

==Phrack Inc.==

Volume One, Issue Eight, Phile #1 of 9

Index

Welcome to the long-awaited Phrack Inc. Issue 8. I'm quite sorry for all of the delays, but it's time to go back to school and it's been a hectic summer. Unfortunately, over the summer, Fatal Error of 617 died in a motorcycle accident. He was the sysop of Metropolis Elite and was around a while back. This issue is released in memory of him, regardless of any personal opinions.

Taran King
Sysop of Metal Shop Private

Contents:

- #1 Phrack Inc. Index by Taran King (1k)
- #2 Phrack Pro-Phile V on Tuc by Taran King (6k)
- #3 City-Wide Centrex by The Executioner (14k)
- #4 The Integrated Services Digital Network by Dr. Doom (18k)
- #5 The Art of Junction Box Modeming by Mad Hacker 616 (6k)
- #6 Compuserve Info by Morgoth and Lotus (8k)
- #7 Fun with Automatic Tellers by The Mentor (7k)
- #8 Phrack World News VII Part I by Knight Lightning (25k)
- #9 Phrack World News VII Part II by Knight Lightning (26k)

==Phrack Inc.==

Volume One, Issue Eight, Phile #2 of 9

==Phrack Pro-Phile V==

Written and Created by Taran King

June 25, 1986

Welcome to Phrack Pro-Phile V. Phrack Pro-Phile is created to bring information to you, the users, about old or highly important/controversial people. This month, I bring to you one of the most influential users of our times and of days of old...

TUC
~~~

Tuc is the sysop of RACS III (TUCBBS), a telecom enthusiasts' bulletin board in Stony Point, N.Y. (914).

### Personal

~~~~~

Handle: Tuc

Call him: Scott Jeffrey Ellentuch

Past handles: None

Handle origin: Nickname in high school derived from teachers calling him EllenTOUCH, EllenTOOK, and his corrections were phrased "TUCK!"

Date of Birth: 10/10/65

Age at current date: 20-1/2 years old

Height: 6'3-1/2"

Weight: About 195 lbs.

Eye color: Brown

Hair Color: Black

Computers: TRS Model I, then, 2 Atari 800's, then, countless Apple II+'s, then, finally, 1 IBM PC.

Sysop/Co-Sysop of: RACS III (TUCBBS), Phreak Advisor: Sherwood Forest II

Tuc started out in the BBS world in July 1980 when he first got his modem, a Novation Acoustic. In August of 1981, Connection-80 of Stony Point, his first bulletin board, was launched into the BBS world. It started on a TRS-80 Model I, Epson MX-80 printer, 2 single density disk drives, a Novation Acoustic modem, and a home built auto-answer module. At the time, he didn't even know what phreaking was, so it was a general public board. A software switch to RACS III occurred on January 10, 1982, running until January 10, 1985. The hard drive arrived a few months ago to build it to the board that it currently is.

Members of the elite world which he has met include King Blotto, Lex Luthor, Dr. Who, Crimson Death, The Videosmith, Jester Sluggo, The Sprinter, Mark Tabas, BIOC Agent 003, Agrajag, Telenet Bob, Big Brother, Cheshire Catalyst, Egyptian Lover, Magnetic Surfer, Paul Muad'Dib, Lord Digital, Sir Knight, 2600 Editor (Emanuelle Goldstein [sp.]), Susan Thunder, Modem Rider, Sharp Razor, Hertz Tone, The Flying Avocado, and The Ace.

His phreak experience began in March of 1982 through the new board's software having a section called "Phreak-80". People started calling and paying attention to it, including one caller by the name of Susan Thunder, which is how he personally began to phreak. She lead him around the scene which included the infamous 8 BBS and to other people such as Larry Kelly. Some of the memorable phreak boards he was on included 8 BBS, MOM, OSUNY, The Private 414 Board (as in THE 414's), Blottoland, The Connection, L.O.D., Plovernet, Pirate 80, Sherwood Forest I, II, and III, WOPR, IROC, Pirate Trek, Pirate's I/O, Datanet, Stalag 13, A.I. Labs, and Hell Phrozen Over. He gives credit for his phreak knowledge to Susan Thunder and the people that she put him in touch with.

Tuc's work is as a computer and communications security freelance consultant. He's done lots of programming in basic for the TRS-80, and assembly language for the IBM 370.

Tuc does hack and phreak, but with his employer's consent. Tuc attends the TAP meetings in New York occasionally, but in the past he was a regular. He's attended all Phreak-Con's, he was an assistant editor of the original TAP, and was a pioneer in the phreak world before blue boxing and Alliance Teleconferencing was common knowledge. Besides that, he was the one on West 57th Street labeled "Scott Jeffrey Ellentuch". He was hard to find on that particular program.

Tuc has been involved with various groups in his lifetime including (in the order that he joined them) The Warelords, The Knights of Shadow, Apple Mafia, and, at the same time as Apple Mafia, Fargo 4A.

Interests: Telecommunications (modeming, phreaking, hacking), martial arts (weaponry), radio controlled cars and airplanes, and video games.

Tuc's Favorite Things

Women: A quiet evening with the girlfriend.

Cars: MG-TD Kit Car.

Foods: Anything vegetarian.

Music: The Hooters, and any band he worked for.

Most Memorable Experiences

Some People to Mention

The CWC (City-Wide Centrex) feature provides multiple location large business customers with centrex features, attendant features, and dialing capabilities that are transparent across geographic locations and are independent of the configuration of the #1AESS switches providing the service. Historically, centrex customers have been somewhat limited to the bounds of the servicing switch. Customers could be built across switches, but with limitations. Multiple locations could be arranged to share some features in common only when placed in a centrex complex served by a single switch. Obviously, for this to be feasible, the locations had to be geographically near

each other. The CWC feature expands the concept of the centrex group by allowing a multi-located business to function as a single centrex arrangement called a CWC group. Although each customer location remains a part of its own switch with its own individual capabilities, it now functions as part of the CWC group. Selected centrex features that were defined to operate within the bounds of a serving switch centrex group are now redefined to operate within the bounds of the CWC group. The outer boundary of the CWC cannot exceed the boundary of the LATA due to LCCIS constraints.

The CWC feature provides a comprehensive communications package for a multiple location centrex customer. Some advantages are:

- o Extension to Extension (Intercom) dialing.
- o Concentration of private facilities access at one location.
- o Elimination of dedicated facilities between locations within the CWC group.
- o Transparency of feature operation across switches.

Use of CCIS trunks to replace tie trunks results in the need for fewer total trunks and trunk groups. Remote access reduces the total number of customer trunks required and centralizes customer facilities at one location. All switches need LCCIS so that information can be passed between locations.

=====
=Intercom Dialing=
=====

Intercom dialing gives the customer the ability to dial extension numbers (intercom) to other locations. This is done either by dialing the interlocation intercom number or by a speed call code which contains an interlocation intercom number. The customer has the option of routing these interlocation intercom calls via simulated private or public facilities. After determining the intercom number dialed is in location, the originating office routes the call to that location. The call is identified in the centrex customer's digit interpreter tables as an interlocation intercom call and normal interoffice call processing determines routing. A decision is made as to whether simulated facilities are used for routing the call based on the location identification of the called line. If needed, a simulated facility is seized. This is determined by a distant line status request on the called line at the end of dialing. The originating offices sends information to the terminating office identifying the call as interlocation intercom call. The CWC group and location identifier of the calling party are also sent. This is done by using the RCLDN (retrieval of calling line directory number) to transmit this information. The terminating office recognizes as incoming call as such. If the two-way simulated private facilities are used, the count on facilities at the terminating office is incremented. The use of 2 way simulated private facilities for a call is based on the location identifier of the calling line and whether simulated private facilities were used on the outgoing side.

=====
=Centrex Attendant Console=
=====

The tie trunks are replaced by CCIS trunks, therefore some changes are required in the use of the attendant console. The changes are as follows:

- o Busy Verification and attendant call through tests are not applicable since there will no longer be specific trunks dedicated to the customer.
- o The existing trunk group busy lamps are replaced with busy lamps for the

simulated facilities between locations.

The digit interpreter table entry at each remote location contains the "Dial 0" DN for the attendant. This is done to process interlocation intercom calls which terminate to the attendant. If the attendant console uses a centrex data link, the line equipment assigned to the DN should specify the call indicator lamp to be used. A different DN should be used for each location if separate call indicator lamps are desired for calls from each location. This call indicator lamp flashes at the intragroup rate of 120ipm (interruptions per minute) to indicate interlocation intercom calls.

The RCLDN primitive is used to transmit information for intercom dialing between locations. In addition, the RDLIS primitive is used to provide CWC information to obtain the CWC group and location identifier of the called line. The originating, incoming, and CCIS incoming registers are used to save information at both the originating and terminating offices. These registers include the CWC group, CWC location identifier, a CWC call type, and an indicator whether simulated facilities were used at the originating.

```
=====
=Remote Access to Private=
=      Facilities      =
=====
```

Remote access to private facilities allows the CWC customer to access physical private trunks and simulated facilities at a single location. This allows customers to consolidate their private facilities at one location. The number of trunks required is reduced. Any station can access these facilities by dialing the same access code as the main location. If a station dials the access code for a private facility, the call is routed to the main location using the same facility as an interlocation intercom call. It is then routed out from the main location. The CWC feature does not allow the customer to use the ACOF (Attendant Control of facilities) feature from a remote location. The types of private facilities which are accessible are:

- o Tie Trunks
- o FX (Foreign Exchange)
- o CCSA (Common Control switching arrangement)
- o ETS (Electronic Tandem Switching)
- o WATS (Wide Area Telecommunications system)
- o FRS (Flexible Route selection)
- o EEDP (expanded electronic tandem switching dialing plan)

The CCIS direct signalling messages are used to communicate between the remote and main locations during the digit collection and analysis of out-going calls. Once the voice path has been established, a CCIS banded signalling message transmits the digits collected. A remote access register is used to store information retrieved during the processing of the signal requests. This register belongs to the OR (Originating Register) pool at the main location.

The remote location is responsible for digit collection and transmission of collected digits. A remote access data CCIS direct signalling message transmits the digits from the remote to the main location, which returns instructions for the next action to be performed. The following items are sent from the remote to the main location:

- o The digits collected.
- o The FRL(facility restriction level) of orig. line.
- o A FRL present indicator
- o A customer changeable speed call indicator.
- o A call forwarding over private facilities indic.
- o An add-on indicator.
- o The CC location identifier of remote location.
- o The remote access register # of the main location.
- o An abandon remote access request indicator.

The main location analyzes the information transmitted and returns the next set of instructions to the remote location. The full analysis of a call may require several direct signalling messages with information saved from the previous direct signalling messages. This is required to process the current direct signalling message being saved in the remote register. The information gathered is used to establish the voice path for the call. Upon receipt of a direct signalling request, processing is done in accordance with the function indicated in the remote register. The types are as follows:

- o Translate access code
- o Translate prefix digit
- o "1+" dialing check
- o Check for possible account code
- o Complete account code received
- o 3 digit translation
- o 6 digit translation
- o 10 digit translation
- o Analyze authorization code
- o FRS 3 Digit translation
- o CCSA translation
- o Abandon call

After processing at the main location is complete, the remote access register is set up to identify the next type of function. Then, the main location returns a CCIS remote message to the remote location. The information returned from the main location is always in the same format and is saved on the OR.

=====
=Features=
=====

The CWC group is allowed many features, here is a list of them.

1. Call Forwarding Variable: Users can forward their calls to remote stations located in another office by dialing the access code and the intercom number of the CWC station.
2. Call Forwarding Busy Line: Provides for the forwarding of calls to any interlocation station within the CWC group upon encountering a busy station.
3. Call Forwarding Don't Answer: Provides for the forwarding of calls that are not answered within a predetermined number of ringing cycles.
4. Call Transfer: Allows the station user to transfer any established call to any other station within the CWC group with the following constraints.
 - o Dropback rules do not permit 2 outgoing trunks to be involved in the final 2 party connection. However, 2 outgoing trunks can be involved in a 3 way conversation.
 - o On interoffice calls involving a fully restricted station, flash capability is allowed. However, the controller is not permitted to connect the fully-restricted station to any other station, either in dropback or a 3 way conversation.

Cross network call transfer transparency requires that each location be provided the Call Transfer-Individual or Call Transfer-Individual-All calls feature. The CTO (call transfer outside) option may be provided.

5. Call Waiting feature provides a burst of tone when the called party is busy

on another call. The types of Call Waiting features and CWC interactions are:

- o Call Waiting Originating: allows a CWC calling station to direct a call waiting tone toward a busy station within the same CWC group.
- o Call Waiting Intragroup: gives call waiting tone to a called party which has call waiting terminating on all intragroup calls.
- o Dial Call Waiting: Allows originating CWC station users to invoke call waiting on CWC intragroup calls by dialing an access code followed by the extension number of the station to be call waited.

6. Distinctive Ringing/CW Tone: Allows a CWC station user to determine the source of a call incoming to the station. This is done by associating a distinctive ringing or tone pattern with the incoming call based on its source. Interlocation CWC calls receive intragroup treatment.

7. Message Desk Service: Provides centralized and personalized call coverage or message answering capabilities which can serve the needs of all CWC locations. The Call Forwarding Variable and Call Forwarding Busy Line/Don't Answer feature are needed of forwarding calls from stations within the CWC group.

8. LASS (Local Area Signalling Service): Provides the called party with call management and security services. Local CCIS is required for multiple-office grouping within a LATA for intercom calls. The following features comprise the LASS offering :

- o Automatic Recall: Enables a station user to place a call to the LCDN (Last Call Directory Number) currently associated with the users fone. The LCDN can either be the last party called by the station user or the last party to call the station user.
- o Distinctive Alerting: Allows the station user to prespecify a set of numbers which activate a distinctive ring or distinctive call waiting tone. The CWC extension numbers can be entered on the screen list. When the user receives a call from one of these numbers, the phone if idle, will ring with a special distinctive ringing pattern. If a call waiting customer's line is busy, a special tone notifies the customer of the impending call.
- o ICLID: provides the number which is calling the station user. (Explained in other files)
- o Selective Call Forwarding: (Explained in other file)
- o Selective Call Rejection: Provides the user with the capability of not being alerted by calls from a specified set of numbers. The user inputs the numbers to be rejected from the station set. These numbers are specified either directly (dialed in) or as the number of the last call received. The CWC extensions are allowed on the screen list.

=====
=(C) 1986 The Executioner and The Egyptian Lover and PLP =
=====

This file is based on the AT&T document for the CWC.

==Phrack Inc.==

Volume One, Issue Eight, Phile #4 of 9

The Integrated Services Digital Network

---==> By Dr. Doom <==---

ISDN or Integrated Services Digital Network has been talked about off and on by AT&T and until now has just been a demented AT&T fantasy, but it is to soon become a reality. This phile is the second I have written on the subject and is a cumulation of information from three basic sources :

- <1> The ISDN AT&T Technical Journal
- <2> An interview with an AT&T Long Distance Operations Center Supervisor who will be referred to as Mr. R.
- <3> and some general ISDN articles from Southwestern Bell Newsletters.

ISDN Definition =====

CCITT Definition : An end to end digital network that supports a wide range of services accessed by a set of standard multipurpose user-network interfaces.

ISDN will allow for incredible new services that will drastically change the telecommunications industry and everyone's lives. For example, one new service ISDN will bring about is calling party identification. This will allow businesses and individuals who subscribe to that service to know exactly what number you are calling from before they even decide whether or not to answer the phone.

In the case of dialups like MCI, the originating # will be stored in a computer along with whatever code and number that person dialed which would greatly hinder abuse of codes from a home phone.

This is just the tip of the iceberg as far as ISDN is concerned. This phile will analyze and describe how The Integrated Services Digital Network will operate when it is implemented.

Out of Band Signalling =====

Essential to a network capable of providing such enhanced services as calling party identification is out-of-band signalling. Until the late 70's, when AT&T introduced the 4ESS toll switch and CCIS into the national network, switches had communicated with each other over the same channels in which our voice or data was transmitted (in-band). During this time, all signalling between switches had to be limited to a type that could be accommodated in the 'voice' channel thus making it impossible to offer any advanced services.

The development of the separate Common Channel Interoffice Signaling (CCIS) network allowed for more freedom and flexibility and thus came about the AT&T Calling Card service.

ISDN brings an interface from the network to the subscriber's equipment. This is a completely digital interface subdivided into two types of channels :

The 'D' Channels are those used for sending signalling and control information across the interface. The 'B' Channels are those used only for customer information which can be in the form of voice, data, or video.

The 'D' Channel hence manages the information or 'B' Channels making the signalling 'out-of-band' and not 'in-band' as it is now. This approach allows for two distinct benefits :

- <1> All the capacity in the information bearing channels is available for customer use.
- <2> The 'D' Signaling channel allows for distributed processing across the ISDN

Network.

ISDN Interfaces

The CCITT has defined two major interfaces that will be used in conjunction with the 'D' and 'B' channels :

The Basic Rate Interface (BRI) consists of one D Channel and two B Channels. This interface is used for locations where information transport is relatively small like a residence.

The Primary Rate Interface (PRI) consists of one 'D' Channel and 23 'B' Channels. It is used for large capacity vehicles such as PBX's.

Notice that there are 2 DIFFERENT 'B' Channels in the Basic Rate Interface. This allows TWO different types of data to be sent over the same connection at the same time. For example, you could be Uring files to a board on Channel 1 while talking to the SYSOP on Channel 2.

So, if both you and a board both have a BRI ISDN Interface, next time the SYSOP says 'Go Voice', you simply pick up the handset, switch it to channel 2, and start talking...

These multiple channels are also the foundation for the widespread use of Video Phones. Just like you were sending data over channel 1, and talking voice on channel 2, you can be sending video over channel 1 (allowing the party's to see each other) and talking on channel 2.

ISDN Devices

=====

AT&T Technologies, Advanced Micro Devices, and Intel are all in the process of designing equipment that will be compatible with ISDN. So far, the two main designs talked about through SWB and AT&T are :

<1> The Voice/Data Terminal This will look like any regular computer terminal with the exception that it has a handset on the side of the terminal and a couple of switches that will allow you to decide which channel is for DATA and which channel is for VOICE. This will also (of course), allow two customers with a V/D Terminal to be exchanging DATA over one channel while talking voice over the other one.

<2> The Video Phone

This is where (yes) Big Brother is arriving... The Video Phone will work pretty much just like it does in Science Fiction movies like 'Aliens' or whatever. If two ISDN customers have video phones, they can talk and see each other or whatever they want to show each other (HAHA) at the same time. Video Phones obviously open up new frontiers for those with entrepreneurial instincts. You can bet there will be some interesting Video Phone Sex lines around... Then, you can have things like 'Dial a Movie...Please enter (1) to view Rambo'..etc... The list goes on. This also leads to a whole new world of problems for the telephone company like 'Obscene Video Calls'. This is again where Calling ID becomes important.

Each of these units, and others that will work with ISDN will have some sort of a special viewing screen that will contain the necessary information about incoming calls which includes the originating number and can include such things as :

<1> The name of the owner of that #
<2> The city and state
<3> The whole address for that #

AT&T ISDN Building Blocks

=====

AT&T has designated certain 'building blocks' that will eventually be laid in place across the entire country to form ISDN.

<1> AT&T Communications Service Node

The service node is the customer's gateway to the AT&T Communications nodal family of services, including MEGACOM, MEGACOM 800, and Acunet. The first service node went into service in 1985 in Philadelphia, PA.

<2> Integrated Access

This allows customers to integrate switched and private line services over a single DS-1 link to the Service Node.

<3> Out-of-Band Signaling

Discussed earlier.

<4> CCS7

The CCS7 Common Channel Signaling Network will soon replace CCIS as an out-of-band signalling between AT&T Network Communications Facilities. Because of its longer message format and layered structure, the CCS7 will support the new features.

<5> Digital Backbone Network

This nationwide AT&T Network includes extensive lightwave and digital radio routes. By the end of 1988, these Digital Lightwave routes will extend to Europe with the TAT-8 lightwave system, and across the Pacific with HAW-4/TPC-3.

<6> Intelligent Software Controlled AT&T Communications Network

This brings about more advanced software related services listed in #1.

AT&T ISDN Operations

=====

Access Transport

Your DS-1 signal is transported from your ISDN equipment to an AT&T Communications Service Node somewhere.

Your line gets to AT&T by tariff from the local exchange carrier (i.e... Southwestern Bell, GTE, or whomever happens to own your local switch...) or AT&T. The direct link to the AT&T Service Node bypasses your local switching.

AT&T Service Node

Your local AT&T Service Node is a service office that acts as a gateway to all the new AT&T Nodal ISDN services. This service node is typically composed of :

<1> A Refinished 4ESS Switch

<2> CNI Ring (Common Net.-Interface)
 <3> Digital Access and Cross Connect System (DACS)

Here is a diagram of how a customer location either goes to a local switch or AT&T's node :

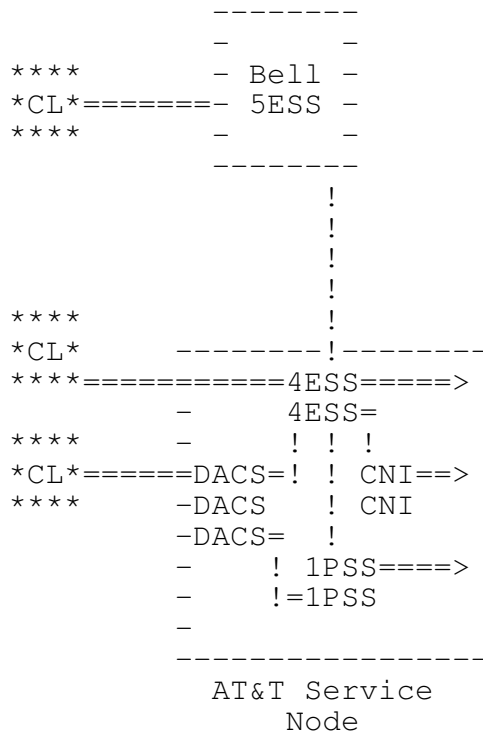
Key

CL = Customer Location

= = DS-1 Line

! = DS-1 Line

> = Exiting out to AT&T Network



The above diagram shows first how an AT&T Customer with ISDN can either continue service with his local telephone co. or go with a direct link to the AT&T Service Mode. All lines going to an AT&T Service Node whether through Bell or a direct link terminate on either the 4ESS or the DACS.

When a line terminates on a DACS it serves as an Integrated Access Distributor and sends the call to the 1PSS (Packet Switch) for Acunet Packet Service or to the 4ESS and then eventually out to the AT&T Network.

The AT&T Internodal Network

In the internodal network facility, AT&T is in the process of deploying both digital lightwave and digital radio systems.

Lightguide Systems :

In areas where growth is low, the FT3C and FTX180 Single mode terrestrial lightguide systems will be used between nodes.

On high growth routes AT&T will install fiber pairs at line rates of 1.7Gb/s with 20 mile repeater spacings.

Digital Radio :

In the digital radio area, 4Gb/s systems such as the TD-90 and the TD-180

provide a vehicle for rapid expansion of digital connectivity.

ISDN and Digital Switches =====

AT&T has redesigned the 5E Switching Modules in such a way that they are fully compatible with ISDN, but many of the existing 5E's and other switches were manufactured without ISDN capability. To meet this need, AT&T has produced ISDN interfaces that modularly connect to the system. Here is a diagram of a 5ESS Switching Module with interfaces :

Key

\$ = ISDN V/D Terminal or Video Phone

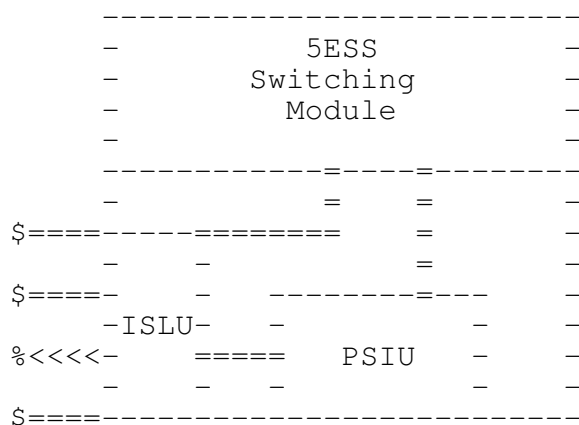
% = Standard Telephone

= = Digital Line

< = In-Band Line

ISLU = Integrated Services Line Unit

PSIU = Packet Switch Interface Unit



The two new hardware additions are :

<1> Integrated Services Line Unit and

<2> The Packet Switch Interface Unit

These units allow a LOCAL 5ESS (or other digital) Switch to serve both ISDN and non-ISDN customers. These interfaces are integrated into a switching module in a way that will allow ISDN customers to maintain all their previous Bell services like Local Calling. Notice also that all lines, whether ISDN or not, terminate on the ISLU.

Calling Party Identification =====

Discussed briefly in the preface of this phile, the ISDN enhanced Calling Party Identification service offered by AT&T ISDN will be into service along with the ISDN.

This quote out of the AT&T ISDN Technical reference should give you a good idea of the impact ISDN will have on hacking and phreaking :

'One example of an enhanced service which has already been included in the ISDN signaling protocol and will have a fundamental impact on day to day telecommunications is the provisions of calling party identification. Calling party ID will help us decide whether or not to answer incoming calls

and will minimize instances of nuisance calls and COMPUTER FRAUD via telephone.'

Mr. R, our AT&T Supervisor has been attending ISDN Conferences that include representatives from all the major LD Companies (AT&T, MCI, GTE, LDS, etc.), the Regional Bells, and other concerned parties. He said quote 'One of the controlling factors behind The Integrated Services Digital Network is the simple fact that AT&T, MCI, and other long distance companies are losing MILLIONS to Phone Phraud.' Once ISDN is realized, so will network wide Calling Party Identification.

Again, our friend Mr. R will enlighten us on the subject of ISDN Calling Party ID and a simple explanation of how it will work :

'Right now, when you pick up the phone in your home, Port Isabel South Western Bell knows that you did. Then, when you dial a number, they know what number you dialed. So they send that information along to us (the AT&T Toll Switch). We then send that along through the network to the person you are calling.'

Of course, there is one transaction between AT&T and a Bell Office at the end that he left off, but if the person or computer you are calling has ISDN Calling Party ID service, your originating # will be sent along the DS-1 Line Interface from Bell to his equipment and show up on his screen after traveling through the network like Mr. R described.

This is rather simple when you think about it and is one example of how a once shattered network is working together.

Some Sample CP ID Uses

This can be used by large telephone ordering companies to instantly display a record of that persons credit, previous orders, etc... before the call is even answered on the attendant's terminal.

When someone logs onto a computer, the originating # is listed on the user log along with the account name, etc... so that if there is an unauthorized login, they can contact the authorities to do whatever or monitor that number until they get enough evidence to prosecute. The same thing holds true with LD Dialups. They will record the originating number along with the code and bill making MCI use rather dangerous.

SWB ISDN News

=====

The following article was extracted from The Southwestern Bell Texas Publication of Telephone Times and is entitled 'User Forum simplifies ISDN' :

" Houston---Houston Marketing employees played show and tell with two customers and all three groups are better off for it.

Marketing Representatives, with support from Bell Comm. Research, Illinois Bell, AT&T, and McDonald's Corp. met with Shell and Tenneco to discuss ISDN.

'ISDN is an evolving technology' said Bob Campbell, division manager marketing business sales. 'It's still in the developmental stage. These User Forums will give customers input on how it's deployed and what it will look like.'

ISDN is an all digital network that transmits voice and data messages simultaneously over a single telephone line.

'The User Forums allow customers to share information on specific problems concerning implementation, training, customer premise equipment and applications,' Campbell said.

Linda Hobson, manager marketing administrative and coordinator of the event, said not only will User Forums be standard practice in Houston, but probably

will become the national standard.

'We're doing it quarterly here, but as more people become interested, we may meet more often,' Hobson said.

Shell and Tenneco, who have signed letters of intent to purchase ISDN, were specifically interested in such topics as trial status (SWBT's ISDN trials will begin soon in St. Louis and Texas), available features, power requirements, and future enhancements.

'In the past, we bought the available enhancements, then sold them to the customer,' said Hobson. 'That's changing. We have to find out what the customer wants, then deliver the service that meets the specific needs' "

That concludes the nice little article which by the way, contained some interesting little tidbits of information.

Conclusion

=====

ISDN is a VERY complicated plan that will drastically change the telecommunications scene in this country and abroad. Although AT&T has boasted in it's Technical Journals of being able to have its ISDN Capable Network completed by Early 1987, this date seems to keep getting postponed back according to our friend Mr. R (The AT&T Supervisor) and he is shooting for large scale ISDN no earlier than late 1988 or 1989. Whenever ISDN does become reality, people will probably just put out files with lists of computers that subscribe to ISDN Calling Party Identification, and tell people not to call them from their home.

I hope you have enjoyed reading this phile on ISDN, I will be on the outlook for more information on it.

If you don't already have the # and New User Passwords to Metromedia BBS, send me (Dr. Doom) mail on any of the boards I am on.

==Phrack Inc.==

Volume One, Issue Eight, Phile #5 of 9

```
*****
***** The Art of Junction Box Modeming *****
***** Written Exclusively For: *****
***** PHRACK INC.! *****
*****
*                               by Mad Hacker of 616                               *
* Watch for Thieve's World ][ coming soon, now with 33 megs!                      *
*****
```

This file will detail the use of a rural junction box to fraud the phone company and make all the free phone calls you want to BBS or AE by.

There are two basic types of rural junction boxes: Residential and Group boxes. I will first discuss Residential as they are easier to find and easier to use. There are a couple of requirements before you can make full use of a Junction Box. First you must have some kind of portable computer with a built-in modem or at least a hand phone if all you want to do is make free calls to your friends. For computer I would recommend something like a Model 100 from Radio Shack. Small, inexpensive but only 300 baud and only 32K of total storage.

Anyway you can find residential junction boxes in most any rural area just a few feet off the road and usually covered over with local weeds. Fish your way thru the weeds and open it up. Some just open with a twist or a turn, others are actually locked and require a little more patience. Anyway

once you have it open, you should see at least 4 pairs (possibly more) of wires. You are only concerned with the pair containing both a red and a green wire.

Now you need to make a choice: Do you want to totally cut off the regular owners of the phone line and do actual damage to this junction box or leave them connected but have the possibility of them picking up their phone and hearing your carrier?

Usually you will want to cut them out totally, so simply find a bit of slack in the line and cut both wires. Now in most boxes the connection to the outside world comes from the bottom of the box, but sometimes you will find one that doesn't conform. Simply attach a hand phone to the wires (matching up colors, of course) and see if you get a dial tone. Anyway once you have the proper pair then hook up to your modem line and dial anyway. Meanwhile the lawful owners of the line will get a dead line on their end, so try to do this only when you think no one would be using the phone, like 11PM to 7AM or else they will probably call their LOC and tell them to fix the line and when they see the cut wires, they will wonder what went on there. Finally be a good guy and when you are done, resplice the wires together and shut the box.

Now usually you don't want to cause permanent damage to the box, so simply strip off the insulation on the line and attach the red and green ends of your modem cord to them. Now when you cut in, it will be much like an extension was picked up. Simply dial away and have fun. Of course if anyone at the house picks up the line they will get your carrier and will wonder, so try to limit your activities also to the same hours mentioned above, unless you know who you are ripping off and when they use the phone. The advantages of this method is that once you strip the wires, there is little work to do each time you use the box again.

Now what do you do if you are lucky enough to find a Group box? Well first you are confronted with a multitude of wires, anywhere from 10 pairs up to 100 if you use a box on the edge of a small town. Finding a pair of the right wires is a little more difficult unless your LOC has done repairs at this box in the last couple of months, in which case a lot of the wires will already be paired off. If you aren't so lucky find a couple of wires and try them out. Once again you have the choice of stripping or cutting the wires, but the advantage here is that you can use this box for about 4-6 months without having to find a new one.

What is the this junk about having to find a new box? Well you see when you use a junction box in this manner, you are basically adding an illegal extension to a private line. Any calls you make will show up on the rightful owners bill. If you are only using the box for one or two short to medium length calls a week, then you might not have any problems. However if you use a box too much and the people keep calling the billing office about the extra calls, the billing office will call those numbers and hear the carrier. This will tip them off to the fact that someone is either lying at the rightful owner's house or that someone has tapped into their phone line. At this present time in the Midwest, it take about 2-3 months for the LOC to realize that someone is playing with their junction box. What they do is come out and repair the wires and usually put a newer lockable box on the site to discourage illegal use. I haven't yet really pushed the LOC to any limits yet, but one might suspect that has Junction boxing catches on to those of us who have access to laptop computers, the LOC may find some way of catching us at our little game.

If anyone has any new information on how your LOC is handling this use of their junction boxes please let us know by leaving mail for Thomas Covenant on any Metal Shop board.

[Postscriptum note by Thomas Covenant: I'd recommend one of those so-called "portable" AT-compatibles. Great clock speed, 1200 baud, and a bigger screen. And why not pack a picnic lunch and some booze? You'll be there all day once you get started!]

^Z, or "EOF"

==Phrack Inc.==

Volume One, Issue Eight, Phile #6 of 9

COMPUSERVE INFO

Compiled and
Related by:
Morgoth and Lotus

Since its rather humble beginnings in Dublin, Ohio some years ago, CompuServe, or CIS, as it will be referred to in this article, has grown to become the largest entertainment/public user oriented system in the country. This file is divided into two parts. The first is how to get your own CIS ID number, and make it last a relatively long time. This part may seem like old hat to some of you out there. The second part is information on what to do once you are on the system...tricks and tips to keep you out of trouble, or cause trouble.

A CompuServe identification number is divided into two parts; a project number and a programmer number. An example would be 70007,1460. This ID is what you will be known by at all times on the system. When you log on, you will also be prompted for a password, in addition to your user ID. The password is divided into two words, kept apart by a separator (-, :, ., etc). The password may be any two words the user desires, including garbage, which makes gaining an ID by hacking the password almost, if not totally, impossible.

The most popular, and about the only way left, of gaining an ID is by buying what the system calls a snapak. These are the little goodies you see in the store in the introductory packets. With this, you can gain access to most, but not all of the system.

The first ID, or the "intro" ID will last about a week, at which time, CompuServe automatically changes the password, and sends the new one to you via the US Postal service. This is a key point to the ID scam. You MUST have valid Credit Card information to be able to continue using the ID. I have heard of intro IDs going bad in a matter of 2 or 3 days due to having non-valid credit card info. So you need to set up a location to which your second password can be mailed. This second password should last about a month, depending on how much credit the CC holder has on his card.

When applying credit to a Visa or Mastercard, CompuServe will submit the charges about once a week. If you run up about \$500 in connect charges, and the credit card cannot hold it, the ID will go bad. This is the most common way for an account to run out.

Your first password has some limits. Due to hackers using snapaks, CompuServe has installed a system which prohibits IDs without the second password from entering any type of game online. This ranges from the ever-popular MegaWars, to YGI, all the way down to Casino. This is one reason why the second password is so important.

If more than one person will be using the account, which is usually the case, there are also some limits to be observed. The same ID can no longer enter the CB simulator more than once. If it is tried, the message "exceeding job limit" will occur, and you will be taken back to the prior menu. The same ID can go into a SIG at the same time, but both people cannot enter CONference mode while on the SIG. The best way to talk to another user who is on the same ID is to go into any forum, say CBMART, and have one of them enter CONference mode. There, the two users can use the /SEN command to relay messages between the SIG and CONference. This is kind of complicated, but it is the only way. Also,

anytime the message "exceeding job limit" goes to your screen, the people at CIS put a small "red mark" by your name. If it occurs too frequently, they look into the situation to find out if more than one person may be using the same ID.

Special IDs -- Ok, now that you are on Compuserve, what should you look out for? As mentioned before, the user ID is divided into [project number, programmer number] format. The Programmer number is of no importance, but the Project number is. Some of the ones you should be aware of while online are:

```
70000,xxxx  Compuserve Security
70003,xxxx  Compuserve Employee
70004,xxxx  Same as above
70005,xxxx  Radio Shack demo account
70006,xxxx  Customer service, or "Wizard" number (see below)
70007,xxxx  Complimentary account
76703,xxxx  SIG SysOp, or Forum Info Provider
```

While on CB, look out for the 70000 IDs, and especially the 70006, or "wizard" numbers. The Wizard ids have some very special functions. The main one is called autogag, or /GAG. This allows the bearer of this ID to banish any user from the system, in a way. What it actually does is to keep the /GAGged person out of everyone's view. They will not show up on the /ust list, and anything they type will not show up on anybody else's screen. Kind of like a mute button on a television. The Chief of CIS security is Dan Pisker, and on CB he uses the handles "Dan'l", or "Ghost", with a 70000 id.

Monitoring -- This is a very popular subject with the users of Compuserve, but when broken down, it is quite simple. CIS is capable of monitoring ANYTHING that is said on the system. This doesn't mean that they do, however. For /TALK to be monitored in a Forum or on CB, CIS must first have a court order...it is supposedly as illegal as tapping a phone line. This has been done before to catch some major hackers on the system. /SEN in a SIG is not supposedly monitorable....the status on it is the same as on /TALK. /SCR mode on CB or on a SIG is definitely monitorable, especially if the the /SCR key is typed on open channel. Keep /SCR conversations to a minimum. As far as anything else goes, anything said on open channel is quite definitely seen by SOMEBODY in the big chair up in Ohio. It would not surprise me at all if they hire people to go through CB Transcripts every day to look for that kind of thing. Also, when you are in Conference mode in a SIG, always check the /Status of the channel. If /STA EVER returns that there are more people on the channel you are on than the /USERS function does, then you can rest assured that the channel is being monitored.

Nodes -- When you log on through CIS, you are going through a node. The node takes the form of 3 letters, designating the site of the computer through which you are connecting through Compuserve. An example would be "NYJ" (New York City). There are some special nodes you should know about, though.

Tymnet - Anybody logging on through Tymnet will be assigned one of these nodes - QAI, QAJ, QAK, QAC, QAM, QAN, QAO, QCA, QCB, QCC, QCE, QCF, QCH. This cannot identify where you are calling from, just that you are logging in through the Tymnet network.

Telenet - QBA, QBC, QBD, QBG, QBF, QEN, QEI, QEP.

Also, another special node would be DB- (DBA, DBB, DBC, etc), which means that the user is logging on from Compuserve's Headquarters in Dublin.

The way to tell what node somebody is in is by typing /UST on either CO mode on a SIG, or CB...the result is like this....

	Job	User Id	Ch.	Node	Handle
	---	-----	---	----	-----
1)	12	70003,1295	17	CSG	Red Leather
2)	133	70006,1293	1s	BAF	Surf's Up!
3)	69	76703,1211	Tlk	BOO	JOE CUFFS
4)	22	70000,1959	30*	DBA	Pig

Now, you can tell something specific about each of these four people based on the info given above. Red is in Columbus, Ohio, and is on Channel 17. She is

also a Compuserve Employee. Surf is in Bakersfield, California, and is a Customer service personnel. He is also using /SCRamble. Joe is in Talk, is a sysop on a SIG, and is in Boston, Massachusetts. This is the format for Talk on CB. Pig is on talk in a SIG, and is a security personnel from Dublin, Ohio. The format for showing if somebody is in /Talk is different on a SIG than in regular CB. Also, the /SEN command is not implemented on CB.

Have fun with this...hope it helps. Distribute the file however you want, but make sure the credits stay at the bottom.

(c) 1986 Morgoth/Lotus

==Phrack Inc.==

Volume One, Issue Eight, Phile #7 of 9

Fun with Automatic Tellers
by
+++The Mentor+++

Preface: This is not a particularly easy scam to pull off, as it requires either advanced hacking techniques (TRW or banks) or serious balls (trashing a private residence or outright breaking & entering), but it can be well worth your while to the tune of \$500 (five hundred) a day.

Laws that will be broken: Credit Fraud, Wire Fraud, Bank Fraud, Mail Fraud, Theft Over \$200, Forgery, and possibly a few others in the course of setting the scheme up (rape and murder are optional, but recommended.)

This all grew from an idea that Poltergeist had about a year ago before he turned fed on Extasy, and Cisban Evil Priest (Android Pope) and myself were implementing it with great success before our untimely arrest and recruitment into the service of the State. It is risky, but no more so than some of the more elaborate carding routines floating around.

The first step is to target your victim. The type person you are looking for is rich. Very rich.

Now, don't go trying to hit on J.P. Getty or Johnny Carson or someone who carries a high name recognition. This will just get you into trouble as everyone notices a famous person's name floating across their desk.

Instead look for someone who owns a chain of hog feed stores or something discreet like that. We targeted a gentleman who is quite active in the silver market, owning several mines in South Africa and not wanting this to be widely known (he had no desire to be picketed.)

Next step, take out a p.o. box in this person's name. Extasy wrote a good file on obtaining a box under a fake name, I don't know if it's still around. If not, there are several others out there. (Yeah, I know, this has already weeded out the weak of spirit. Anyone who has gotten this far without panic is probably going to get away with it.)

Now comes the fun part, requiring some recon on your part. You need to know some fairly serious details about this person's bank dealings.

- 1) Find out what bank he deals with mainly. This isn't too difficult, as a quick run through his office trash will usually let you find deposit carbons, withdrawal receipts, or *anything* that has the bank name on it.
- 2) Find out the account number(s) that he has at the bank. This can usually be found on the above-mentioned receipts. If not, you can get them in TRW (easier said than done) or you can con them out of a hassled bank teller over the phone (Use your imagination. Talk slowly and understandingly and give plausible excuses ["I work for his car dealership, we need to do a transfer into his account"].)
- 2a) [optional] If you can, find out if he has an ATM (Automatic Teller) card. You don't need to know numbers or anything, just if a card exists. This can also be ascertained over the phone if you cajole properly.
- 3) Armed with this information, go into action.
 - a) Obtain some nice (ivory quality) stationary. It doesn't

Change) had it. They converged on a sleeping RC who confessed everything.

Dr. Who is being charged with 16 counts of theft.

RC Modeler is being charged with larceny & possibly as an accomplice to theft.
Telenet Bob is being charged with 1 count of attempted theft.

Dr. Who and RC Modeler are reportedly out of the scene permanently and Dr. Who may be serving some prison time. Also, RC Modeler, when being questioned, was asked about Legion of Doom. This is VERY strange since we cannot figure out quite WHY this was asked.

Sysops are asked to clear their accounts form any bbs they were on.

The following is the interpretation of the same events as described by the Concord Journal. The real names of the phreaks involved have been censored.

Computer Theft Charge

An 18-year-old Concord man was charged on August 5, 1986 with stealing a \$3,300 computer [PDP-11/23 with Venix software] from Harvard University and a portable stereo from an unknown store by using checks, police allege he knew to be forged, to pay for the items, police said.

RC Modeler, was charged with two counts of larceny over \$100, police said.
[Also, accessory to the crime, RC says.]

Police issued a warrant for RC's arrest after being tipped-off by the North Adam's police that he had allegedly made purchases with checks they alleged to be stolen and forged.

North Adam's police, according to reports, arrested Doctor Who, of Lenox, MA. [and Telenet Bob], and charged him with using stolen and forged checks earlier this month. Police said Who told them about RC's purchases. They said Who wrote checks for the purchase of the computer equipment and the stereo for RC.

Well, RC might get off with 3 years of probation (including possible drug testing according to RC.). Dr. Who's court set is set for August 25, 1986. He will most likely be doing some prison time unfortunately. Please address all further questions to The Clashmaster.

Information Provided By The Clashmaster

Portrait Of The Typical Computer Criminal

August 11, 1986

from PC Week Magazine

In studying the typical computer criminal, the National Center for Computer Crime Data, in L.A., may have recently shattered some common myths.

Rather than being some genius computer programmer, according to the center's recently published report, the typical computer criminal is just that: quite typical. He's most often a male, with an average age of 22, and if not, he's next likely to be 19. Chances are he's a programmer, but if that job description doesn't fit, he's most likely a student or an input clerk.

Less than 5% of the time, this criminal will be either unskilled or unemployed, and less than 2% of the time will he be a computer executive.

In more than 40% of the cases that the center studied, criminals stole money, and if cash wasn't their style, they split between stealing information or programs and damaging software.

For these crimes, 4/5ths of those caught had to pay a fine or do community service or both, or serve less than 6 months in jail. In close to 1/5th of the cases, the criminal's only punishment was to make restitution.

Some notes from Sally Ride:::Space Cadet

Pisses me off! How dare they suggest we are not GENIUS computer programmers! Oh wait a minute, I know why they screwed up the statistics! They haven't caught the geniuses, so we throw off the statistical skew since we're still free.

Also I think it's high time computer executives start accounting for their fair share of computer crime! They probably don't get in the statistics either since they pull off the really big money rip-offs and it doesn't get published by the high power companies they work for so the public keeps faith in them.

Information Provided By Sally Ride:::Space Cadet

Dan Pasquale: Still Hostile or Ancient History?

September 8, 1986

Some updated information on Sergeant Dan Pasquale (Fremont, CA Police Department) aka The Revenger here. Supposedly he has been calling Oryan QUEST on several occasions and filling in Oryan as to his plans on whom to bust. However, an investigation into the truth of this matter shows otherwise.

Most recently, Oryan QUEST informed me that Dan Pasquale was trying to gain information on The Yakuza. I told The Yakuza about this and had him call Dan himself to find out what was going on.

Apparently he had no idea of who he was and had no idea of what he was talking about. He just said he'd no idea what I was talking about. He also said that he'd heard about a Shooting Shark incident much like this one. The Rocker of Speed Demon Elite also has called him claiming a similar story. The weird thing is, he also claims to not have talked to Oryan QUEST since around the beginning of summer. [Please note that Shooting Shark and The Rocker have been disliked by Oryan QUEST for some time and that situation has not changed].

Dan seemed pretty lax, didn't get excited, and seemed like a decent person all around. He said he hadn't been on a board for at least 3 months and that board was a legit one at that. He concluded by saying he didn't know who or why these rumors were starting up.

Some last things to add, Dan said that he isn't into busting phreaks/hackers and all that stuff anymore. He just proved his point with Phoenix Phortress, took his raise, and got out of the deal. He is now teaching at the academy and is doing patrols. But, aside from that, he claims to have nothing at all to do with the modem world.

Information Provided By [%] The Yakuza [%]

Please refer to past issues of Phrack World News for more information on Dan Pasquale and/or Phoenix Phortress

Zigmond Exposed

September 1, 1986

Finally after months of confusion and question, the truth about Daniel Zigmond is out. It would appear that Zigmond is not an on-staff programmer at Carnegie Mellon University after all, but instead was a sort of part time worker there. Indeed, Daniel just graduated high school with the class of 1986 and currently attends the University of Pittsburgh this fall. He started part time work at CMU on April 1, 1984 (April Fools? Not this time).

He does have a book coming out on Lisp programming which is what he did at Carnegie Mellon. All of this information came from his boss at CMU. As for Amiga World, Daniel has submitted a few articles, but he isn't "on staff." This came from his Amiga World editor.

The reason there is nothing listed in his TRW account now is obvious since he is not old enough to have obtained credit cards, bought a car/house, or much of anything else.

Zigmond says he lied about his age because he thought he would get more respect. He thought that people would think he was a rodent if they knew he was only 17 years old.

Daniel Zigmond received(s) quite a lot of prank phone calls, including a bomb threat that brought the police to his house, and I ask everyone to stop. He tried to screw around with the phreak/hack community, but no damage was done. Its time to leave him alone because ragging serves no purpose.

As for his article...only time will tell, but the general idea is that he made that up too just so he could become involved with the phreak/hack community.

Information Provided and Researched by Lucifer 666

Maxfield Strikes Again

August 20, 1986

Many of you probably remember a system known as "THE BOARD" in the Detroit 313 NPA. The number was 313-592-4143 and the newuser password was "HEL-N555,ELITE,3" (then return). It was kind of unique because it was run off of an HP2000 computer.

On the Private Sector BBS (Sponsored by 2600 Magazine), Bill From RNOC had posted a list of numbers that were related to John Maxfield and while none of the numbers were anything close to the bbs number listed above, Bill reminded us that Maxfield was the proud owner of an HP2000 computer.

This started started several people (including Sally Ride:::Space Cadet and myself) thinking that there might be a connection. Using resources that I cannot reveal, I was able to prove that "THE BOARD" was indeed a Maxfield/BoardScan operation. I also had learned that the BBS number itself really had call forwarding to one of Maxfield's own numbers. On August 15, 1986 I made this knowledge semi-public and warned Sally Ride:::Space Cadet and Ax Murderer (who lives locally to Maxfield). Unfortunately these warnings were in vain because on August 20, 1986 the following messages were found and sent to me by Sally Ride.

Welcome to MIKE WENDLAND'S I-TEAM sting board!
(Computer Services Provided By BOARDSCAN)
66 Megabytes Strong

300/1200 baud - 24 hours.

Three (3) lines = no busy signals!
Rotary hunting on 313-534-0400.

Board: General Information & BBS's
Message: 41
Title: YOU'VE BEEN HAD!!!
To: ALL
From: HIGH TECH

Posted: 8/20/86 @ 12.08 hours

Greetings:

You are now on THE BOARD, a "sting" BBS operated by MIKE WENDLAND of the WDIV-TV I-Team. The purpose? To demonstrate and document the extent of criminal and potentially illegal hacking and telephone fraud activity by the so-called "hacking community."

Thanks for your cooperation. In the past month and a half, we've received all sorts of information from you implicating many of you to credit card fraud, telephone billing fraud, vandalism, and possible break-ins to government or public safety computers. And the beauty of this is we have your posts, your E-Mail and--- most importantly ---your REAL names and addresses.

What are we going to do with it? Stay tuned to News 4. I plan a special series of reports about our experiences with THE BOARD, which saw users check in from coast-to-coast and Canada, users ranging in age from 12 to 48. For our regular users, I have been known as High Tech, among other ID's. John Maxfield of Boardscan served as our consultant and provided the HP2000 that this "sting" ran on. Through call forwarding and other conveniences made possible by telephone technology, the BBS operated remotely here in the Detroit area.

When will our reports be ready? In a few weeks. We now will be contacting many of you directly, talking with law enforcement and security agents from credit card companies and the telephone services.

It should be a hell of a series. Thanks for your help. And don't bother trying any harassment. Remember, we've got YOUR real names.

Mike Wendland
The I-team
WDIV, Detroit, MI.

Board: General Information & BBS's
Message: 42
Title: BOARDSCAN
To: ALL
From: THE REAPER
Posted: 8/20/86 @ 12.54 hours

This is John Maxfield of Boardscan. Welcome! Please address all letter bombs to Mike Wendland at WDIV-TV Detroit. This board was his idea.

The Reaper (a.k.a. Cable Pair)

Board: General Information & BBS's
Message: 43
Title: BOARDSCAN
To: ALL
From: AX MURDERER
Posted: 8/20/86 @ 13.30 hours

Hey guys, he really had us for awhile. For any of you who posted illegal shit, I feel sorry for you. I just can't wait to see his little news article. Cable Pair, do you have some sort of problem? If you've noticed, just about *everything* posted on this board is *legal*!!! So fuck off! You wanna get nasty? Well go ahead, call my house! Threaten me! HaHaHa, so what are you gonna do, take me to court for calling a bbs? Freedom of speech. YOU lose!

Ax Murderer

Your guess is as good as mine as to what happens next. For those of you who are interested, Mike Wendland can be reached at WDIV-TV, 313-222-0444, 313-222-0540, 313-222-5000, 313-222-0532.

Information Provided by

Ax Murderer/John Maxfield/Sally Ride:::Space Cadet/Knight Lightning
and the PWN Special Investigation Team

Maxfield is in general pretty proud of his efforts with THE BOARD. He says that a lot of the people that he voice verified should have known it was him. However, it is believed that he had a kid helping him do some of the validations.

According to John F. Maxfield the only reason this sting board was done was to show "What is currently happening in the phreak/hack community." He said no legal action will be taken at all, and besides, its fattened his "dossiers" on a lot of people!

PWN Quicknotes

There is a bulletin board called Alpha Center in the 514 NPA (Canada) that is being run by a guy named Mike Holmes who is writing a book on the personalities of phreakers and hackers. Mike will ask for your real name, address, phone number and other things, but it is not completely required. The board is 300 baud only.

The name of the book is reported to be "Phreak me out!" and it is supposed to be "not about how to phreak or hack, but about hackers lives and their trials and tribulations." If you would like to find out more about this board or the book before calling, either contact Attila the Hun or leave Mike Holmes a message at his voice mailbox (214)733-5283. For the general password contact anyone of the below contributors, myself or Taran King.

Information Provided By (8/1/86)

Attila The Hun/Ryche/Sticky Fingers/The Pyro

People in foreign countries will soon be able to have the benefits of our famous 800 (toll free) numbers. In place of the 800 number, foreign callers will dial 196. This will be followed by a unique prefix and the line number from the company's domestic 800 service.

It would work like this: 196-NXX-XXXX. AT&T will bill and record all these calls. This will give our overseas (and maybe Canada too) friends the opportunity to take advantage of the US toll network.

Information Provided By Sally Ride:::Space Cadet (8/1/86)

Mountain States Telephone and Pacific North West Bell are trialing work stations to be used to allow operators to work from home via the personal computer. Mountain States Telephone has over 100 people in various occupations working from home now, while Pacific North West has just built one entire operating office equipped with IBMs and have several employees working remotely using the same technology.

Information Provided By Sally Ride:::Space Cadet (8/8/86)

Supposedly, Bug Byter, Soft Jock, Street Urchin, the Bandit, the Gray Elf, Sea-Saw, and Quick Zipper have all were busted on August 5, 1986. It has also been reported that Street Urchin has to pay \$7000 in restitution.

Information Provided By Silent Assault (8/8/86)

A Commodore Hacker, Hackin Hank was busted for abusing MCI codes and had to pay a \$2000 phone bill. He was caught after a person he called was called by MCI Investigations. This person got scared and told them everything he knew.

Information Provided By Red Baron (8/8/86)

The following two phreaks were sentenced about 2 months prior to the date.

MOB RULES, who was busted for MF Scanning that he had done 2 years previous, got 90 days in jail, 360 hours of community service, and 5 years probation.

Video Vance has been given a flat 90 days in jail for being caught with 11 cases of dynamite.

Information Provided By <S><C><A><N><M><A><N> (8/8/86)

There is a bulletin board in Australia with many users interested in learning to phreak and hack. They need experienced people to converse with. Tell the sysop that you are calling from America. The number is 61-3-509-9611.

Information Provided By Mad Madness (8/14/86)

Shadow Hawk 1 was busted for hacking two RSTSS in Chicago. They acquired all of his printouts and disks with information on it. Info by Shadow Hawk 1. (8/11/86)

The Prophet, formally of the PhoneLine Phantoms, was recently contacted by authorities for as yet unknown reasons. He has had his computer equipment confiscated, but as of this writing he has not been formally charged. And to clear up the rumor, I did not have anything to do with it.

Information Provided By Solid State (8/23/86)

Some notes about Night Stalker's bust here, I haven't really talked much to him because his phone line is bugged, I could tell that much from all of the clicks that I heard after he had hung up while I was still on the line.

Some of the reasons that he may have been busted were that credit Card numbers were frequently posted on The Underground and two months ago a member of the Underground called the White House with a bomb threat and was later visited by the U.S. Secret Service. They knew this person had used illegal extenders and codes to make the call. They inquired to where he obtained them and he told them all about The Underground.

He is currently under surveillance, the Secret Service thinks he is transferring funds and have been following him and taking pictures, especially when he visited his bank. That's about all I know...end of the investigation.

Information Provided By Night Stalker

In the last week of July, Cyclone II mistakenly was playing with a local VAX and became a bit careless with his methods. He was caught. You may have noticed that he hasn't been calling around for quite awhile. He won't be until this mess is cleared up, which should be in the near future.

His computer was confiscated, as well as all of his files, papers, notes, and anything else the authorities could find that was illegal. He is laying low and would prefer not to receive too many calls.

Information Provided by Cyclone II (8/4/86)

Msg#: 7284 *COMMUNICATIONS*
05/28/86 19:43:24 (Read 42 Times)
From: SHAWN
To: ALL
Subj: CODES

OK HERE WE GO 800 446 4462 SKYLINE (CODE: XXXXXXXX)
 800 626 9600 CODE (XXXXXXX)
 800 222 4482 CODE (XXXXXX)
 800 521 8400 CODE (XXXXXXXXX)
 800 227 0073 CODES (xxxxXxx X=0-9)
METRO CODES: XXXXXX, XXXXXX, XXXXXX, XXXXXX, XXXXXX
PBX: 312 455 7287 (CODE XXXX+Y)
503 652 6016: ID: XXX,XXX PASS ****

later,
 Shawn

[In the above message, the numbers were followed by codes that I have since censored out. This magazine will *NOT* publish codes.]

[It's common knowledge that a BBS userlog must be blanked before a BBS can be used as a sting board. I've also heard that law enforcement officials have been trying to bust P-80 and Scan Man for a long time, but have not been able to accomplish anything. Even the infamous Detective Dan Pasquale {See past issues of Phrack World News, "Phoenix Phortress Stings 7" and "Oryan QUEST Vs. Dan Pasquale"} and John Maxfield, head of BoardScan, are frustrated at being unable to deal with Scan Man. On June 20, 1986, or thereabouts, the following message appeared in the logon to P-80;

 "BI-ANNUAL USERLOG CLEANUP IN
 EFFECT. ALL MEMBERS PLEASE
 RE-LOGIN AS A NEW USER..."]

Msg#: 7870 *COMMUNICATIONS*
06/20/86 22:04:41 (Read 50 Times)
From: ICARUS 1
To: ALL
Subj: TMC BUST

TMC has just nailed a hacker associate of mine for \$935. The destination numbers were called and someone spilled their guts. The guy who got busted is worried because the Alliance bills have not come in yet. TMC users beware. Make sure your friends are amnesiacs as the phreaker's bible says.

Icarus

[Some friendly advice from Icarus 1, too bad not everyone heeded the message.]

Msg#: 7894 *COMMUNICATIONS*
06/21/86 19:44:09 (Read 44 Times)
From: ICARUS 1
To: SCAN MAN (Rcvd)
Subj: REPLY TO MSG# 7870 (TMC BUST)

He was busted by TMC in the state of Nebraska.

Icarus

Msg#: 7898 *COMMUNICATIONS*

06/21/86 20:43:10 (Read 43 Times)
From: MAX MADDNESS
To: ICARUS 1 (Rcvd)
Subj: REPLY TO MSG# 7870 (TMC BUST)

Hey check it out, I use TMC in Youngstown, Ohio (216-743-6533), but when TMC calls my phreak friends, they think the calls originate from Akron, Ohio which is 60 or so miles away. So when TMC calls and asks, "Do you know anyone in Akron?" people usually are honest and just say no. So even if I call +relatives, etc. usually I'm safe.

Max

Msg#: 7880 *COMMUNICATIONS*
06/21/86 05:30:37 (Read 51 Times)
From: THE FALCON
To: ALL
Subj: TMC

What is the number to TMC? I just want to know so that I'm sure not to use it. Oh well, thanx and later.

The Falcon

Msg#: 7952 *COMMUNICATIONS*
06/23/86 13:06:23 (Read 44 Times)
From: SHAWN
To: ICARUS 1 (Rcvd)
Subj: REPLY TO MSG# 7870 (TMC BUST)

Well I told you guys a while ago that this would happen so stay away from them.

Icarus

Msg#: 7961 *COMMUNICATIONS*
06/23/86 17:15:41 (Read 47 Times)
From: BLADE RUNNER
To: ALL
Subj: TMC

I was wandering around some guys hard drive this weekend and found some AT&T mail regarding TMC. From what I understand TMC is involved in the AT&T AGETRIAL project. Which indicates to me that TMC is also into computers and consequently knows what a hacker is. Another thing that was found was some information on the 1PSS switch that has been developed by AT&T and has already been deployed in dome BOCS and other communications networks. This troubles me in that this is the first that I have heard about it. I meant to say that it has been deployed on some networks already. If you have any valid information on the 1PSS SWITCH please post it and it will show up in the P.H.I.R.M. update issue for July, giving you credit for the information of course.

BLADE RUNNER (PRESIDENT)
P.H.I.R.M.

Msg#: 8456 *COMMUNICATIONS*
07/13/86 13:48:51 (Read 75 Times)
From: SCAN MAN
To: SHAWN (Rcvd)
Subj: REPLY TO MSG# 7691 (GENERAL)

GOT ANY CODES FOR 800-451-2300?

[***IMPORTANT*** This is TMC's Miami, Florida dial-up. An interesting request from the sysop of one of the nation's top code boards. For those of you who remember it was Scan Man who asked the infamous Whacko Cracko Brothers, Inc. {See PWN Issue II, "The Life And Crimes of The Whacko Cracko Brothers, Inc."} to scan some codes on a certain dial-up just before they were arrested. Now he is asking Shawn for TMC codes, kinda interesting that Shawn got investigated less than a week later by TMC Security Department isn't it?]

Msg#: 8970 *COMMUNICATIONS*
08/10/86 06:41:48 (Read 34 Times)
From: SHAWN
To: SCAN MAN (Rcvd)
Subj: REPLY TO MSG# 8456 (GENERAL)

Well sorry it took me so long to find this message I kept forgetting to look at this one. Anyway if you really need some [codes, referring to the last message] I can dig some up easy enough well hack some I should say noting you can get about 100 in a matter a 10 or 15 minutes so its no big deal to me either way also watch 800 637 7377 I'm telling you now people that this company has tracing stuff and I have talked with them they offer me a job and I'm goin to take it but dont worry I'm not goin to be busting people I have to make it so you guys cant get in notin it is very easy to make it at least very hard to do ho well be careful.

[Be careful indeed! 800-637-7377 is TMC's Las Vegas dial-up. What would you do if you were about to lose your computer and maybe your freedom? Work for the other side? The kid really has a way with words, I haven't seen spelling and grammer like that since first grade. As for his not busting people, isn't that a laugh, he has already stated that he will bust anyone he can starting with the lower level phreaks who are only into code abuse.]

Msg#: 8974 *COMMUNICATIONS*
08/10/86 13:14:13 (Read 34 Times)
From: JOHNNY ROTTEN
To: ALL
Subj: PHREAKERS QUEST

To all users of Phreaker's Quest...

What happened to it? It just rings. If you have any info. Leave mail or whatever.

<Johnny Rotten>

Msg#: 9058 *COMMUNICATIONS*
08/13/86 06:58:12 (Read 30 Times)
From: SHAWN
To: JOHNNY ROTTEN
Subj: REPLY TO MSG# 8974 (PHREAKERS QUEST)

Well you see I came very close to getting busted they called my voice line that is TMC of 800 637 7377 and I have never given it out to anyone at all [I bet!] so I knew that i was in for it they told me they knew I ran a board and they said they could not get in I kept deleted them haha anyways I had 2 choices 1 take it down 2 get busted.

[Wonder how they got your home number Shawn? Did you give it out for validation on Pirate-80? Maybe around the time of the "Bi-annual userlog

cleanup"? Or, could it be the cops are smart enough to ask the phone company for any other line running into a house where a suspect BBS is running?]

Msg#: 9052 *COMMUNICATIONS*
08/12/86 19:10:47 (Read 29 Times)
From: JIM RATH
To: ALL
Subj: TMC

Listen people... it is time to stop screwing with TMC.. (7377 number). Our good friend Shawn of Phreakers Quest just had his BBS put down from them. Shawn met some guy from TMC, and they have had ANI on the number for months now. If you value your own security, throw away any and all TMC information NOW, or you might be suffering the consequences later.

For details on the "Bust" call Theives Underground II. It's SCARY!

Msg#: 9054 *COMMUNICATIONS*
08/12/86 23:50:02 (Read 28 Times)
From: SCAN MAN
To: JIM RATH (Rcvd)
Subj: REPLY TO MSG# 9052 (TMC)

Where is Thieves Underground located?

[Why is Scan Man so interested in what Shawn is saying about his experience with TMC? I mean plenty of people on Pirate-80 have run-ins with some form of security everyday and he doesn't go researching them, why is this "TMC Run-IN" so important to him? Maybe he has a personal reason to be interested, then again maybe not.]

Msg#: 9086 *COMMUNICATIONS*
08/14/86 13:36:37 (Read 25 Times)
From: JIM RATH
To: SCAN MAN (Rcvd)
Subj: REPLY TO MSG# 9054 (TMC)

I believe TU is in Texas somewhere.. dunno where exactly (never really bothered remembering).. 214 AC though

Msg#: 9110 *COMMUNICATIONS*
08/15/86 03:54:20 (Read 16 Times)
From: SHAWN
To: JIM RATH (Rcvd)
Subj: REPLY TO MSG# 9052 (TMC)

If you want some details why dont you just ask me seeing as though i would be the one to ask the TU only knows what i tell him and scan man i need to talk with you about this they did have an idea of some things going on here and so one i would rather say it to yo then type it in

shawn

Indeed, what is going on here Shawn? Just what did TMC mention about Pirate-80? And why not post it in on the public boards? For the answer to that maybe one could talk to Jeff Namey who works for TMC and is very proud to acclaim the efforts of one Scott Higgonbotham and his sting BBS Pirate 80 which has, in his own words, "Saved my company from near bankruptcy at the hands of

the hackers."

It is also interesting to note that Scan Man recently admitted to being a computer security consultant in Phrack Pro-Phile IV. He said his boss didn't know about his outside phreak/hack interests.

Scan Man also claims to have infiltrated various security organizations. I wonder if he has infiltrated or simply joined as a regular member.

The following are highlights of a conversation with Ben Graves of TMC, around August 25th or 26th (SR=Sally Ride BG=Ben Graves):

SR: Mr. Graves I need to talk to you about one of your employee's a Scott Higgonbotham (Scan Man).

BG: What about Scott?

SR: Well, my company is concerned with the impact of computer hackers on our business. Scott attended a convention in Miami around January and gave his business card to one of our security people. I'm following up on their conversation with the idea that perhaps my company could be given access to Scott's electronic bulletin board. In this way we could monitor for hackers abusing our codes.

BG: That may be something we can arrange. I know that Scott has been a great help to TMC since we were able to pick him up. We began to have a big problem with hackers awhile back and Scott seems to have some of the answers. He's not in right now, can I have your number and I'll have him call you back?

SR: You sure can. So, Scott's bulletin board has helped you reduce your losses to toll fraud?

BG: Well, that's just one of the ways Scott has used to work on the problem. But, he has been very effective.

SR: Thanks, Ben, I'll be waiting for the call.

The following are highlights of conversation with Pauline Frazier of TMC from around September 5, 1986 (Sally Ride: SR Pauline Frazier: PF)

Operator: TMC, may I help you?

SR: Yes, Ben Graves, please.

Operator: I'm sorry, Mr. Graves is no longer employed here.

SR: Oh!? Well, is Scott Higgonbotham in?

Operator: One moment, please.

PF: Hello, this is Pauline Frazier, I'm the office manager, may I help you?

SR: Well, maybe, I was trying to reach Ben Graves, I just talked to him last week about another one of your employees, Scott Higgonbotham, now the receptionist says Ben no longer works here.

PF: Yes, that is true, and neither does Mr. Higgonbotham.

SR: May I ask why?

PF: I'm really not able to say much, I think you should talk to our

Regional Security Director, Kevin Griffio, he's on 804-625-1110. He could tell you much more than I can.

SR: O.K., but maybe I should tell you why I'm interested. I was talking to Ben about an electronic bulletin board Scott is running. My company has someone on it and we're concerned that things might not be legal on there. There are access codes being posted of my company's and yours'. Could that be why they're no longer employed?

PF: Do you mean he is posting TMC codes on there?

SR: Well, I can't say he's the one posting the codes, but he is letting them be posted, along with a lot of other information such as computer logins and passwords.

PF: Well, you know I never did like it when they hired that fellow. And, I told them so, too. When he started we had a problem with toll fraud, but nothing like it is now. He was able to catch a few of those hackers while he was here, and we pressed charges, but the problem just seemed to get worse and worse.

SR: So, he actually had some hackers arrested?

PF: Yes, several. He started working here in Charleston and then they sent him to New York when things got bad up there. But, things never have gotten any better since he's started here or in New York either. Sir, please, call Mr. Griffio about all this he can tell you more than I.

SR: I will. Do you think he'd be in now?

PF: Well, it's late here and he's probably gone home, try Monday.

SR: Thanks, I will.

(But you told me plenty, sweetheart!)

[For the record I had a VERY similar chat with Pauline Frazier, it turned up the same results.]

The following are highlights of a conversation with Kevin Griffio, TMC, September 9th (Sally Ride: SR Kevin Griffio: KG).

Oper: TMC, may I help you?

SR: Yes, Kevin Griffio, please.

Oper: His line is busy now, can he call you back?

SR: Well, this is urgent, may I hold?

Oper: Certainly, I'll let him know you're holding.

KG: Hello, this is Kevin.

SR: Mr. Griffio I've been referred to you by one of your Charleston employees, Pauline Frazier. She felt I should tell you what I told her yesterday about one of your now former employees, I think, Scott Higgonbotham.

KG: Yeah, we let him go just last week. What about him?

SR: My company feels Scott is running an illegal BBS and has for sometime been allowing access codes to be posted. Codes for your company's toll switches as well as ours and other's are being entered on his system as

well as computer system logins and passwords.

KG: Well, I'm not surprised. I have been to Scott's home to see the bulletin board. I knew codes were being posted, but I thought he was taking care of reporting them.

SR: May I ask why you let him go?

KG: Certainly, Scott just wasn't solving our problems. In fact, some of our people have thought he was somewhat to blame for many of them. Even though, at first, he appeared to be the answer. He was able to identify several computer hackers for us.

SR: So, he did bust some hackers? Has he done so recently? I think a young man using the name Shawn on the bulletin boards was recently identified by your company.

KG: No, he hasn't gotten anyone recently that I'm aware of, but he could have turned them over to one of the local franchises. You see TMC is a franchise operation. We try to help the franchises, but many do their own thing. We wouldn't necessarily know about all that goes on.

SR: I'm sorry to hear you had this trouble. Perhaps, my company could be of assistance. We do work of a similar nature.

KG: I'd certainly be interested in any help you could give. Can you put together a written proposal?

I also had an interesting conversation with Larry Algard of Pacific Northwest Bell. He confirmed that he had met Scott Higgonbotham at the Miami CFCA conference last January. He also mentioned that Scott had told him about his "sting" bulletin board, Pirate-80 in West Virginia.

For those who are interested:

TMC (Charleston Office).....304-345-7275
Pauline Frazier, Office Manager (TMC).....See above
Jeff Namey, Accounts Receivable (TMC).....304-744-6555
TMC (Miami Office).....305-371-3544
TMC (Tidewater).....804-625-1110
Larry Algard (Pacific North West Bell).....503-242-8862
Pacific North West Bell (Employee Directory)..800-426-7039

Or write to; TMC
405 Capitol St.
Parlor Suite
Charleston, West Virginia 25301

All the thoughts in []'s and other information are the insane ramblings of Sally Ride:::Space Cadet and Knight Lightning, you tell me, are we spaced out or what?! The TMC employee interviews were by Sally Ride:::Space Cadet with me doing the background information.

It was at this point in time that we decided to have a talk with Scan Man directly and give him a chance to clear his name and reputation.

Unfortunately, Scan Man was very uncooperative and constantly avoided answering the questions I asked him. He also added that everything said in the interviews were lies. He claims that Kevin Griffio has never been to his house, he doesn't know Ben Graves, and Pauline Frazier hated him because she knew he was a hacker.

He then went on to imply that Sally Ride:::Space Cadet was actually an employee

of some communications carrier himself because of the terminology he used in some of his posts on P-80.

Scan Man claimed that he has been telling people that he worked for TMC for quite some time and he only needed the codes from Shawn because he was going to be in Miami later that week. In other words, Shawn's near bust and his asking for TMC codes may have been a simple coincidence.

He claims to have done system analysis for TMC, but also admitted to securing some of their computer systems, which isn't a crime.

As for his being at the Miami CFCA conference, I will assume that he was infiltrating the con and was spotted as being a hacker. In order to gain the respect and confidence of the security officials, he told them that his bulletin board was a sting. Now, that story completely is believable with the exception of how he arrived, a plane trip paid for by TMC.

Scan Man's last words contained a threat that if this affected his home life, he would personally track down the writers and contributors and shoot them with his rifle.

Notes from KL:

One thing that I should mention is the fact that Pirate-80 has *NEVER* been busted or investigated. I mean its not hard to get onto and there are codes plastered everywhere you look. How many boards do you know of that have been busted for having codes on them? One example of this is with the credit card numbers owned by Richard Sandza, author of "The Night Of The Hackers" and "The Revenge Of The Hackers," both printed in Newsweek Magazine.

"It wasn't long before I found out what was being done with my credit-card numbers, thanks to another friendly hacker who tipped me to Pirate 80, a bulletin board in Charleston, W. Va., where I found this: 'I'm sure you guys have heard about Richard Standza [sic] or Montana Wildhack. He's the guy who wrote the obscene story about phreaking in NewsWeek [sic]. Well, my friend did a credit card check on TRW...try this number, it's a VISA...Please nail this guy bad...Captain Quieg [sic].'"

See this? This was published in "The Revenge Of The Hackers" in Newsweek Magazine! And what happened to P-80? Nothing! Here Richard Sandza has just announced to thousands of people that P-80 has credit card numbers posted on it and nothing happened. Why? The answer to that is left to the reader.

There are a few other things to mention about Scan Man/P-80/TMC. Supposedly all of the computer equipment that P-80 runs on was donated by TMC themselves. It is also believed that Scan Man's only duty to the company was to report TMC codes so that they could be turned off. It would appear that this had changed but, we at Phrack Inc. in no way take any opinion whatsoever about the innocence or guilt of Scan Man. We leave it to the reader to decide for him/herself.

I'm sure all parties concerned would appreciate you NOT calling the above numbers if all you plan to do is harass people or anything else among those same lines. After all a job is a job and harassing someone wouldn't do anyone any good either, it would just make them mad. If you are going to call, make sure it is for knowledge purposes only! Above all do NOT call Scan Man to harass him or his innocent family. My suggestion is that if you feel that Scan Man is an informant or whatever, then stop just calling his board.

One last thing, a *VERY* big thank you to Sally Ride:::Space Cadet for a job well done and for all the time he spent working on the article.

Information Provided by

Knight Lightning & Sally Ride:::Space Cadet

and directly/indirectly by

Blade Runner/Evil Jay/Forest Ranger/Icarus 1/Jack The Ripper/Jim Rath
Johnny Rotten/Larry Algard/Max Madness/Oryan QUEST/P-80 Systems/Scan Man/Shawn
Suicidal Nightmare/Taran King/The Falcon/TMC Staff

and other Anonymous Sources

PS: For those interested, this investigation was sparked by the interception of a memo from Larry Algard (Pacific Northwest Bell) to his boss, George Reay. What was in the memo? Several things, but mostly it spoke of the January CFCA (Communications Fraud Control Association) conference in Miami, Florida where Larry met one Scott Higgonbotham, Security Director for TMC (Tele-Marketing Company) who told him that he operated a "sting" bulletin board named Pirate 80 in West Virginia.
