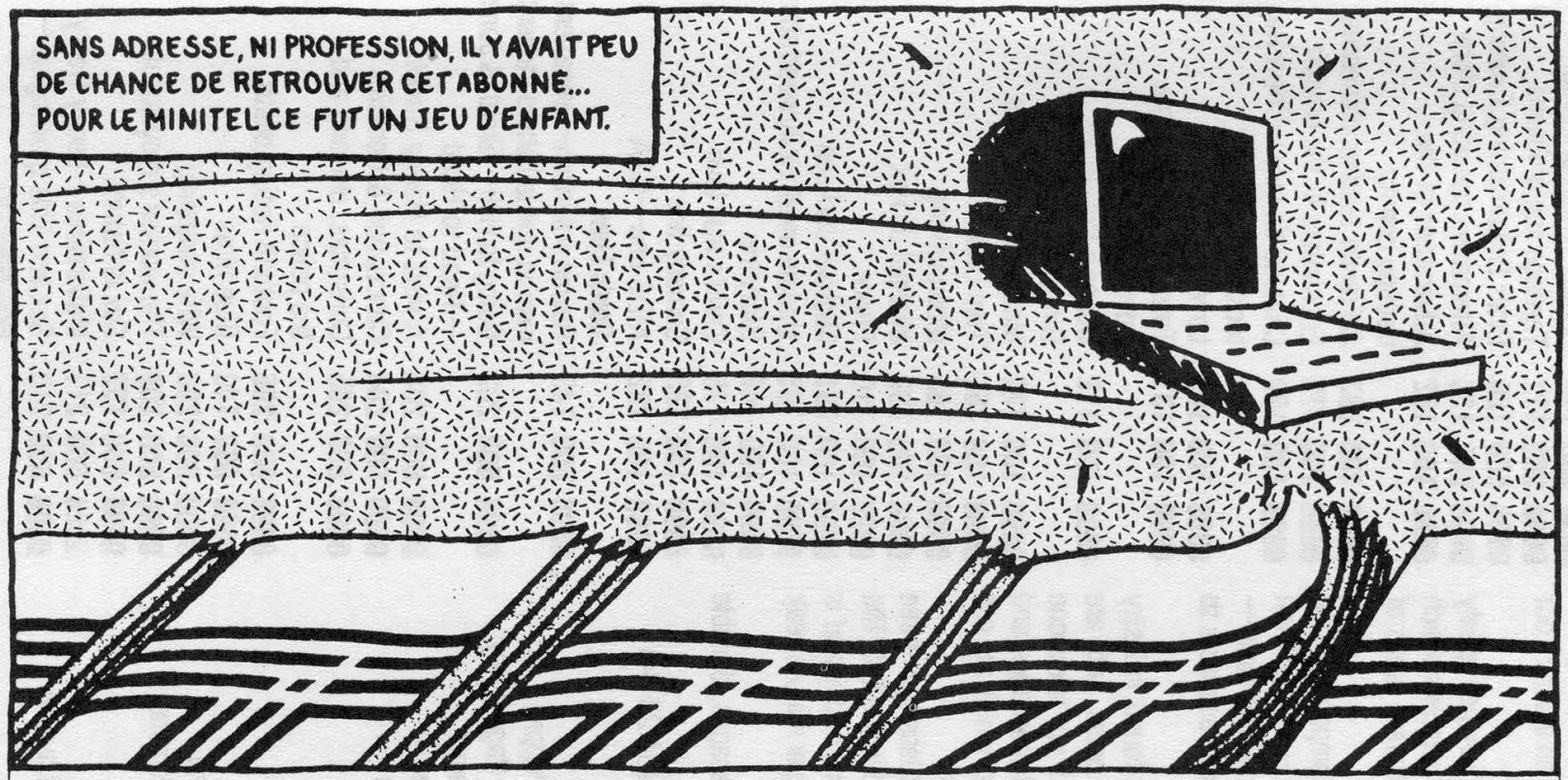
Present Day Toll Board for Operator handled Long Distance Calls.

the telecom informer

BY AL FRESCO

The telephone company in France tried a wild experiment seven years ago: they cut back on printing telephone directories and started giving out computer terminals with built-in modems to all of their customers. But replacing directory assistance wasn't all they had in mind—the terminals can also be used to access Minitel, France's videotext system. Videotext is an all-encompassing word used to describe nearly any kind of home information service. Most of these services in other countries use special adapters built into TV sets to display information that is "piggy-backed" on the carrier of a broadcast or cable station. Minitel is much more flexible because it uses the telephone network to connect to users (which makes two-way communication with the videotext system easy) and computer terminals for its input/output devices (which allow the user to enter all sorts of interesting data, as opposed to just pressing a few buttons on a numeric keypad). Two years ago, Minitel allowed outside companies to provide services over the videotext network. It soon became evident that one of the things videotext customers were willing to pay $10 an hour of online time for was sex. Message services (messageries) sprang up giving anyone in the country a chance to talk dirty, either with on-line chatting or via electronic mailboxes. These message services account for 16 percent of all Minitel traffic. Service providers advertise heavily in the Paris Metro and on public billboards with lines like: "For a good time dial 36-15 and type in "MARIE". Some of the sleazier services actually hire people to participate in conversations and keep them going as long as possible (the longer you type, the higher your bill), and some even sleazier try to program computers to do the same thing. Experienced Minitel users say that these ruses are easy to see through, and there's always a better service to sign onto. To use Minitel, plug your government-provided terminal into the wall, and the telephone into the terminal. Dial 36-15 and type in the name of the service you want. That's it. Any online charges you run up will show up on your phone bill. No need to log on and there's no way to hack passwords. Employers who are unhappy with large Minitel bills run up by their disaffected staff during office hours can buy software that blocks calls to the message services. Have any readers of *2600* found their way onto Minitel yet? The thought of an entire population using computer terminals, not just the technologically literate minority, is truly revolutionary....If you try calling certain payphones in Manhattan, you just might hear a recording that says, "The number you have reached is being checked for drugs." Or words to that effect. As part of the ongoing war against drugs in New York City, police have received the cooperation of New York Telephone in cutting off incoming service to phone booths that were "under siege" by drug dealers. Dealers and pushers along "Cocaine Strip" (Amsterdam Avenue from 80th to 96th Streets) and other drug supermarkets were forced to fight high-tech fire with even higher tech: they now carry beepers so that their connections can reach out and score without having to go through public payphones. Beepers are also rumoured to be in use by all sorts of other illegal operations, including numbers runners and stockbrokers. For some strange reason, no one has talked about having the Secret Service or the FBI raid any beeper companies because of all the crime-oriented traffic passing through their computers. Nice to know that some people are still protected by their Constitutional rights....

THIS AD FOR MINITEL IS FOUND IN FRENCH PHONE BOOKS.



Retrouver un correspondant : faites-le en Minitel.

Le Minitel, c'est un petit terminal branché sur le téléphone qui permet de faire toutes sortes de choses en direct : retrouver quelqu'un rapidement n'importe où en France avec l'Annuaire Electronique ; consulter son compte bancaire, les horaires des transports, les programmes de spectacles, faire des achats sur catalogue...

C'est tellement pratique qu'on a toujours un service à lui demander. Certains de ces services sont gratuits, d'autres payants ; tout dépend du fournisseur.

La communication elle, ne coûte en général qu'une taxe téléphonique de base toutes les deux minutes aux heures de plein tarif*.

Vous pouvez louer un Minitel dans toutes les Agences Commerciales des Télécommunications. Et là où le Minitel est proposé en remplacement de l'annuaire papier, vous pouvez en obtenir un sans supplément à votre abonnement téléphonique.

(*) Pour le Service Annuaire Electronique, là où le Minitel est proposé en remplacement de l'annuaire papier, les trois premières minutes sont gratuites (accès par le 11).

Alors, la prochaine fois, allez cherchez vos correspondants en Minitel. Appelez gratuitement le Numéro Vert 05.10.20.10 pour avoir de plus amples renseignements, notamment sur les coûts de Télétel.

La puissance de l'informatique, la simplicité du téléphone.

England's Mass Announcements

by John Drake

Besides offering a regulated loop or party line, British Telecom has also created an industry out of the pre-recorded message.

The most upmarket version, which they openly publish, consists of the Citycall numbers which offer hourly reports based on different areas of the stock market.

But industrious third party companies have taken up the idea and offer—via British Telecom—recorded messages and services—anything from horoscopes to comedians' acts to fetish fashion information.

Advertisements for this new found industry can be found in the tabloid press and are controlled from a specially set up telephone exchange handling the recorded messages and direct dial cellular phone numbers which are not formally listed in any directories.

On average, each call will last less than three minutes. All local calls are billed in the UK. The rate structure is based on the time of day and is raised to an average of 38 pence per minute peak and 25 pence off peak.

Here is a list of recorded messages, dialable from anywhere in England:

0898 300 153	Jenny Blythe (34-23-34)
0898 300 101	Page 3 Girls
0898 300 146	Lipstick
0898 300 162	How to be a Yuppie
0898 300 158	Kevin Petts—Page 7 guy
0898 300 100	Other programmes
0898 300 445	Couple troubles
0898 300 416	Sex & Women
0898 300 417	Sex & Men
0898 300 345	Dateline
0898 300 377	Loveline
0898 300 346	UFO Line
0898 300 370	Adult Joke Line
0898 300 444	Teenage problemline
0898 300 164	Cleo Rocos
0898 300 165	Mr. Know-all
0898 300 110	Horoscope & Lovelife predictions
0898 300 154	The Wallys—shocking new version
0898 300 141	Pillow Talk
0898 300 166	Confessions of an Air Stewardess
0898 300 183	Why leather is sexy
0898 300 143	Boots—Thigh or Ankle
0898 300 172	Teenage sex problems
0898 500 109	Eva's Embarrassing Evening
0898 500 123	Alternative speaking clock
0898 100 162	Adventures of the bathing beauty
0898 100 133	A French teacher confesses
0898 100 175	Encounters in the hayloft
0898 100 129	Chateau de vice—Chevette rock star
0898 100 167	Lovecasts
0898 100 131	Tarzan & Jane Jungle Adventures
0898 100 112	Donna's Disastrous Dinner Party
0898 100 720	Madonna—the facts
0898 100 755	Tom Cruise
0898 100 765	Moonlighting
0898 100 700	Michael J. Fox
0898 100 710	Prince
0898 100 781	Michael Jackson
0898 100 795	Update on all Hollywood stars
0898 100 740	Storyline
0898 100 775	Carol's true love
0898 100 735	Comedy line
0898 100 782	AIDS line—Q&A
	Comic Lines
0898 600 143	Rowan Atkinson—Impatient man in queue behind student
0898 600 202	Going to Hell—Smith & Jones—Head to Head
0898 600 203	A visit to Harley Street
0898 600 204	Conception & Genetics
0898 600 205	Christmas, drinking and the police
0898 600 206	Football rioting death
0898 600 149	Blue films
0898 600 208	Wife swapping
0898 600 209	The women's movement
0898 600 152	Sex is natural
0898 600 211	Millionaires—Lenny Henry
0898 600 213	Sex and kids growing up—Bob Newhart
0898 600 218	The driving instructor
0898 600 219	Introducing tobacco to civilisation
0898 600 220	The cruise of the SS Codfish

(continued on page 16)

The Growing Worldnet

(continued from page 5)

steve. The %-sign is used as a kludge to indicate indirect addressing via a gateway that is not directly addressable from all over the WorldNet. The last example is one of UUCP addressing. It reads from left to right. With standard RFC822 addresses, you do not need to know the path the mail will take to get to its final destination. The system takes care of that. UUCP is dumb in that respect. You need to know the path the mail will take. So example 4 says to send it to a machine called philco, which will send it to a machine called sun which in turn will send it to a machine called munarri, which has a user called john. You can see why people hate UUCP addressing. This type of "bang" addressing is slowly being phased out for the new style of addressing detailed below. But there are still many UUCP sites that prefer their "old" ways. Then again, there are still a lot of people who like Cobol.

Here are some examples of a RHS address:

taunivm.bitnet
wiscvm.wisc.edu
relay.cs.net
decwrl.dec.com
vax.camb.ac.uk
vm1.tau.ac.il

The first is an example of the old style of addresses—taunivm.bitnet. It is a nodename and a network identifier. The next three are examples of Arpanet addresses. They read from right to left and are tree based. The right-most token represents the higher authority, such as .EDU (educational), .NET (network information center), or .COM (commercial). It no longer makes a difference if wiscvm.wisc.edu resides in Arpanet or Bitnet or Csnet. It may indeed be directly connected to all three. The user shouldn't care what network the end user is connected to. Imagine if your friend was connected to Sprint while you used ATT. It shouldn't make a difference in your dialing to know that the end destination is being serviced by Sprint. Just dial the number. That is the concept of "dotted domain names".

As soon as you leave the United States, things get even more organized. Every country has an ISO (International Standards Organization) country code. Within each country, an authority decides what second level domain names to assign—such as .AC (academic), .RD (research and development), .COM (commercial), etc. As you move from the right to left of the RHS address, you move from the macro to the micro. Once again, it is important to note that the concept of what network the user resides on becomes a "thing of the past".

Putting it all together, we end up with addresses that might look like these:

Hank@vm1.tau.ac.il
John Smith@decwrl.dec.com
steve%hbo.HAIRNET@relay.cs.net

In conclusion, the Worldnet supplies electronic mail traffic for free to users with an account on any machine that is connected to one of the networks listed above. The institution ends up picking up the bill for the leased line, while the user only gets charged for the local cpu time and connect time used to create and send the letter. Abuse (chain letters, mass mailings, commercial use of the network, etc.) is frowned upon by the ones who run the networks as well as the hackers who make use of them. If you use the network, don't abuse it.

For further reading: Communications of the ACM, October 1986, Notable Computer Networks, Quartermain and Hoskins.

Notes and Replies

Dear *2600*:

First off, thanks to you I now have the Radio Shack Duophone Computerized Phone Accountant model 1000. What a nifty little device! I always wondered who the babysitters were calling...and for how long.

Secondly, here's some cellular phone information that the dealer gave me after I showed him copies of *2600* and its cellular-related information. He was very happy to swap information.

Thirdly, in reply to The Sorcerer's letter (*2600*, August 1987), if the police were as inept in their "capture" as he claims they were, it says one of two things: either The Sorcerer wasn't as "discrete" as he should have been, or the rest of the hacking/phreaking community is put on warning when a "Robocop" starts cleaning up.

The Sorcerer also requested information regarding Bill Landreth (aka The Cracker), author of "Out of the Inner Circle". Enclosed please find the cover story, September 20, 1987, to the Southern California computer magazine "Byte Buyer", which I penned. This should give you all the information you may need on Mr. Landreth.

Lastly, I run a BBS called Mainstreet Data (619-438-6624). In it is a section called TAP Magazine. This section of the board is filled with information gleaned from the AP wire, international, national, and all 50 states individually regarding the keywords: hacking, phreaking, and computer crime. It is an extremely popular section of my large online system. To receive a complimentary account, call, enter 12 for your ID, for your password enter DAKOTA, and at the first command prompt enter PRO (of course there is no punctuation). You will be given access to the entire system. I would be happy to be one of your West Coast BBS envoys.

Thanks for being!
Rainer Mueller

Thanks for the cellular info. We will try to do something with it for a future issue.

Your article on Landreth was very informative and while we cannot print it in its entirety, here are the main points for the benefit of our readers. As a result of intruding on GTE Telemail back in 1983, Landreth was sentenced to three years of probation. He then put out a book entitled "Out of the Inner Circle" which sold over 50,000 copies. Because of this, he became something of a celebrity, a role which he apparently wasn't comfortable with. In the fall of 1986 he vanished entirely. He wasn't seen again until early this summer when he was discovered in a town 40 miles north of Portland, Oregon, "apparently dressed like a bum". He was arrested on a charge of federal probation violation and sentenced to five years in prison. He is due to return to court on October 13. His sentence may be commuted at that point or he may receive a different sentence. Regardless, as of this writing, Landreth was still incarcerated at the Metropolitan Correctional Center in downtown San Diego.

As ones who have seen the results of being thrust into the spotlight unwillingly or half-willingly, we find this whole series of events to be quite sad and unfortunate. Too often, the media jumps on individuals for one thing or another, completely forgetting that they are mere human beings, subject to the same fears and insecurities we all have at one time or another. It's happened to rock stars, lottery winners, and crime victims. Now it's happened to a computer hacker.

S SPEAK OUT

Clearly, Landreth should not be locked up in jail. His "crimes" have hurt no one more than himself. Imprisonment in this case is barbaric and inhuman. We call on our readers to speak out against this kind of injustice in whatever way they can. And we wish him well.

Readers who want to hear more about this case should call the above-mentioned board. Hopefully, the facts will be passed around on different bulletin board systems as well.

We thank the many readers who have expressed an interest in running bulletin boards for 2600. Last month we mentioned certain features we would require: full access to all callers, private mail that ensured privacy, and no verification of identity for users. If you want your board to be a 2600 board, it must also have 24-hour access, 300/1200 baud capability, the ability to store at least 100 messages on at least 3 public boards, the ability to handle at least 100 users, storage capacity for certain text files, and a way of having information uploaded. If you can meet those requirements, then contact us. All kinds of computers are welcome as are all kinds of software, provided they can handle the above.

An Explanation

Dear *2600*:

Regarding my September letter, allow me to clarify my position—you're right that I made a mistake in ripping off the phone company. That was something I did because I was having fun with BBS's at the time, and when we discovered that dial-up and figured out what was happening, we went a little berserk. But like the kid whose interest is sparked by a ninja movie and later gets into serious martial arts, that was where I got my first glimpse into the world of amateur hacking. Since then, I've been trying to learn more from BBS's and *2600*.

I just wanted to clear things up so I don't sound like a total defiant scumbag.

Also, I think Audie's idea of a special issue sounds good.

Respectfully,
The Sorcerer

Your comments have been noted. And, by the way, that was your August letter you were referring to. This is your September letter.

Newsstand Update

Dear *2600*:

You've been saying that you'll be on newsstands soon. Is this in fact in the works?

Curious

We are in the process of working out an arrangement with a distributor in New York City. Right now you can find 2600 in some bookstores and magazine stands. Among them are: Hudson News, Coliseum Books, Soho Zat, and St. Mark's Books (all in New York City) with more on the way. We're also working out deals with book shops in England, Holland, Germany, and Finland. If you have any ideas or can help out, contact us. We'll keep you posted.

Misinformation? Us?

Dear *2600*:

I was very upset with the misinformation you printed in your September issue. In an answer to a letter, you said that pen registers can be bypassed by using cordless phones. Nothing could be further from the truth! Pen registers record the number you're dialing no matter what kind of a phone you're using. And your suggestion of dialing on a cordless phone to avoid the pen register and then hopping back onto a regular phone to avoid being monitored on the radio is ridiculous, to say the least. I

(continued on page 18)

Author: Mel Beckman
Abstract: Explains how to locate and decrypt the user-ID and password of the master security officer.

Introduction

The System/36 password security file is encrypted in a slightly more vigorous fashion than the System/34 method (which simply inverted the bits). However, IBMs Rochester cryptographers are not exactly Enigma material, since only three hours effort was required to crack this scheme.

Step by step

1. Locate the file #SECUID0 on disk using a catalog listing, which gives the starting block number. Multiply this number by 10 to get the starting sector number. Add 1 to that, since we're skipping the first sector of the file, which contains pointer information.

2. You must now print out or examine this disk sector. You can use either the PATCH procedure, or Alter/Display option 2. If you use Alter/Display, you'll have to convert the number to hex (PATCH allows you to enter a decimal sector number, followed by the word 'DEC'). The file contains 128 byte records, each record starting with X'01'. This procedure will show how to decrypt the user-ID and password for the first record - which is the master security officer record; thus we are concerned with just the first line (16 bytes) of the sector.

3. The remaining steps use the attached worksheet to perform the decryption. After you've displayed the sector from disk, write down the 2nd through 9th bytes on worksheet line 1. Be sure to skip the first byte (which is X'01').

4. Subtract the hex bytes on line 2 from the corresponding bytes on line 1 and write the result on line 3. Treat each byte as an isolated number - don't borrow from neigboring bytes. If the result goes negative, don't worry; just use the complement that you come up with after subtracting. A hexadecimal calculator is handy here if you're not fluent in hex arithmetic. The result on line 3 is the user-ID in EBCDIC, which you can convert to characters using the attached EBCDIC chart.

5. Now write down the 12th through 15th bytes on the worksheet line 4. Note that you are skipping over two bytes.

6. Subtract the hex bytes on line 5 from the corresonding bytes on line 4 and write the result on line 6.

7. Write down the 4th through 7th bytes on the worksheet line 7. Subtract the hex bytes on line 7 from the corresponding bytes on line 6 and write the result on line 8, which is the password in EBCDIC.

Security Decryption Worksheet

1. __ __ __ __ __ __ __ __

2. 32 0A B9 16 8C 59 7E A3

3. __ __ __ __ __ __ __ __ (User-ID in EBCDIC)

4. __ __ __ __

5. B9 16 8C 59

6. __ __ __ __

7. __ __ __ __

8. __ __ __ __ (Password in EBCDIC)

Example: 0106CB9B F95132BE E338D52B D0BF6D3C

1. 06 CB 9B F9 51 32 BE E3

2. 32 0A B9 16 8C 59 7E A3

3. D4 C1 E3 E3 C5 D9 40 40 (User-ID is 'MASTER')

4. 2B D0 BF 6D

5. B9 16 8C 59

6. 72 BA 33 14

7. 9B F9 51 32

8. D7 C1 E2 E2 (Password is 'PASS')

(continued from page 10)

UK Mass Announcements

Citycall

0898 121 212	Citycall directory
0898 121 220	General market report
0898 121 221	Company news
0898 121 225	Active shares
0898 121 230	Foreign exchanges
0898 121 235	Currency Hotline
0898 121 240	Leading shares A-K
0898 121 241	Leading shares L-Z
0898 121 245	Traded options
0898 121 246	Options review
0898 121 250	USM
0898 121 255	Recent issues

(Note: These numbers seem to be reachable from England only. However, we know there's got to be a way around that. It's possible the British Telecom operators at 800-445-5667 will put calls through to the above. It's also possible blue boxes can get through. We'll let you know what we find out. In the meantime, the following numbers are meant to supplement the list from our July, 1986 issue. All of them need country code 44.)

1-2468015	Dialing Instructions
1-2468017	Dialing Instructions
1-2468026	Financial Report
1-2468035	British Telecom Guideline
1-2468040	Christian Message
1-2468050	Challenge Line
1-2468060	Racing Bulletin
1-2468072	VD info
1-2468080	Newsline
1-2468088	Civil Emergencies
1-2468090	Weather
1-2468200	Time
1-2468400	Music
1-2468600	Music
61-2468011	US dial tone
203-8069	Coventry Radio
246-8015	Cricket Line
634-8069	Kent Radio
702-8900	Essex Radio

(continued from page 3)

are most of our readers pass by something every day that a good many of our other readers would find interesting—like a central office with a statue of Stalin in front of it. There are all kinds of possibilities.

But pictures aren't all that we find interesting. If you go away someplace, look at the phone books. Sometimes there are hilarious pages contained in them. You may get some bizarre notice in the mail that you can share with the rest of the phone/computer crowd.

2600 is not like other magazines. Our subscribers serve as our eyes and ears. You tell us when something new is going on and we investigate. You send us material that we print. We're all in this together—phones and computers have touched every one of us, whether we wanted them to or not. 2600 is here to give you the individual's view of high technology so you can grab the future before it grabs you.

So send us what you've got—articles, pictures, drawings, letters, clippings, etc. The address to send things to is 2600, PO Box 99, Middle Island, NY 11953. By pitching in a little bit, you'll be helping to make us that much more well-rounded and informative.

LETTERS

(continued from page 13)

just hope nobody gets in trouble believing that this technique is safe.

Worried and Upset in Arizona

There seems to have been some misunderstanding on this topic, judging from the way 2600 has been blasted by some readers in the last couple of weeks. A reader wrote in last month to tell us that his Radio Shack pen register didn't record numbers he dialed when he used a cordless phone. We found this to be true with this model of pen register and with certain cordless phones. We don't know if that is true of other "real" pen registers and that is what we said. If someone wants to give us access to a genuine law enforcement-type pen register, we'll be happy to tell our readers everything it does and doesn't do. Until then, we have to be honest: we're not entirely sure. We'd appreciate hearing from people who have actual hands-on experience in this field.

WRITE A LETTER!

And send it to us!

If you have questions or comments about our magazine or about computer hacking and phone phreaking, write them down and send them to

2600
Letters Dept.
PO Box 99
Middle Island, NY
11953

operating

(continued from page 6)

are made by the NYT TOPS operators to some older mechanical central offices, the operator will sometimes come onto the line with a reorder (fast busy) or recording. Sometimes when the operator leaves the line the recording stays there and the interrupted party cannot hang up. One reader wrote us and said that after an interrupt there was a recording saying "the area code for the number you dialed has been changed to 718" on his line for 2½ hours! During the course of this ordeal, two or three other people got tied in on crosstalk and also could not hang up.

- There aren't enough facilities to handle the bulk of calls the NYT operators seem to be receiving. Many times after dialing a 0+ call and hitting a 0 at the tone, you will get a reorder. Sometimes you get a recording telling you to wait because all operators are busy and then you get a reorder. Every once in a while you get a reorder when a New York Telephone operator tries to pass you to an AT&T operator.
- Finally, these new operators seem to have less experience dealing with people than AT&T operators. They can be quite rude and often don't know what they can and can't dial. It's not hard to get them to waste everyone's time by trying over and over to dial an 800 number.

The introduction of these NYT operators has proven to be fun, educational, and annoying as hell. If you have any observations, comments, or questions on this latest change in the system, contact me at *2600* and I'll do my best to investigate.

2600 marketplace

FOR SALE: Ex-Bell blue boxes, old and stylish, may even work! Also a wide range of old Bell comms equipment. Call (514) 228-6731 and ask for Rick for details.

DO YOU HAVE old outdated computer equipment lying around gathering dust? Why not donate it to 2600's growing bulletin board network? Support freedom of speech in your time! Contact 2600 at (516) 751-2600 or write 2600, PO Box 752, Middle Island, NY 11953.

FOR SALE: SWTPC Model CT-82 intelligent video terminal. Completely programmable (150 separate functions), RS-232C & parallel printer ports, full ASCII keyboard w/cursor control pad, 9" P-31 CRT w/7x12 dot matrix—up to 92 column capability, 32 baud rates to 38,400—much more. Excellent condition with full documentation. Originally $800, sell for $125 or best offer. Bernie Spindel, 144 W. Eagle Rd., Suite 108, Haverton, PA 19083.

FOR SALE: COMMODORE 8-BIT ROBOTICS KIT by Fischertechnik. All hardware, interface, software and manuals included. Mint condition. $399. Send phone # to: Box 571, Forest Hills, NY 11375.

BEST HACKER AND PHREAKER written public domain software for the Apple II family. Two double sided diskettes full of communication and deprotection utilities. These programs were combed from the best BBS and clubs nationwide. Send $10 cash, check, or MO to Mark B., 1486 Murphy Rd., Wilmington, OH 45177-9338.

WANTED: Technical data for pay phones, dot matrix printers, and/or modems. Looking for schematics and theory of operation. Call (205) 293-6333/6395, 7 to 4 CST. Ask for Airman Parochells. Cannot accept collect calls.

TAP BACK ISSUES—complete set (vol. 1-84) of high quality copies shipped via UPS or first class mail for $100.00. Over 400 pages of TAP material including schematics and special reports. Checks/M.O. to "P.E.I." Cash, M.O. shipped same day. SASE for sample. Pete G., P.O. Box 463, Mt. Laurel, NJ 08054.

GOT SOMETHING TO SELL? Looking for something to buy? Or trade? This is the place! The *2600* Marketplace is free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses! Address: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

32K MODEL 100, U1-Rom II, drive, TS-DOS, spreadsheet, modem cables, AC adaptors, briefcase included, good condition, $1200. New, make an offer. Tandy 2000 version of WordPerfect 4.0 $150 or trade for 1200 or 2400 baud external modem. IBM PC & XT & AT version of WordPerfect 4.1 and MathPlan 2.1. $250 or trade for 1200 or 2400 baud external modem. Call (803) 244-6429 or (803) 233-5753. Ask for Paul.

WANTED: Looking for a good used 5 or 10 megabyte hard drive for the Apple II series of computers. If you are selling one or know of anyone that is then send replies to: Brian F., 1003 W. Main, Apt. 3, Ottawa, IL 61350.

TAIWAN! All Taiwan computers and accessories available for direct shipment for cost plus shipping plus 3% (quantities of 50 or more). Giles, PO Box 12566, El Paso, TX 79913.

***2600* MEETINGS.** Fridays from 5-8 pm at the Citicorp Center in the Market—153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Questions? Call 516-751-2600.

Deadline for October issue: 10/5/87.

New England Telephone

J.B. Field
Manager

35 St. Peter Street
Salem, MA 01970
Phone: (617) 741-1030

Dear

Telephone service is furnished on condition that the identity of the person for whom service is provided is as represented at the time of the request.

On , telephone service was connected for you at
When the request for service was placed, you identified yourself as
and asked that the bills be rendered in that name.

We have since received information that leads us to believe this identity was not correct and that you misrepresented your identity in violation of Rule 5.1 of the Massachusetts D.P.U. Order of December 19, 1977. We have reason to believe that your true identity is
for whom we have a final bill for service rendered on
which has been outstanding since in the amount of .
Accordingly, we are notifying you that telephone service on will be disconnected on , IF YOU DO NOT COME TO OUR OFFICE IN SALEM WITH VALID I.D. AND A SIGNED LEASE. FOR

To avoid disconnection of your service, the final bill must be paid in full, a deposit of $120— must be paid to secure your present account, and the billing name on your present account must be changed to your name.

If service is disconnected, it will be restored if the requirements described above are met. A restoral charge of 20— will also be applied to your account.

_____ _____
Manager

THIS NASTY LETTER WAS SENT TO ONE OF OUR SUBSCRIBERS WHO SOMEHOW GOT THE PHONE COMPANY TO THINK HE WASN'T BEING HONEST ABOUT WHO HE WAS. IT WAS ALL AN UNFORTUNATE MISTAKE, BUT WE GOT ANOTHER NEAT FORM LETTER OUT OF IT.

THE IMPORTANCE OF YOUR TELEPHONE

A personal message about your home telephone from the former F.B.I. Director Clarence M. Kelley

Your family's single most important link to the outside world is your home telephone. Your family's ability to communicate quickly and effectively has a direct impact on their safety and security.

My experience as Director of the Federal Bureau of Investigation has given me a keen awareness of the many security problems facing the homeowner of the 80's, and I am proud to be associated with one company that has actually listened to the needs of the public in designing a complete line of quality telephones for home and office use. UNISONIC has made these telephones to work not only for your convenience, but for your critical security needs as well.

The main thing to remember is that your telephone is an extremely important part of your household—it can act as your guardian. When you purchase a quality telephone from UNISONIC, you have chosen wisely.

Former Director, F.B.I.

Clarence M. Kelley

THIS IS BY FAR THE SILLIEST THING WE'VE EVER SEEN ON THE OUTSIDE OF A NEW TELEPHONE PACKAGE. IS OLIVER NORTH NEXT?

Review: CO Magazine Enlightening

CO Magazine
Published monthly by Telecom Library Inc.
12 West 21st Street
New York, NY 10010
212-691-8215
Subject matter: switching, transmission, and network service.
Cost: *CO Magazine* is sent free to "qualified" subscribers in the U.S. and Canada. If you're not in the industry, U.S. subscriptions are $36 per year.

Review by Dan Murphy

Running approximately 60 pages each month, *CO Magazine* is one of the better telecommunications magazines available. It's geared for the telecom industry personnel and is broken into theme sections, each containing an article or two.

One section common to each issue is "News" featuring topics such as what companies are using what new equipment and recently passed laws affecting the telecommunications world. The news often has an analysis which is an editor's note on how something will affect things, written from the perspective of an individual or a small business. "New Services" tells of the latest services and features offered by local and long distance companies with an occasional piece on how new technology will affect the telecom market.

"New Products" previews and reviews the latest in telecom gadgets, gizmos, and equipment. This is one of my favorite features—it deals with everything from ISDN dataline monitors to mini-responders for testing lines and trunks to US West's MPOW multi-purpose operator workstation.

The "Services" section which appears almost every month has a diverse collection of articles getting down to the nitty-gritty of how the telephone companies do what they do best. For instance, in the May 1987 issue an article entitled "Advancing Advanced 800" explains in detail how AT&T's Advanced 800 services function. The April 1987 issue describes New York Telephone's Network Service Center operations quite interestingly in "New York Telephone's War Room".

Some of the themes that *CO Magazine* has presented are enhanced 911 service, ISDN, and fiber optics. In each instance there were several articles describing available services and techniques in use in the field.

CO Magazine provides an up to the minute look at the telecom world. I think it's one of the best magazines around and, you have to admit, it's hard to beat the price.

2600 HAS MEETINGS

Every Friday afternoon between the hours of 5 and 8

in the Market area of the Citicorp Center
in New York City,
53rd Street and 3rd Avenue

NOTICE

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind. Simply indicate the amount enclosed and which, if any, back issues you want. Your address label should be on the back of this form.

$15 ..... 1 year of 2600
$28 ..... 2 years of 2600
$41 ..... 3 years of 2600
$40 ..... 1 year corporate subscription
$75 ..... 2 year corporate subscription
$110 ..... 3 year corporate subscription
$25 ..... overseas subscription (1 year only)
$55 ..... overseas corporate subscription (1 year only)
$260 ....lifetime subscription (never again will we bother you)

Back issues are available. Prices are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 .....Any two years
$75 .....All three years (36 issues)
(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

AMOUNT ENCLOSED FOR SUBSCRIPTION:_____

AMOUNT ENCLOSED FOR BACK ISSUES: _____

1984 1985 1986 (circle years ordered)

TOTAL AMOUNT ENCLOSED: _____

(clip and send to us—your address is on the back)

CONTENTS

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.