==Phrack Inc.==

Volume Three, Issue 26, File 1 of 11

Phrack Inc. Newsletter Issue XXVI Index
%%
April 25, 1989

Greetings and welcome to Issue 26 of Phrack Inc. Things are really beginning to heat up as SummerCon '89 rapidly approaches. Be sure to check out
Phrack World News for further information concerning this incredible event. You do not want to miss it.

This issue we feature The Disk Jockey's personal rendition of the events that can occur in the criminal legal process (after all he should know). Some of the terms and situations may vary from state to state due to slight differences in state laws.

We also present to you a file on COSMOS that is written from more of a security standpoint rather than hacker intrusion tips. The Future Transcendent
Saga continues in this issue with a file on NSFnet and the third appendix of the never ending series. This particular appendix is geared to be used as a general reference to chapter three of the FTSaga, "Limbo To Infinity." As this
file is more of a complied directory than actual "how to" knowledge, we just consider it a Phrack Inc. release.

As always, we ask that anyone with network access drop us a line to either
our Bitnet or Internet addresses...

Taran King
C488869@UMCVMB.BITNET
C488869@UMCVMB.MISSOURI.EDU

Knight Lightning
C483307@UMCVMB.BITNET
C483307@UMCVMB.MISSOURI.EDU

Table of Contents:

==Phrack Inc.==

Volume Three, Issue 26, File 2 of 11

Computer-Based Systems for Bell System Operations

by

Taran King

This file contains a variety of operating systems in the Bell System. Some of them are very familiar to most people and others are widely unknown. Each sub-section gives a brief description of what the computer system's functions are.

Table Of Contents:

TIRKS (Trunks Integrated Records Keeping System)

TIRKS is the master record-keeping system for the network. It supports network operations related to growth and change in the network by providing accurate records of circuits and components that are in use and available for use. It was developed to mechanize the circuit-provisioning process. Two circuit-provisioning aspects are applied: daily circuit provisioning and current planning.

Daily circuit provisioning is processing orders to satisfy customer needs for special service circuits and processing orders initiated for message trunks and carrier systems for the PSTN. The process begins at various operations centers and ends up at the CPCs (Circuit Provision Centers) which track orders, design circuits, and assign the components using TIRKS. It also prepares work packages and distributes them to technicians working in the field

who implement them.

Current planning determines the equipment and facility requirements for future new circuits. It apportions forecasts for circuits among the circuit designs planned for new circuits.

TIRKS consists of five major interacting component systems: COC (Circuit Order Control system), E1 (Equipment system), F1 (Facility system), C1 (Circuit system), and FEPS (Facility and Equipment Planning System).

- o COC controls message trunk orders, special-services orders, and carrier system orders by tracking critical dates throughout the existence of an order as it flows from the source to the CPC and on to the field forces. It provides management with the current status of all circuit orders and provides data to other TIRKS component systems to update the assigned status of equipment, facilities, and circuits as orders are processed.

- o C1 is the heart of TIRKS. It automatically determines the types of equipment required for a given circuit, assigns the equipment and facilities needed, determines levels at the various transmission level points on the circuit, specifies the test requirements, and establishes circuit records for the circuits. All records of circuits already installed are kept in C1 for future additions or changes.

- o E1 is one of the two major inventory component systems in TIRKS. It contains equipment inventory records, assignment records, and pending equipment orders. The records show the amount of spare equipment that is available and equipment's circuit identification.

- o F1 is the other of the major inventory component systems. It contains cable and carrier inventory and assigns records.

- o FEPS supports the current planning process which determines the transmission facilities and equipment that will be required for new service. It uses data in E1, F1, and C1 as well as other forecasts to allocate existing inventories efficiently, to determine future facility and equipment requirements, and to update planning designs.

TIRKS uses IBM-370 compatible hardware and direct-access storage devices. It provides benefits to the BOCs through improved service to customers, capital and expense savings, and better management control.

PICS (Plug-in Inventory Control System)

%%

PICS is the mechanized operations system developed for the efficient management of large amounts of equipment inventories. It assists with both inventory and materials management. Inventory managers establish corporate policies for the types of equipment and for equipment utilization, assist engineering organizations in introducing new types of equipment while phasing out older types, and set utilization goals that balance service objectives and carrying charges on spare equipment. Material managers work to achieve utilization goals by acquiring spare equipment for growth and maintenance purposes. They also administer a hierarchy of locations used for storing spare equipment.

PICS/DCPR (PICS with Detailed Continuing Property Records) administers

all types of CO equipment. The DCPR portion of PICS/DCPR serves as a detailed investment database supporting accounting records for all types of CO plug-in and "hardwired" equipment. PICS/DCPR accomplishes its goals of increasing utilization, decreasing manual effort, and providing a detailed supporting record for phone company investment through software, databases, administrative procedures, and workflows.

Two new functional entities are created in the BOC first: PIA (Plug-In Administration) and the central stock. PIA is the materials manager and is responsible for acquiring equipment, distributing it as needed to field locations, repairing it, and accounting for it. The central stock is a warehouse where spare equipment is consolidated and managed.

There are five subsystems in PICS/DCPR:

- Plug-in inventory subsystem - maintains order, repair, and inventory records for all types of plug-in equipment.
- Inventory management subsystem - provides the PIA with mechanized processes to assist in various tasks.
- Plug-in DCPR subsystem - provides processes required to maintain investment records for plug-in units.
- Hardwired DCPR subsystem - maintains detailed accounting records for hardwired CO equipment.
- Reference file subsystem - provides and maintains reference data used by all other subsystems.

PICS/DCPR runs on IBM-compatible equipment with the IBM Information Management System database manager. It interfaces with TIRKS as well as a few other circuit-provisioning systems.

PREMIS (PREMises Information System)

PREMIS provides fast, convenient access to information needed to respond to service requests. It was developed in response to the need for address standardization. It has three mechanized databases: address data, a credit file, and a list of available telephone numbers. It also serves a function to the LAC (Loop Assignment Center), called PREMIS/LAC. PREMIS/LAC is an extension of the address database and provides for the storage of outside plant facility data at each address entry.

PREMIS supports the following service representative tasks:

- Determining the customer's correct address. The address related- and address-keyable information is the major feature of PREMIS. If an input request does not contain an accurate or complete address, PREMIS displays information that can be used to query the customer. The address database allows PREMIS to give the full address and information about the geographic area which includes WC (Wire Center), exchange area, tax area, directory group, and the service features available for that area. It also displays existing or previous customer's name and telephone number, modular jacking arrangement at the address, and an indication of whether a connect outside plant loop from the address back to the CO was left in place. If service was discontinued at the site, the reason for disconnect and the date of disconnect are also displayed.

- Negotiating service features. PREMIS indicates the service features that can be sold at that address, providing useful information for discussing these with a customer.

- Negotiating a service date. If it indicates that an outside plant loop back to the CO has been left in place, PREMIS allows for earlier installation as no installer will need to visit the site.

- Checking a customer's credit status. PREMIS maintains a name-keyable file of customers with outstanding debts to the telephone company. If there is a match in the database, the customer's file is displayed.

- Selecting a telephone number. There is a file in PREMIS listing all available telephone numbers from which service representatives request numbers for a specific address. The available telephone numbers are read from COSMOS (COmputer System for Mainframe OperationS) magnetic tape.

PREMIS/LAC has a feature called DPAC (Dedicated Plant Assignment Card). Records of addresses where outside plant loop facilities are dedicated are organized and accessed by address by the LAC through DPAC.

PREMIS is an on-line interactive system whose prime users are service representatives interacting with customers. It uses the UNIVAC 1100 as its main computer. It has network links to various other computer systems, too, to obtain various pieces of information that are helpful or necessary in efficiently completing service functions.

TNDS (Total Network Data System)

TNDS is actually a large and complex set of coordinated systems which supports a broad range of activities that depend on accurate traffic data. It is more of a concept that incorporates various subsystems as opposed to a single computer system. It consists of both manual procedures and computer systems that provide operating company managers with comprehensive, timely, and accurate network information that helps in analysis of the network. TNDS supports operations centers responsible for administration of the trunking network, network data collection, daily surveillance of the load on the switching network, the utilization of equipment by the switching network, and the design of local and CO switching equipment to meet future service needs.

TNDS modules that collect and format traffic data usually have dedicated minicomputers which are at the operating company's Minicomputer Maintenance (Operations) Center (MMOC/MMC). Other modules generate engineering and administrative reports on switching systems and on the trunking network of message trunks that interconnects them. These mostly run on general-purpose computers. Still others are located in AT&T centers and are accessed by various operating companies for data.

The functions of TNDS are carried out by various computer systems since TNDS itself is just a concept. These subsystems include EADAS, EADAS/NM, TDAS, CU/EQ, LBS, 5XB COER, SPCS COER, ICAN, SONDS, TSS, CU/TK, TFS, and CSAR. The following sections cover these systems briefly.

EADAS (Engineering and Administrative Data Acquisition System)

EADAS is the major data collecting system of TNDS and runs on a

dedicated minicomputer at the NDCC (Network Data Collection Center). Each EADAS serves up to fifty switching offices. The 4ESS and No. 4 XBAR both have their own data acquisition systems built into the switch and they feed their data directly to other TNDS component systems that are downstream from EADAS, thereby bypassing the need for EADAS on those switches. EADAS summarizes data collected for processing by downstream TNDS systems and does so in real-time. EADAS is used by network administrators to determine quality of service and to identify switching problems. It also makes additional real-time information available to these administrators by providing traffic data history that covers
up to 48 hours. This data history is flexible through the module NORGEN (Network Operations Report GENerator) so that administrators can tailor their requests for information to determine specifics. Information from EADAS is forwarded to other downstream systems in TNDS via data links or magnetic tape.

EADAS/NM (EADAS/Network Management)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

EADAS/NM is one of the three TNDS systems that EADAS forwards traffic data downstream to either by data links or magnetic tape. EADAS/NM uses data directly from EADAS as well as receiving data from those switching systems which do not interface with EADAS previously mentioned. It monitors switching systems and trunk groups designated by network managers and reports existing or
anticipated congestion on a display board at local and regional NMCs (Network Management Centers). It is used to analyze problems in near real-time to determine their location and causes. EADAS/NM provides information that requires national coordination to the AT&T Long Lines NOC (Network Operations Center) in Bedminster, NJ which uses it's NOCS (NOC System) to perform EADAS/NM-like functions on a national scale. Like EADAS, EADAS/NM uses dedicated minicomputers to provide interactive real-time response and control.

TDAS (Traffic Data Administration System)
%%

The second of three TNDS systems that is downstream from EADAS is TDAS
which formats the traffic data for use by most of the other downstream systems.
It accepts data from EADAS, local vendor systems, and large toll switching systems on a weekly basis as magnetic tape. It functions basically as a warehouse and distribution facility for the traffic data and runs a batch system at the computation center. Correct association between recorded traffic
data and the switching or trunking elements is the result of shared information
between TDAS and CU/EQ. Data processed through TDAS is matched against that stored in CU/EQ. The data is summarized weekly on magnetic tape or printout and is sent for use in preparation of an engineering or administrative report.

CU/EQ (Common Update/EQuipment)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

CU/EQ is a master database which stores traffic measurements taken by TDAS and it shares information with TDAS, ICAN and LBS. As said before, correct association between recorded traffic data and the switching or trunking
elements is due to the shared information between CU/EQ and TDAS. It runs as a
batch system in the same computer as TDAS and is regularly updated with batch transactions to keep it current with changes in the physical arrangement of CO

switching machines which ensures that recorded measurements are treated consistently in each of the reporting systems that use CU/EQ records.

ICAN (Individual Circuit ANalysis)

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

The final of the three systems downstream from EADAS is ICAN, which also uses data directly from EADAS but uses CU/EQ for reference information. It is a CO reporting system which detects electromechanical switching system faults by identifying abnormal load patterns on individual circuits within a circuit group. ICAN produces a series of reports used by the NAC (Network Administration Center) to analyze the individual circuits and to verify that such circuits are being correctly associated with their respective groups.

LBS (Load Balance System)

%%%%%%%%%%%%%%%%%%%%%%%%%

LBS is a batch-executed system that helps assure the network administrator that traffic loads in each switching system are uniformly distributed. It analyzes the traffic data to establish traffic loads on each line group of the switching system. The NAC uses the resulting reports to determine the lightly loaded line groups to which new subscriber lines can be assigned. LBS also calculates load balance indices for each system and aggregates the results for the entire BOC.

5XB COER (No. 5 Crossbar Central Office Equipment Reports)

%%

The 5XB COER provides information on common-control switching equipment operation for different types of switching systems. It is a batch-executed system that runs on a BOC mainframe that analyzes traffic data to determine how heavily various switching system components are used and measures certain service parameters. It calculates capacity for the No. 5 Crossbar. Network administrators use 5XB COER reports to monitor day-to-day switching performance, diagnose potential switching malfunctions, and help predict future service needs. Traffic engineers rely on reports to assess switching office capacity and to forecast equipment requirements. It produces busy hour and busy season reports so service and traffic load measurements can be most useful in predictions.

SPCS COER (Stored-Program Control Systems Central Office Equipment Reports)

%%%

The SPCS COER is basically the same as the 5XB COER as it too monitors switching system service and measures utilization in the same manners as mentioned above. The essential differences between the 5XB COER and the SPCS COER are that the latter calculates capacity for 1ESS, 2ESS, and 3ESS switching offices as opposed to the No. 5 Crossbar switch and SPCS COER is an interactive system that runs on a centralized AT&T mainframe computer.

SONDS (Small Office Network Data System)

%%

SONDS collects its own data from small step-by-step offices independently of EADAS and TDAS. It performs a full range of data manipulation functions and provides a number of TNDS features economically for smaller electromechanical step-by-step offices. The data collected is directly from

the offices being measured. It processes the data and automatically distributes weekly, monthly, exception, and on-demand reports to managers at the NACs via dial-up terminals. SONDS runs on an interactive basis at a centralized AT&T mainframe computer.

CU/TK (Common Update/TrunKing)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

CU/TK is a database system that contains the trunking network information and as well as other information required by TSS (Trunking Servicing System) and TFS (Trunk Forecasting System). The CU/TK is regularly updated by CAC (Circuit Administration Center) by personnel to keep it current with changes in the physical arrangements of trunks and switching machines in the CO. For correct trunking and switching configuration in the processing by TSS and TFS, this updating process, which includes maintaining office growth information and a "common-language" circuit identification of all circuits for individual switching machines, ensures that traffic data provided by TDAS will be correctly associated.

TSS (Trunk Servicing System)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%

TSS helps trunk administrators develop short-term plans and determine the number of circuits required in a trunk group. Data from TDAS is processed in TSS and the offered load for each trunk group is computed. Through offered load calculation on a per-trunk-group basis, TSS calculates the number of trunks theoretically required to handle that traffic load at a designated grade of service. TSS produces weekly reports showing which trunk groups have too many trunks and which have too few that are performing below the grade-of-service objective. Trunk orders to add or disconnect trunks are made by the CAC after they use the information provided through TSS.

TFS (Trunk Forecasting System)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

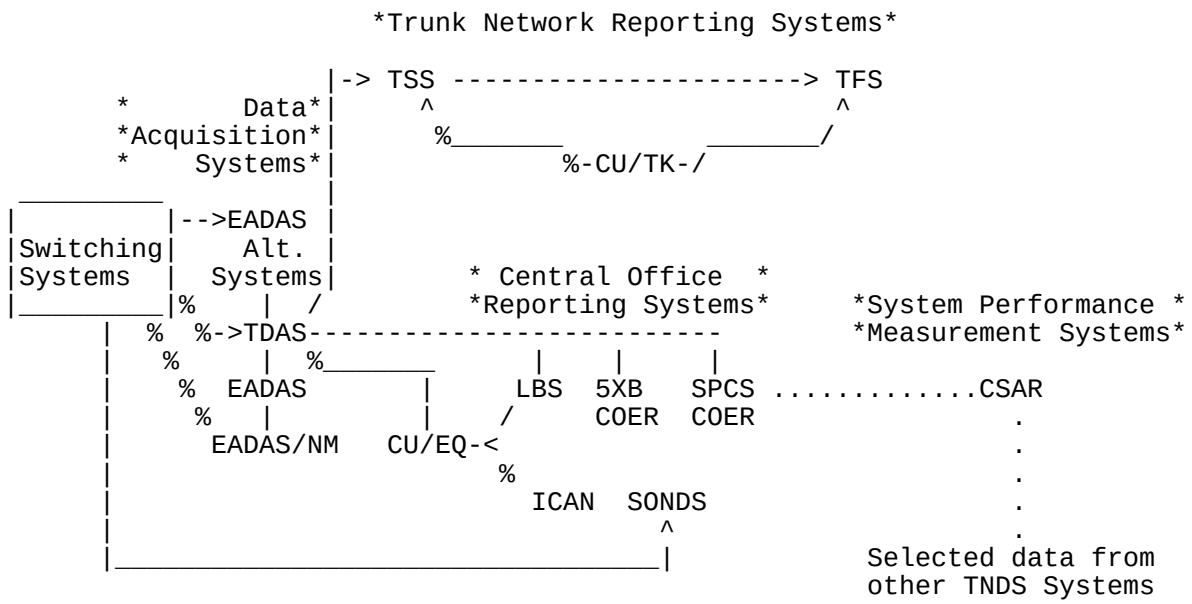
TFS uses traffic load data computed by TSS as well as information on the network configuration and forecasting parameters stored in the CU/TK database for long-term construction planning for new trunks. TFS forecasts message trunk requirements for the next five years as the fundamental input to the planning process that leads to the provisioning of additional facilities.

CSAR (Centralized System for Analysis and Reporting)
%%

CSAR is designed to monitor and measure how well data is being processed through TNDS. It collects and analyzes data from other TNDS systems and provides operating company personnel at NDCCs, NACs, and CACs with quantitative measures of the accuracy, timeliness, and completeness of the TNDS data flow as well as the consistency of the TNDS record bases. CSAR also presents enough information to locate and identify a data collection problem. CSAR summarizes the results of its TNDS monitoring for the company as input to the TPMP (TNDS Performance Measurement Plan) which is published monthly by AT&T. CSAR runs as a centralized on-line interactive system at an AT&T computer center. Its data is placed into special files, which, at the end of a CSAR run, are merged and transferred to the AT&T computer center. CSAR performs the proper associations and analyzes each system's results. These results are obtained by company managers via dial-up and they can be arranged in a number of formats that provide details on overall TNDS performance or individual system effectiveness. Specific problems can also be identified

through these reports.

The following is a diagram of data flow among TNDS systems:



SCCS (Switching Control Center System)
%%

The Switching Control Center (SCC) was created to centralize the administration, maintenance, and control of the 1ESS switching system. By using the remote-interaction interfacing of the MCC (Master Control Center), which is a frame of equipment in a 1ESS system that indicates the current state
of the office equipment, the SCC functions as the centralized maintenance center for the switch.

At the SCC, a minicomputer system called the CSS (Computer Sub-System)
is added and along with the equipment units that remote the MCC, it makes up the SCCS. The CSS can support a number of SCCs. Generally, the CSS is located
in the MMOC. Basically, a number of switches are handled by each SCC and the various SCCs are handled by the CSS.

The SCCS contains maintenance and administrative data that is sent directly from the switches. Through the SCCS, a technician can remotely operate
the MCC keys on the switches hooked up to it as well as perform any available command or task supported by the switch. The SCCS can handle up to 30 or more offices although usually only 15 or so are handled per SCC. This number depends also on the size of the offices and the amount of data that is transmitted.

Major alarms that sound at a switching office set off alarms at the SCC within seconds and it also causes an update of the status of the office on the critical indicator panel and it displays a specific description of the alarm condition on a CRT alarm monitor at a workstation. Software enhancements
to the SCCS fall into four broad classes:

- Enhanced Alarming - Besides alarms sounding, incoming data can generate failure descriptions for easy interpretation and

real-time analysis techniques.

- Interaction with Message History - Using past information on a switch's troubles, the SCCS allows pertinent information on a specific switch to be provided in case of an alarm.

- Mechanization of Craft Functions - Certain conditions no longer need to be looked into directly. If an alarm goes off, the SCCS can perform routine tests and fix the problem as best it can or else, if that doesn't work, a trouble ticket is issued.

- Support for Switch Administration - Through the SCCS, data can be sent automatically to different operations centers as well as other operations systems which require data from the switches.

Since the original SCCS came into operation, many changes have taken place. The current SCCS supports all of the entire ESS family of switches as well as network transmission equipment and it also can maintain several auxiliary processor systems, like TSPS (Traffic Service Position System) and AIS (Automatic Intercept System), and supports network transmission equipment.

COEES (Central Office Equipment Engineering System)

COEES is a time-sharing system that runs on a DEC PDP-10. It is the standard system for planning and engineering local switching equipment. COEES contains component systems for Step-By-Step, Crossbar, 1/1AESS, and 2/2BESS switching systems, each of which has a different capability.

The COEES database stores information obtained from forecasts for each local switching office on number of lines of all types, number of trunks of all types, average call rate per line and trunk, average usage per line and trunk, and all features, signaling types, etc. that are required. COEES determines the quantity of each type of equipment in the office needed to satisfy the forecasted load at objective service levels, determines an estimated price for engineering, procuring, and installing the equipment addition needed to reach the require level, and then it sums up the costs of doing it eight different ways for the network designer to review. The system also takes into account varying parameters like call rate or proportion of lines with certain features which is called sensitivity analysis.

With the information provided by the COEES forecast, the designer can then make a recommendation. After a decision is made on the recommendation, COEES prints out an order so that the additional equipment can more quickly and easily be obtained.

COEES also puts out a report called call store on a 1ESS, which tells the engineer and the equipment supplier how much memory to allocate to different functions in the switch depending on inputs that the engineer provides to the system.

MATFAP (Metropolitan Area Transmission Facility Analysis Program)

MATFAP is a computer program that aids in facility planning. It analyzes the alternatives available to the operating company for its future transmission equipment and facilities using present worth of future expenses and other measures.

By combining trunk and special-service circuit forecasts with switching plans, network configuration, cost data, and engineering rules, MATFAP can identify what transmission plant will be needed at various locations

and when it will be needed. It also determines economic consequences of specific facility and/or equipment selections as well as routing choices and it
provides the least-cost assignment of circuits to each facility as a guide to the circuit-provisioning process. It is oriented towards metropolitan networks
and facilities/equipment found in those regions.

MATFAP provides two benefits. It helps automate the transmission-planning process and it takes into account economies that cannot be identified by restricted analysis. It also balances circuit loads on high-capacity digital lines with additional multiplex equipment. Data from MATFAP is edited through RDES (Remote Data Entry System).

Various Operating Systems

The following is a list of other operating systems used by the Bell System with
brief descriptions:

ATRS (Automated Trouble Reporting System) - aids in the analysis of trouble reports by sorting, formatting, forwarding, and examining them from the entire country for standard errors

BOSS (Billing and Order Support System) - allows access to customer records, CN/A, bill adjustments, and information routing

CAROT (Centralized Automatic Reporting On Trunks) - operations system that tests a trunk on electromechanical and electronic switching systems and sends its findings to a remote computer terminal

CATLAS (Centralized Automatic Trouble Locating and Analysis System) - an operations system that automates trouble location procedures that identify faulty circuit packs in a switch when trouble is detected and diagnosed

CMDS (Centralized Message Data System) - analyzes the AMA tapes to determine traffic patterns

COSMOS (COmputer System for Mainframe OperationS) - stores the full inventory of telephone numbers

CRIS (Customer Records Information System) - contains the customer billing database

CRS (Centralized Results System) - a management information system that automates the collection, analysis, and publication of many measurement results

CUCRIT (Capital Utilization CRITeria) - used mainly for project economic evaluation and capital budgeting and planning

DACS (Digital Access Cross-connect System) - remote digital access for testing of special-service circuits in analog or digital form

EFRAP (Exchange Feeder Route Analysis Program) - used in planning of the loop network

IFRPS (Intercity Facility Relief Planning System) - also like MATFAP but deals with radio and coaxial cable as opposed to voice-frequency facilities

IPLAN (Integrated PLanning And Analysis system) - used mainly for project economic evaluation

LMOS (Loop Maintenance Operations System) - maintenance outages on loops remotely by a service employee

LRAP (Long Route Analysis Program) - like EFRAP, used in planning of the loop network

LSRP (Local Switching Replacement Planning system) - a system used in the planning of wire centers

NOTIS (Network Operations Trouble Information System) - aids in the analysis of trouble reports

NSCS (Network Service Center System) - at the NSC, aids in the analysis of trouble reports

OFNPS (Outstate Facility Network Planning System) - similar to MATFAP but
%%%%% contains a decision aid that identifies strategies for the introduction of digital facilities in a predominantly analog network; rural transmission facility network planning
RDES (Remote Data Entry System) - allows for remote editing of on-line
%%%% computer data
RMAS (Remote Memory Administration System) - changes translations in the
%%%% switching systems
SARTS (Switched Access Remote Test System) - accessed to perform sophisticated
%%%%% tests on most types of special-service circuits
SMAS (Switched Maintenance Access System) - through the use of relays,
%%%% provides concentrated metallic access to individual circuits to permit remote access and testing by SARTS
TASC (Telecommunications Alarm Surveillance and Control System) - an alarm
%%%% program that identifies the station and transmits it back to the central maintenance location
TCAS (T-Carrier Administration System) - an operations system responsible for
%%%% T-carrier alarms
TCSP (Tandem Cross Section Program) - a program for analysis of traffic
%%%% network planning
TFLAP (T-carrier Fault-Locating Application Program) - a subprogram of
%%%%% Universal Cable Circuit Analysis Program which analyzes networks with branches, multiple terminations and bridge taps

Acronym Glossary
%%%%%%%%%%%%%%%%

AIS	Automatic Intercept System
AMA	Automatic Message Accounting
ATRS	Automated Trouble Reporting System
BOSS	Billing and Order Support System
C1	Circuit system
CAC	Circuit Administration Center
CAROT	Centralized Automatic Reporting On Trunks
CATLAS	Centralized Automatic Trouble Locating and Analysis System
CMDS	Centralized Message Data System
CPC	Circuit Provision Center
CO	Central Office
COC	Circuit Order Control
COEES	Central Office Equipment Engineering System
COSMOS	COmputer System for Mainframe OperationS
CRIS	Customer Records Information System
CRS	Centralized Results System
CRT	Cathode-Ray Tube
CSAR	Centralized System for Analysis and Reporting
CSS	Computer SubSystem
CUCRIT	Capital Utilization CRITeria
CU/EQ	Common Update/EQuipment system
CU/TK	Common Update/TrunKing system
DACS	Digital Access and Cross-connect System
DPAC	Dedicated Plant Assignment Card
E1	Equipment system
EADAS	Engineering and Administrative Data Acquisition System
EADAS/NM	EADAS/Network Management
EFRAP	Exchange Feeder Route Analysis Program
ESS	Electronic Switching System
F1	Facility system
FEPS	Facility and Equipment Planning System
5XB COER	No. 5 Crossbar Central Office Equipment Report system
ICAN	Individual Circuit ANalysis
IFRPS	Intercity Facility Relief Planning System

IPLAN	Integrated PLanning and ANalysis
LAC	Loop Assignment Center
LBS	Load Balance System
LMOS	Loop Maintenance Operations System
LRAP	Long Route Analysis Program
LSRP	Local Switching Replacement Planning system
MATFAP	Metropolitan Area Transmission Facility Analysis Program
MCC	Master Control Center
MMC	Minicomputer Maintenance Center
MMOC	Minicomputer Maintenance Operations Center
NAC	Network Administration Center
NDCC	Network Data Collection Center
NMC	Network Management Center
NOC	Network Operations Center
NOCS	Network Operations Center System
NORGEN	Network Operations Report GENerator
NOTIS	Network Operations Trouble Information System
NSCS	Network Service Center System
OFNPS	Outstate Facility Network Planning System
PIA	Plug-In Administrator
PICS	Plug-in Inventory Control System
PICS/DCPR	PICS/Detailed Continuing Property Records
PREMIS	PREMises Information System
PSTN	Public Switched Telephone Network
RDES	Remote Data Entry System
RMAS	Remote Memory Administration Center
SARTS	Switched Access Remote Test System
SCC	Switching Control Center
SCCS	Switching Control Center System
SMAS	Switched Maintenance Access System
SONDS	Small Office Network Data System
SPCS COER	Stored-Program Control System/Central Office Equipment Report
TASC	Telecommunications Alarm Surveillance and Control system
TCAS	T-Carrier Administration System
TCSP	Tandem Cross Section Program
TDAS	Traffic Data Administration System
TFLAP	T-Carrier Fault-Locating Applications Program
TFS	Trunk Forecasting System
TIRKS	Trunks Integrated Records Keeping System
TNDS	Total Network Data System
TPMP	TNDS Performance Measurement Plan
TSPS	Traffic Service Position System
TSS	Trunk Servicing System
WC	Wire Center

Recommended reference:

Bell System Technical Journals

Engineering and Operations in the Bell System

Phrack IX LMOS file by Phantom Phreaker

Phrack XII TNDS file by Doom Prophet

Various COSMOS files by LOD/H, KOTRT, etc.

Completed 3/17/89

==Phrack Inc.==

Volume Three, Issue 26, File 3 of 11

=-
=
-
-
= %> The Disk Jockey <%
=
-
-
= Presents
=
-
-
= Getting Caught
=
- - Legal Procedures -
-
=
=
- March 24, 1989
-
=
=
- An Unbiased Look Into The Ways Of Criminal Proceedings
-
=
=
-=-
=-

Preface
%%%%%%%

Through this file, I hope to explain what legal action is followed during an investigation of toll fraud. All of the contained information is based upon
actual factual information, and although it differs slightly from state to state, the majority of it is applicable anywhere. There seems to be a lot of misconception as to the actual legal happenings during and after an investigation, so hopefully this will answer some of the too often unasked questions.

Initiation
%%%%%%%%%%

In our particular story, the whole investigation is tipped off from a phone call by someone to the U.S. Sprint security office. The volume of calls of "hackers" calling in on other "hackers" is incredible. It is amazing how when one user is mad at another and seeks some "revenge" of sorts, he calls a security office and advises them that they know of a person who is illegally using said company's long distance services. Usually the person will talk to either a regular customer service representative, or someone from the security office. Typically they will merely say "Hey, a guy named 'Joe' is using your codes that he hacks, and his home phone number is 312-xxx-xxxx."

Next our security person has to decide if this may indeed be a somewhat legitimate call. If all seems fairly reasonable, they will start their own in-house investigation. This could mean just doing a CN/A on the phone number in question to see who the phone is registered under, and check to see if this person is a legitimate subscriber to their system.

A call is placed to the person in question's home telco office. Usually they will talk to someone in the security office, or a person whom would carry such a capacity in the area of security. They will usually coordinate an effort to put some type of DNR (Dialed Number Recorder) on the subscriber's telephone line, which will record on an adding machine type of paper all data pertaining to: Numbers dialed, DTMF or pulse modes, any occurrence of 2600hz, codes and other digits dialed, incoming calls including number of rings before answer, time the line was picked up and hung up, etc.

This DNR may sit on the subscriber's phone line from merely a few weeks, to several months.

At some point either the U.S. Sprint security representative or the telco security person will decide that enough time has passed, and that an analysis of the DNR tape is due. The Sprint official may visit the telco site and go over the tapes in person, or they may be sent from the telco to the Sprint office.

After going over the tapes and finding dialups and codes that were used that may possibly be used illegally, Sprint will find the actual owners of the codes in question and verify that the codes were indeed used without any knowledge or permission of the legitimate owner. They will also put together an estimate of "damages," which can include cost of dialup port access, cost of investigation, as well as the actual toll charges incurred from the usage.

The Sprint security representative and the local telco security person will then go to the local police, usually either state or whatever has the real
power in that area. They will present the case to the detective or other investigator, display all findings, and provided that the case findings seem pretty plausible, a search warrant will be composed. After the warrant is fully written out (sometimes it is merely a short fill-in-the-blank form) the three people investigating the case (the police detective, the local telco security representative, and the Sprint security investigator) will go in front
of a judge and under oath state the evidence and findings that they have as to date contained in a document called a "discovery" which justify the need for a search warrant. Assuming that the findings seem conclusive, the judge will sign the warrant and it will then be active for the time specified on the warrant. Usually they are valid for 24 hours a day, due to the circumstances that more than likely calls were being made at all hours of the day and night.

On some agreed date, all the above parties will show up at the suspect's house and execute the search warrant and more than likely collect all the phone
and computer equipment and bring it to the state police post for further investigation.

All information and evidence as well as all the reports will then be forwarded to the prosecutor's office to determine what, if any, charges are going to be pursued.

Once charges are finalized through the prosecutor, another discovery document is made, listing all the charges and how those charges were derived. It is then brought in front of the judge again and if approved, warrants will be issued for the individual(s) listed.

The warrants are usually served by sending over one of the local officers to the suspect's house, and he will knock, introduce himself and ask for the individual, and then present the warrant to the individual and take them in to the station.

The individual will be processed, which usually means being photographed and fingerprinted twice (once for the FBI and once for the state records), and then is put into either a holding cell or regular jail.

Sometimes the bond is already set before the individual is arrested, but sometimes it is not. If not, it will be at the arraignment.

Within 72 hours, the suspect must be arraigned. The arraignment is a time

when the formal charges are read to the suspect in front of the judge, bail is set if it has not been already, and the suspect may pick if he wants a jury trial or a trial by judge. This, of course, assumes that the suspect is going to plead not guilty, which is the best thing to do in most cases of somewhat major capacity. Further court dates are also set at this time. If the suspect
is unable to afford to retain an attorney, the court will assign a court appointed lawyer at this time.

After the arraignment, the suspect is either allowed to post bail, or is returned to the jail to await the next court date. His next court date, which is the omnibus, is usually slated for about a month away.

If the set bail seems unreasonably high, your attorney can file for a "bond reduction." You will go in front of the judge and your lawyer will argue
as to why your bond should be reduced, and how you have a stable life and responsibilities and would not try to skip bail. The prosecutor will argue as to why your bail should not be dropped.

At the omnibus hearing, also known as a "fact-finding" hearing (or in some
states, this is known as the "preliminary hearing."--Ed.) the suspect is again brought in front of a judge, along with his own attorney, and the prosecuting attorney. At this time the state (meaning the prosecutor) will reveal evidence
against the suspect, and the judge will decide if the evidence is enough to hold the suspect in jail or to continue the case to trial. Nearly always there
is enough, as warrants would not be issued if there was not, since the state could be opening themselves up to a false arrest suit if they were wrong. From
here a "pre-trial" date is slated, again usually about a month down the road.

The pre-trial is the last chance for the suspect to change his mind and enter a guilty plea, or to continue to trial. It is also the last point in which the prosecutor will offer the suspect any type of plea-bargain, meaning that the suspect enters a guilty plea in exchange for an agreed upon set of reduced charges or sentencing. Assuming the suspect still wishes to enter a plea of "not-guilty," the date for jury selection will be slated.

During the jury selection, your lawyer and you as well as the prosecutor will get to meet as many prospective jury members as you wish, and you can each
ask them questions and either accept or reject them based on if you think that they would be fair towards you. This eliminates most possibilities of any jury
members that are biases before they every sit down to hear your case. After the prosecutor and your attorney agree on the members, your trial date is set, usually about a week later.

At trial, the prosecutor will present the case to the jury, starting with questioning detectives and investigators on how the case was first discovered and how things lead to you, and in each instance, your attorney will be able to
"cross-examine" each witness and ask questions of their own, hopefully making the jury questionable as to the validity of everything that is said. After that, your attorney is allowed to call witnesses and the prosecutor will be allowed to ask questions as well. By rights you do not have to go to the stand
if you do not want to, as you have the right to not incriminate yourself. After
all is said and done, the prosecutor will get to state his "closing arguments,"
a basic summary of all that was presented and why you should be considered guilty, and your lawyer will give his arguments to the jury, as to why you should not be judged guilty.

The jury will go into deliberation, which can last a few minutes, or several days. They must all vote and decide if you should be judged guilty or not guilty. After the deliberation, court is called back in and the jury will announce the results.

If it is decided that you are guilty, you normally have about 10 days to file an appeal, which would have your case sent to a higher court. Otherwise your date for sentencing will be set, again usually about a month away.

At the sentencing, your lawyer will argue why you should be let off easy, and the prosecutor will argue why you should be given a hard sentence. The judge will come to a decision based on the arguments and then make a decision on your sentence. You will then be released to the agency that you are assigned to, be it the probation department, the prison system, or the county jail.

I hope this file gives you a more clear view on what happens in the legal system, in future files I hope to discuss the actual dos and don'ts of the legal system and advise as to what tricks of the trade are used by legal authorities.

Any questions/comments/threats can be directed to me at;

Lunatic Labs 415.278.7421

-The Disk Jockey

==Phrack Inc.==

Volume Three, Issue 26, File 4 of 11

The Future Transcendent Saga continues...

NSFnet

National Science Foundation Network

brought to you by

Knight Lightning

April 16, 1989

NSF Network Links Scientific Community And SuperComputer Centers

When the National Science Foundation (NSF) established its national supercomputer centers in 1985, it also planned to create a communications network that would give remote locations access to these state-of-the-art facilities. NSF planners envisioned a system they dubbed "NSFNET." Based on a
"backbone" connecting the supercomputer centers, NSFNET would combine existing networks and newly created ones into an InterNet, or network of networks, to serve the centers and their users. In addition to gaining access to the centers' computing technology, researchers at geographically dispersed locations would be part of a nationwide research network across which they could exchange scientific information. Although the primary role of NSFNET remains access to NSF-funded supercomputers and other unique scientific resources, its use as a general-purpose network, which enables scientists to share research findings, is becoming increasingly important.

NSFnet Components

%%%%%%%%%%%%%%%%%

NSFNET is organized as a three-level hierarchy: The backbone; autonomously administered wide-area networks serving communities of researchers; and campus networks. The backbone has been in use since July 1986 and is fully operational. It provides redundant paths among NSF supercomputer centers. While several wide-area networks are already connected to the NSFNET backbone, more are being built with partial funding from NSF and will be connected as they are completed (see the section on NSFnet Component Networks).

SuperComputer Centers

%%%%%%%%%%%%%%%%%%%%%

NSF created the supercomputer centers in response to a growing concern that a lack of access to sophisticated computing facilities had severely constrained academic research. A project solicitation in June 1984 resulted in the creation of the following centers -- the John Von Neumann National Supercomputer Center in Princeton, New Jersey, the San Diego Supercomputer Center on the campus of the University of California at San Diego, the National
Center for Supercomputing Applications at the University of Illinois, the Cornell National Supercomputer Facility at Cornell University, and the Pittsburgh Supercomputing Center under joint operation by Westinghouse Electric

Corporation, Carnegie-Mellon University, and the University of Pittsburgh. All the centers are multi-disciplinary and are available to any researcher who is eligible for NSF support. They offer access to computers made by Cray Research, Inc., Control Data Corporation, ETA, and IBM. The Scientific Computing Division of the National Center for Atmospheric Research is the sixth center which is part of NSFNET. The SCD has been providing advanced computing services to the atmospheric sciences community since the late 1960s.

Protocols

NSFNET is using the TCP/IP protocols of the DARPA InterNet as the initial standard. The system will work toward adopting international standards as they become established. The protocols link networks that are based on different technologies and connection protocols, and provide a unified set of transport and application protocols. As the NSFNET system continues to evolve, the typical user working at a terminal or work station will be able to connect to and use various computer resources -- including the supercomputer centers -- to run interactive and batch jobs, receive output, transfer files, and communicate with colleagues throughout the nation via electronic mail. Most researchers will have either a terminal linked to a local super-minicomputer or a graphics work station. These will be connected to a local area network that is connected to a campus network, and, via a gateway system, to a wide-area network.

Management

Four institutions are sharing the interim management of NSFNET: The University of Illinois (overall project management and network engineering), Cornell University (network operations and initial technical support), the University of Southern California Information Sciences Institute (protocol enhancement and high-level technical support), and the University Corporation for Atmospheric Research (management of the NSF Network Service Center through a contract with BBN Laboratories, Inc.).

NSF Network Service Center

The NSF Network Service Center (NNSC) is providing general information about NSFNET, including the status of NSF-supported component networks and supercomputer centers. The NNSC, located at BBN Laboratories Inc. in Cambridge, MA, is an NSF-sponsored project of the University Corporation for Atmospheric Research.

The NNSC, which currently has information and documents on line and in printed form, plans to distribute news through network mailing lists, bulletins, newsletters, and on-line reports. The NNSC also maintains a database of contact points and sources of additional information about the NSFNET component networks and supercomputer centers.

When prospective or current users do not know whom to call concerning their questions about NSFNET use, they should contact the NNSC. The NNSC will answer

general questions, and, for detailed information relating to specific components of NSFNET, will help users find the appropriate contact for further assistance.

In addition the NNSC will encourage the development and identification of local campus network technical support to better serve NSFNET users in the future.

Connecting To NSFnet

NSFNET is part of a collection of interconnected IP-networks referred to as the InterNet. IP, the Internet Protocol, is a network protocol which allows heterogeneous networks to combine into a single virtual network. TCP, the Transmission Control Protocol, is a transport protocol which implements the packet loss and error-detection mechanisms required to maintain a reliable connection between two points on the network. TCP/IP therefore offers reliable delivery of data between heterogeneous computers on diverse networks. An example of an application which uses TCP/IP is TELNET, which provides virtual terminal service across the network.

Only IP-based networks can connect to the Internet; therefore, an organization that plans to use NSFnet either must have an existing IP network or have access to one. Many large universities and technical firms have links to the InterNet in place. The computer science department of a university or the engineering support division of a company are most likely to have IP connectivity or to have information on the local connections that exist. Prospective users can ask the NNSC to determine whether an organization is already connected to the Internet.

If an organization does not have an IP link, it can obtain one in several ways:

- NSF has a program that funds the connecting of organizations to the NSF regional/state/community networks that are part of NSFNET. The NNSC has more information on this program.
- The Computer Science Network, CSNET, provides gateway service to several IP-networks, including NSFNET. To get CSNET service, an organization must become a CSNET member.
- Users may be able to get access to NSFNET through time-share accounts on machines at other organizations, such as local universities or companies.

Some supercomputer centers support access systems other than NSFNET, such as Bitnet, commercial X.25 networks, and dial-up lines, which do not use IP-based protocols. The Supercomputer Centers' user services organizations can provide more information on these alternatives (see list).

NSF COMPONENT NETWORKS

STATE AND REGIONAL NETWORKS

BARRNET (California's Bay Area Regional Research Network)
MERIT (Michigan Educational Research Network)

MIDNET (Midwest Network)
NORTHWESTNET (Northwestern states)
NYSERNET (New York State Educational and Research Network)
SESQUINET (the Texas Sesquicentennial Network)
SURANET (the Southeastern Universities Research Association Network)
WESTNET (Southwestern states)

CONSORTIUM NETWORKS

JVNCNET connects the John Von Neumann National Supercomputer Center at Princeton, NJ, with a number of universities.
PSCAANET is the network of the Pittsburgh Supercomputing Center Academic Affiliates group.
SDSCNET is centered at the San Diego Supercomputer Center.

==Phrack Inc.==

Volume Three, Issue 26, File 5 of 11

COSMOS

COmputer System for Mainframe OperationS

Part One

by King Arthur

Introduction

Throughout the last decade, computers have played an ever growing role in information storage and retrieval. In most companies, computerized databases have replaced a majority of all paper records. Where in the past it would take 10 minutes for someone to search through stacks of paper for some data, the same information can now be retrieved from a computer in a fraction of a second.

Previously, proprietary information could be considered "safe" in a file cabinet; the only way to see the data would be to have physical access to the files. Now, somebody with a computer terminal and a modem can make a quick phone call and access private records. It's unfortunate that there are "hackers" who try to gain unauthorized access to computers. Yet, it is just as unfortunate that most reported computer break-ins could have been prevented if more thought and common sense went into protecting computers.

Hackers

There have been many cases of computer crime reported by the Bell Operating Companies (BOCs), but it is hard to say how many actual break-ins there are. Keep in mind that the only reported cases are those which are detected. In an interview with an anonymous hacker, I was told of one of the break-ins that may not have ever been reported. "My friend got the number when he misdialed his business office -- that's how we knew that it was the phone company's. It seems this Unix was part of some real big Bellcore computer network," says the hacker.

The hacker explains that this system was one of many systems used by the various BOCs to allow large Centrex customers to rearrange their Centrex groups. It seems he found a text file on the system with telephone numbers and passwords for some of Bellcore's development systems. "On this Bellcore system in Jersey, called CCRS, we found a list of 20 some-odd COSMOS systems.... Numbers, passwords, and wire centers from all over the country!" He adds, "Five states to be exact."

The hacker was able to gain access to the original Unix system because, as he says, "Those guys left all the default passwords working." He was able to login with a user name of "games" with the password being "games." "Once we were on we found that a large number of accounts didn't have passwords. Mary, John, test, banana, and system were some, to name a few." From there he was

able to eventually access several COSMOS database systems -- with access to ALL
system files and resources.

COSMOS

%%%%%

COSMOS, an acronym for the COmputer System for Mainframe OperationS, is a database package currently supported by Bellcore. COSMOS is presently being used by every BOC, as well as by Cincinnati Bell and Rochester Telephone. COSMOS replaces paper record-keeping and other mechanized record systems for plant administration. COSMOS' original purpose was to alleviate congestion in the Main Distributing Frame (MDF) by maintaining the shortest jumpers.

It can now maintain load balance in a switch and assign office equipment, tie pairs, bridge lifters and the like. Additional applications allow COSMOS to aid in "cutting-over" a new switch, or even generate recent change messages to be input into electronic switches. COSMOS is most often used for provisioning new service and maintaining existing service, by the following departments: The frame room (MDF), the Loop Assignment Center (LAC), the Recent Change Memory Assistance Center (RCMAC), the network administration center, and the repair service.

Next year COSMOS will celebrate its 15th birthday, which is quite an accomplishment for a computer program. The first version or "generic" of COSMOS was released by Bell Laboratories in 1974. In March 1974, New Jersey Bell was the first company to run COSMOS, in Passaic, New Jersey. Pacific Telesis, NYNEX, Southern Bell, and many of the other BOCs adopted COSMOS soon after. Whereas Southwestern Bell waited until 1977, the Passaic, NJ Wire Center is still running COSMOS today.

Originally COSMOS ran on the DEC PDP 11/45 minicomputer. The package was written in Fortran, and ran the COSNIX operating system. Later it was adapted to run on the DEC PDP 11/70, a larger machine. Beverly Cruse, member of Technical Staff, COSMOS system design at Bellcore, says, "COSNIX is a derivation of Unix 1.0, it started out from the original Unix, but it was adapted for use on the COSMOS project. It bears many similarities to Unix, but
more to the early versions of Unix than the current... The COSMOS application now runs on other hardware understandard Unix."

"The newest version of COSMOS runs on the standard Unix System V operating
system. We will certify it for use on particular processors, based on the needs of our clients," says Ed Pinnes, the District Manager of COSMOS system design at Bellcore. This Unix version of COSMOS was written in C language. Currently, COSMOS is available for use on the AT&T 3B20 supermini computer, running under the Unix System V operating system. "There are over 700 COSMOS systems total, of which a vast majority are DEC PDP 11/70's. The number fluctuates all the time, as companies are starting to replace 11/70's with the other machines," says Cruse.

In 1981 Bell Laboratories introduced an integrated systems package for telephone companies called the Facility Assignment Control System (FACS). FACS
is a network of systems that exchanges information on a regular basis. These are: COSMOS, Loop Facilities Assignment and Control System (LFACS), Service Order Analysis and Control (SOAC), and Work Manager (WM). A service order from
the business office is input in to SOAC. SOAC analyzes the order and then sends an assignment request, via the WM, to LFACS. WM acts as a packet switch,

sending messages between the other components of FACS. LFACS assigns distribution plant facilities (cables, terminals, etc.) and sends the order back to SOAC. After SOAC receives the information form LFACS, it sends an assignment request to COSMOS. COSMOS responds with data for assigning central office equipment: Switching equipment, transmission equipment, bridge lifters,
and the like. SOAC takes all the information from LFACS and COSMOS and appends
it to the service order, and sends the service order on its way.

Computer Security

Telephone companies seem to take the brunt of unauthorized access attempts. The sheer number of employees and size of most telephone companies makes it very difficult to keep tabs on everyone and everything. While researching computer security, it has become evident that COSMOS is a large target for hackers. "The number of COSMOS systems around, with dial-ups on most of the machines... makes for a lot of possible break-ins," says Cruse. This is why it's all the more important for companies to learn how to protect themselves.

"COSMOS is power, the whole thing is a big power trip, man. It's like Big Brother -- you see the number of some dude you don't like in the computer. You
make a service order to disconnect it; COSMOS is too stupid to tell you from a real telco dude," says one hacker. "I think they get what they deserve: There's a serious dearth of security out there. If kids like us can get access
this easily, think about the real enemy -- the Russians," jokes another.

A majority of unauthorized access attempts can be traced back to an oversight on the part of the system operators; and just as many are the fault of the systems' users. If you can keep one step ahead of the hackers, recognize these problems now, and keep an eye out for similar weaknesses, you can save your company a lot of trouble.

A hacker says, "In California, a friend of mine used to be able to find passwords in the garbage. The computer was supposed to print some garbled characters on top of the password. Instead the password would print out AFTER the garbled characters." Some COSMOS users have half duplex printing terminals. At the password prompt COSMOS is supposed to print a series of characters and then send backspaces. Then the user would enter his or her password. When the password is printed on top of the other characters, you can't see what it is. If the password is being printed after the other characters, then the printing terminal is not receiving the back space characters properly.

Another big problem is lack of password security. As mentioned before, regarding CCRS, many accounts on some systems will lack passwords. "On COSMOS there are these standardized account names. It makes it easier for system operators to keep track of who's using the system. For instance: all accounts that belong to the frame room will have an MF in them. Like MF01, you can tell
it belongs to the frame room. (MF stands for Main Frame.) Most of these names
seem to be common to most COSMOS systems everywhere. In one city, none of these user accounts have passwords. All you need is the name of the account and you're in. In another city, which will remain unnamed, the passwords are the SAME AS THE DAMN NAMES! Like, MF01 has a password of MF01. These guys must not be very serious about security."

One of the biggest and in my eyes one of the scariest problems around is what hackers refer to as "social engineering". Social engineering is basically the act of impersonating somebody else for the sake of gaining proprietary information. "I know this guy. He can trick anybody, does the best BS job I've ever seen. He'll call up a telco office, like the repair service bureau, that uses COSMOS. We found that most clerks at the repair service aren't too sharp." The hacker said the conversation would usually take the following course:

Hacker: Hi, this is Frank, from the COSMOS computer center. We've had a problem with our records, and I'm wondering if you could help me?

Telco: Oh, what seems to be the problem?

H: We seem to have lost some user data. Hopefully, if I can correct the problem, you people won't lose any access time today. Could you tell me what your system login name is?

T: Well, the one I use is RS01.

H: Hmm, this could present a problem. Can you tell me what password and wire center you use that with?

T: Well, I just type s-u-c-k-e-r for my password, and my wire centers are: TK, KL, GL, and PK.

H: Do you call into the system, or do you only have direct connect terminals?

T: Well, when I turn on my machine I get a direct hook up. It just tells me to login. But I know in the back they have to dial something. Hold on, let me check. (3 Minutes later...) Well, she says all she does is call 555-1212.

H: OK, I think I have everything taken care of. Thanks, have a nice day.

T: Good, so I'm not gonna have any problems?

H: No, but if you do just give the computer center a call, and we'll take care of it.

T: Oh, thank you honey. Have a nice day now.

"It doesn't work all the time, but we get away with it a good part of the time. I guess they just don't expect a call from someone who isn't really part of their company," says the hacker. "I once social engineered the COSMOS control center. They gave me dial-ups for several systems, and even gave me one password. I told them I was calling from the RCMAC and I was having trouble logging into COSMOS," says another.

This last problem illustrates a perfect example of what I mean when I say these problems can be prevented if more care and common sense went into computer security. "Sometimes, if we want to get in to COSMOS, but we don't have the password, we call a COSMOS dial-up at about 5 o'clock. To logoff of COSMOS you have to hit a CONTROL-Y. If you don't, the next person who calls will resume where you left off. A lot of the time, people forget to logoff. They just turn their terminals off, in the rush of going home."

The past examples do not comprise the only way hackers get into systems, but most of the problems shown here can exist regardless of what types of systems your company has. The second article deals with solutions to these problems.

==Phrack Inc.==

Volume Three, Issue 26, File 6 of 11

+-=-+

Basic Concepts of Translation

Brought to you by

The Dead Lord
and
The Chief Executive Officers

February 17, 1989

+-=-+

This tutorial is meant for the hardcore hackers who have entered the world of ESS switches. The information here is useful and valuable, although not invaluable. You can easily reap the benefits of access to a switch even if you
only know RC:LINE, but to really learn the system in and out, the concepts about translation are ones that need to be mastered.

In electromechanical switches, switching was directly controlled by whatever the customer dialed. If a 5 were dialed, the selector moved across 5 positions, and so on. There were no digit storing devices like registers and senders. As the network grew larger, this became inefficient and switching systems using digit storage and decoding devices were put into use. In this type of setup, the customer dials a number, which is stored in a register, or sender. The sender then uses a decoder and gives the contents of the register as input. The decoder translates the input into a format that can be used to complete the call, and sends this translation back to the digit storage device.
This is a simplified example of translation, since the only input was dialed digits and the only output was routable information, but it shows what translation is: The changing of information from one form to another.

When 1 ESS was first tested in Morris, Illinois in 1960, it introduced a switching method called Stored Program Control. Instead of switching and logic
functions being handled by hardware, it was done through computer programs. This greatly expanded the translation function. Because calls are handled by many programs, information must be provided for each program. For example, when a customer picks up a phone, the switch needs to know if outgoing service is being denied, if the line is being observed, line class, special equipment features, etc. The line equipment number is given to the translation program as input. The translator translates the LEN and produces the answers to these and other pertinent questions in a coded form that can be used by the central processor of the switch.

If the call is an interoffice call, the first three dialed digits are given to a translator as input and they translate into a route index and, possibly, other information. The route index, in turn, is given as input to another translator, which translates into: Which trunk to use (trunk identity), transmitter identity, the alternate route, etc. So actually, in early systems,
translation was a single shot thing, and in Stored Program Control Systems (SPCS), the translation function is used many many times.

In the 1 ESS, translation data is stored on magnetic memory cards in the program store. However, since translation data is constantly being changed, there is a provision made to store the changes in an area of the call store memory. The area of call store is called the recent change (RC) area. The changes are eventually transcribed from the call store into the program store by a memory card writer.

In the 1A ESS, translation data is stored in the unduplicated call store, with backup in the form of disk memory called file store. Additionally, magnetic tapes are made of the translation area of call store. When a change in translation is made, the change is entered in a duplicated copy of call store. After checks are made as to the validity of the change (format and everything),
the change is then placed in the unduplicated copy of call store. After that, the change is also written to a set of disk files in file store. Before the new data is written, the old data is written to a part of the disk file called "rollback."

DATA	1 ESS	1A ESS
Transient Information	Duplicated Call Store	Duplicated Call Store
Generic Program	Duplicated Program Store	Program Store
Parameter Table	Duplicated Program Store	Unduplicated Call Store
Translation Information	Duplicated Call Store + Program Store	Unduplicated Call Store

Transient Information: Telephone calls or data messages in progress; present
state of all lines, junctors, and trunks in the office.

Generic Program: The operating intelligence of the system. It controls actions like line and trunk scanning, setting up and taking down connections, etc.

Parameter Table: Informs the generic program of the size and makeup of
the office. This information includes equipment items (frames and units), call store allocation (call
registers, hoppers, queues, etc.) and office options (days AMA tapes will be switched, etc.).

Translation Information: Day to day changeable info which is accessed by translator programs. Also includes form tables, lists called "translators" which are linked in an hierarchical pattern.

This is a quote from Engineering and Operations in the Bell System, pages 415-416:

> "The 1 ESS includes a fully duplicated No. 1 Central Processor Unit (Central Control includes the generic program), program store bus, call store bus, program stores, and call stores. The 1 ESS uses permanent magnet twister program store modules as basic memory elements. These provide a memory that is fundamentally read only, and have a cycle time of 5.5 microseconds. The call store provides "scratch pad," or temporary duplicated memory.
>
> As with the 1 ESS, the 1A CPU has a CPU, prog store bus, and call store bus that are fully duplicated. However, the 1A processor uses readable and writable memory for both prog and call stores, and has a cycle time of 700 nanoseconds. However, the program stores aren't fully duplicated, but 2 spare stores are provided for reliability. A portion of the call store is duplicated, but only one copy of certain fault recognition programs, parameter information, and translation data is provided. An extra copy of the unduplicated prog and call store is provided for in file store."

The program store translation area in the 1 ESS and the unduplicated call store
translation area in the 1A ESS contain all the info that can change from day to
day for that office. Here is a list of things that are stored in the translation area:

+ Line Equipment Number (LEN), Directory Number (DN), trunk assignments (all explained later).
+ Office codes.
+ Rate and route information.
+ Traffic measurement information.
+ Associated miscellaneous info for call processing and charging.

Call store can be thought of as RAM; it is filled as long as the ESS is powered.

Program store is like ROM; it is physically written onto magnetic cards. File store is simply information stored on magnetic tapes (or disk drives). All data that's changeable (rate and route, customers' features, trunk selection, alternate paths, etc.) is called translation data and is stored in the translation area.

Changes in translation are called recent changes and are stored in an area called the recent change area.

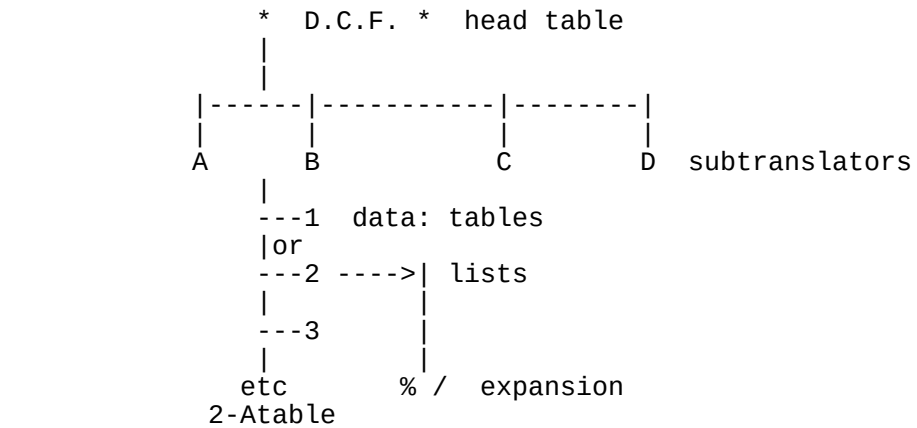
Once again, I stress that this article is sort of a "masters" file for hackers who are interested in ESS. If the concepts are too difficult, don't panic. Knowledge comes with time. Don't feel bad if you don't catch on right away.

Translation data is stored in the form of tables or lists. Each table is linked in a hierarchical pattern. Tables high in the hierarchy contain pointers (addresses) to the lower tables. Tables low in the hierarchy contain the actual data.

Most translators are broken down into subtranslators, which are linked by a Head Table, or "HT". The HT points to the different ST's stored in memory, in the same way that a table of contents in a book points to the pages of each chapter. This way, when a new feature is added, it's just a matter of adding a new entry in the HT, and having the entry point to a newly stored ST.

Translation input is divided into 2 parts: the selector and the index. The selector determines which ST to access, and the index determines which item (word number) in that particular ST to access. In some cases, the translation

information may not fit into the space allotted to an ST, so pointers to auxiliary blocks and/or expansion tables may have to be given. You can think of a BASIC program, where a GOSUB points to a subroutine at location 4000. Now, if the subroutine is 100 bytes long, but you only have room for 75, another GOSUB must be issued to point to the rest of the subroutine. So a full
translator is quite a large unit -- it can have a head table, subtranslators, auxiliary blocks, abbreviated codes, lists, subauxiliary blocks and expansion tables. The example below shows a custom calling feature that exists on 5 ESS:
Dog Control Frequency, "DCF". In the e below diagram, DCF represents the Head Table, and has a list of pointers that identify the location of subtranslators "A" through "D". The data field "2" in subtranslator "D" is too small to store
the entire subroutine, so an expansion table "2A" was produced to house the entire program.



ESS programs access translators by locating their octal address in the Master Head Table, which is also called the Base Translator.

1 ESS MHT
%%%%%%%%%
The 1 ESS has 2 copies of the MHT: One in program store, and one in call store. The copy in call store is the one that's used normally, since call store memory has a faster cycle time. The one in program store is there for backup. The MHT is 338 bytes long (23 bit bytes), and as we mentioned, is used
as a sort of directory for locating translators. The MHT can point to starting
addresses of Head Tables (which point to translators), or to tables and lists. Head Tables point to subtranslators. Subtranslators can point to auxiliary and
expansion blocks, lists, or tables.

There is another Master Head Table called the Auxiliary Master Head Table, which points to other translators. There are 2 copies of the AMHT, one in program and one in call store. The AMHT is found by accessing the MHT, and for
those interested, the address of the AMHT is located in the 28th byte of the MHT. The MHT is fixed; meaning that the first byte will ALWAYS be the address of the DN translator. The last byte will ALWAYS be the address to the JNNL to JNNT/JCN Head Table (explained later). ESS needs a table to read this table. Otherwise, how would it know what byte leads where? There is a "T-reading octal program" located at (octal address) 1105615 in the parameter area in the program store.This address is stored in the generic program and is used to read

the Master Head Table.

1A ESS

A 1A ESS switch call store byte contains 26 bits, named 0 through 25, which is a lot more than I can say about an Apple... Bits 24 and 25 are used for parity, and are not used for data. This leads to what is known as a K-code. No, a K-code is not used by lowly software K-rad pirates, but it is used by us ESS hackers. Each call store K-code contains 65,536 bytes, and can be thought of as a "page" of memory.

Anyway, translation data is stored in the unduplicated call store. Remember, we're still talking about 1A ESS. In generic 1AE6 and earlier, unduplicated call store starts at K-code 17, and as more translation data is fed into the system, it pushes down into K-code 16, 15, 14, etc. In generic 7 and above, call store has been increased by a great deal, because of a huge memory expansion unit. On the early generics, the entire call store and program store had to fit in 38 K-codes. In the later generics, there are 38 K-codes assigned to call store (that's split between duplicated and unduplicated), and another 38 K-codes for program store.

Not all K-codes may be used, so it's not really a full 38 K-codes, but hey, you can't have all your memory and use it too. Anyhow, because generics 1A E7 and higher have such huge call store memories, it's convenient to divide call store into 3 parts: The "duplicated call store" (DCS), which is located at the very top of the memory map, the "low unduplicated call store," (LUCS), which is located in the middle of call store, and the "high unduplicated call store," (HUCS). The LUCS area starts at K-code 17 and goes down as it fills up (being very watchful about not going into the DCS area. The HUCS area starts at K-code 37 and goes down as it fills up to K-code 20, being mindful not to step on LUCS's toes. Translators are classified as being either HUCS or LUCS translators, (but not both).

LUCS translators aren't fixed; they can exist anywhere in the area as long as they're identified by the MHT. HUCS translators can either be fixed or not fixed. Note that in generics 1AE6 and earlier, there is no such distinction, because there's not enough memory to make such a distinction feasible. As for the location of the MHT, in generic 1AE6 and earlier, it's located in K-code 17 at octal address 3724000, and is 1376 bytes long. The later MHT's were moved to K-code 37 at octal address 7720000, and is 3424 bytes long.

Translator Types

As I said, translators take data as input and change it into another form for output. All translators exist in the form of hierarchical lists and tables. They reside in call store on 1A's and program store on 1's. The higher data in a translator points to the location of the lower data. The lower data contains the actual information. The different translators are located by the Master Head Table, which contains pointers to all the translators in the system. The kind of data that needs to be translated is changeable data.

For example:

o line equipment number
o directory number
o 3/6 digit codes
o trunk network number to trunk group number
o trunk network number to peripheral equipment number

Now, there are two types of translators: Multilevel and expansion. The multilevel translators contain a maximum of six levels of information in the form of linked hierarchical tables:

1- Head Table
2- Subtranslator
3- Primary translator word
4- Auxiliary block or expansion table
5- List
6- Subauxiliary block

(1) Head Table: The HT is the "directory" for the translator. It contains addresses or pointers to each subtranslator.

(2) Subtranslator: The ST's are the main subdivisions, so as an office grows larger, or as more features are added, the number of ST's grows larger. For example, there is a translator for every 1,000 directory numbers, so if an office grows from 3,000 to 8,000 lines, an extra 5 subtranslators must be added. Input for translation must contain 2 things: A selector and an index. The selector contains the information as to which subtranslator to use (in the case of DCF, the selector would either be an A, B, C, or D). The index shows which item or word in that particular subtranslator to access. In the DCF example, if the selector were "D", the index could be 1, 2, 3, etc.

(3) Primary Translation Word (PTW): Each index points to a PTW, which is a byte of information. Often, all you need is 1 byte of information (remember that each byte is 23 bits!). If the data isn't stored in the PTW, an address will be there to point to an auxiliary block or expansion table, where the data will be found. The ESS can recognize whether the byte contains data or an address by:

    1 ESS) The 3 most significant bits will be 0.
    1A ESS) The 4 most significant bits will be 0.

    So, if all the 3 (or 4 for 1A) most significant bits contain 0's, the word will be interpreted as an address. (Anyone want to throw the ESS switch into an endless loop????)

(4) Auxiliary Block: The first byte in the AB contains the length of the block. This byte is called the word number (WRDN), and is used by the ESS so it knows where the auxiliary block ends. Remember that when the ESS reads data, all it sees is:

    11000101110001010101001001011100100101010001010101001001011111

    So, in order to stop at the end of the block, the WRDN number must be present.

(5) List: The list is used when additional information other than the standard found in the auxiliary block is needed. The list, like the ST, has an associated index. The address of the list is found in the AB and the index shows which item of data in the list should be looked at. A good example

of what kind of information is found in the list would be a speed calling list.

(6) Subauxiliary Block: The list is only large enough to hold a 7 digit phone number, and if more information has to be stored (like a 10 digit phone number or a trunk identity), an address is stored in the list that points to an SB, which acts very much like an AB.

Expansion Translator
%%%%%%%%%%%%%%%%%%%%
The expansion translator has one table (called an expansion table). This type of translator gets only an index as input, since this type of translator is only a bunch of words. It could have auxiliary blocks, if the space allocated to a word is too small.

RECENT CHANGE AREA OF CALL STORE (1 ESS)
%%
The recent change area consists of:

+ primary recent change area
+ auxiliary recent change area
+ customer originated recent change (CORC)

The starting and ending addresses for these rc areas are stored in the MHT. The primary recent change area is used to store changes affecting primary translation words. Each change is stored in a primary RC register, which consists of two 23 bit bytes. These two bytes contain status bits, primary translation address in the program store, and the primary translation word (PTW) address in call store. The first byte in the register is the "address word" (AW) and the second is the new primary translation word. When looking through the AW, bits 22 and 21 can tell you what kind of recent change is being
implemented:

11: temporary (not to be put into PS)
10: permanent (to be put into PS)
01: delayed (not active yet)
00: deleted (this space is available)

The PTW (abbreviations make things SO much easier) contains the translation data or the address of the auxiliary RC (TAG). You can tell whether the data is an RC or an address by looking at bits 22 to 18. If they are 0, then this byte contains an address, which is stored in bits 17 to 0.

==Phrack Inc.==

Volume Three, Issue 26, File 7 of 11

<><><><><><><><><><><><><><><><><><><><><><>
<> <>
<> PHONE BUGGING <>
<> <>
<> Telecom's Underground Industry <>
<> <>
<> By Split Decision <>
<> <>
<><><><><><><><><><><><><><><><><><><><><><>

In today's landscape of insider trading, leveraged buyouts and merger mania, it is no great shock that a new underground industry has developed within telecom -- eavesdropping.

Bugs are cheap (starting at $30) and can be installed in as little as 10 seconds. And you can bet your bottom $1 million that this expense pales in comparison to the rewards of finding out your takeover plans, marketing strategies, and product developments.

According to Fritz Lang of Tactical Research Devices (Brewster, NY), there is a virtual epidemic of bugging going on in the American marketplace. Counter-surveillance agencies like TRD have sprung up all over. They search for eavesdropping equipment, then notify the client if they're being tapped. It's up to the client to respond to the intrusion.

Each of TRD's employees is a retired CIA or FBI operative. Formerly, they planted bugs for Uncle Sam. Since it's illegal to plant bugs for anyone else, these men now engage in counter surveillance work, pinpointing eavesdropping devices, and sometimes the culprits who put them there, for TRD's client companies.

Where Do They Put The Bugs?
%%%%%%%%%%%%%%%%%%%%%%%%%%%

Your TELEPHONE, of course, is a convenient place to install an eavesdropping device. But this doesn't mean that the illegal tapping will be limited to your phone conversations.

Electronic phones have microphones which are always "live," even when the telephone is on-hook. Stick an amplifier and transmitting unit to the microphone, and you have constant surveillance of all conversations taking place in that room, whether or not the phone is off-hook at the time.

A device rapidly gaining popularity among today's wire-tappers is a mouthpiece containing a tiny bug, which looks exactly like the one of your 2500 set. All it takes is one trip to the water cooler or the men's room for the insider to surreptitiously make the old switcheroo.

LOUDSPEAKERS are another favorite location for wire-tappers, because they can pick up conversations when not in use. Paging systems, piped in music, and telephone systems all employ some variety of amplifier which the culprit can use to his advantage.

LINE INTERCEPTORS allow eavesdroppers more extensive coverage of your

activities, since they can monitor more than on-line communications from a single listening post.

But really, the number of places you can find a bug is limited only by the tapper's imagination. Light switches, plugs, clocks, calculators, legs of wooden chairs, staplers, ashtrays, the underside of a toilet bowl -- all of these items have proved fertile territory for the little critters.

Tools For Finding The Bugs

TRD's people use a patented Surveillance Search Receiver to locate the bugs. The Receiver uses a broad-band radio spectrum, from 25 kHz to 7 gHz.

If there is an unaccounted-for radio frequency emission on the premises, the Receiver will tune it in on a small spectrum monitor. It then traces the emission to its inevitable source, the bug.

For room bugs, they also use a Non-Linear Junction Detector, which can pinpoint all electronic circuit diodes or resistors in the architecture of the building.

The Detector emits a high microwave signal into walls, furniture, et al., causing any circuit hidden within to oscillate. As soon as they oscillate, they become detectable.

Mr. Lang clears up a misconception about the Russians bugging our embassy in Moscow. "They didn't riddle the building with actual bugs, instead, they buried millions of little resistors in the concrete."

The embassy, therefore, became a hot bed for false alarms. Whenever the American counter-measure people came in with their detectors to look for a bug, they'd pick up oscillation readings from the countless resistors and capacitors buried in the walls. Finding any real bugs would be infinitely more difficult than finding the old needle in a haystack.

For finding wire-taps along the phone lines, TRD uses a computerized electronic Telephone Analyzer. The unit runs 18 different tests on phone lines between the CPE block and the Central Office (CO). Resistance, voltage, and line balance are just a few of them. Once they locate a tapped line, they send a pulse down it with a time-domain reflectometer, which can pinpoint exactly where in the line the bug has been affixed.

Bear in mind that wire-tapping is extremely difficult and time consuming. As much as 20 hours of conversations has to be monitored every single business day. Because of this, key executives' telephones are usually the only ones slated for a wire-tap.

Catching The Culprit

Finding a wire-tap is easier than finding the spy who bugged your office. Direct hardwire taps can be traced to the remote location where the snoop stores his voltage-activated electronic tape recorder. After you've found the monitoring post, it's a matter of hanging around the premises until someone comes to collect the old tapes and put in fresh ones.

As for room bugs, your best bet is to make the device inoperable, without removing it, and wait for the eavesdropping to come back to fix or replace it.

Once Is Never Enough

%%%%%%%%%%%%%%%%%%%%

Some of TRD's clients have their offices checked monthly, some quarterly. After the initial sweep, you can have equipment installed on your phone lines which constantly monitors any funny stuff.

As for TRD, they offer a money-back guarantee if they fail to detect an existing bug on your premises. Mr. Lang assures us that Fortune 500 company has been bugged to a greater or lesser extent. That's how out-of-hand the problem is getting.

Toward the end of our conversation, Mr. Lang pauses. "So you're really going to print this, huh? You're really on the up and up?" Then he spills the beans.

It turns out Mr. Fritz Lang is really Mr. Frank Jones (he says), a licensed private investigator with a broad reputation in the industry. He used the alias because he suspected I was from a rival counter-measure agency, or worse,
a wire-tapper, trying to infiltrate his operations.

Which quite possibly I am. You can't trust anybody in this spy business.

_

==Phrack Inc.==

Volume Three, Issue 26, File 8 of 11

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                      <>
<>         Future Transcendent Saga Appendix III        <>
<>                 "Limbo To Infinity"                  <>
<>                                                      <>
<>                   Internet Domains                   <>
<>                                                      <>
<>                      April 1989                      <>
<>                                                      <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Special thanks goes out to Henry Nussbacher who did the actual compiling of this list. For those of you on Bitnet, you may have seen this previously in the form of BITNET GATES.

For readers who are a little unsure of what this file shows, I will try to explain a little. As you already know from the Future Transcendent Saga, there
are many different networks all around the world. Most of these networks are connected in some way, usually all being called the Internet.

Now, as you should know, Taran King and Knight Lighting both have addresses on Bitnet that are on the node UMCVMB.BITNET. However, this node also exists on the Internet in a different form: UMCVMB.MISSOURI.EDU.

EDU is the Internet domain for academic nodes. Not every node on Bitnet has a translation on the Internet. Then again, only a small fraction of the nodes on Internet have Bitnet equivalents.

So what this file really shows is what network you are sending mail to when you
have an address that contains a nodename or routing designation that looks a little strange. For people on Bitnet it also shows what Bitnet address serves as the gateway between Bitnet and whichever network they are sending to on the Internet.

The following is a table of gateways between Bitnet and other networks. It is in the format of;

Domain: The upper level recognized name by the Columbia University VM mail system.

Name: The descriptive name of this network.

Gateway: Where the mail is sent to in Bitnet. Unless otherwise specified,
the gateway expects to receive a BSMTP (Batch Simple Mail Transfer Protocol) envelope. Users in general do not need to worry about the contents of this field. This is not a mailbox for general questions but rather the server machine (daemon) that
acts as the transporter of mail from one network to another. Software postmasters are expected to configure their system so that their system sends to the nearest gateway and not to the default gateway.

Translation: Upon occasion, certain addresses will be translated internally to
              point to an indirect gateway. In such a case, the complete
              address is specified.

- -

Internet Commercial Clients (COM)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Domain: COM
Name: Internet - Commerical clients
Gateway: SMTP@INTERBIT

Domain: CRD.GE.COM
Name: General Electric Corporate Research & Development
Gateway: MAILER@GECRDVM1

Domain: HAC.COM
Name: Hughes Aircraft Co. Local Area Network
Gateway: SMTPUSER@YMIR

Domain: STARGATE.COM
Name: Stargate Information Service
Gateway: SMTP@UIUCVMD

- -

Internet Academic Clients (EDU)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Domain: EDU
Name: Internet - Academic clients
Gateway: SMTP@INTERBIT

Domain: ARIZONA.EDU
Name: University of Arizona, Tucson
Gateway: SMTPUSER@ARIZRVAX

Domain: BATES.EDU
Name: Bates College Local Area Network
Gateway: MAILER@DARTCMS1

Domain: CMSA.BERKELEY.EDU
Name: University of California at Berkeley
Gateway: MAILER@UCBCMSA

Domain: BERKELEY.EDU
Name: University of California at Berkeley Campus Mail Network
Gateway: BSMTP@UCBJADE

Domain: BU.EDU
Name: Boston University Local Area Network
Gateway: MAILER@BUACCA

Domain: BUCKNELL.EDU
Name: Bucknell University Local Area Network
Gateway: SMTP@BKNLVMS

Domain: BUFFALO.EDU
Name: State University of New York at Buffalo

Gateway: SMTP@UBVM

Domain: BYU.EDU
Name: Brigham Young University Campus Network
Gateway: MAILER@BYUADMIN

Domain: CALTECH.EDU
Name: California Institute of Technology local area network
Gateway: MAILER@HAMLET

Domain: CLAREMONT.EDU
Name: Claremont Colleges Local Area Network
Gateway: SMTPUSER@YMIR

Domain: CLARKSON.EDU
Name: Clarkson University Local Area Network
Gateway: MAILER@CLVM

Domain: CMU.EDU
Name: Carnegie Mellon University Local Area Network
Gateway: MAILER@CMUCCVMA

Domain: COLORADO.EDU
Name: University of Colorado at Boulder Local Area Network
Gateway: SMTPUSER@COLORADO

Domain: COLUMBIA.EDU
Name: Columbia University Local Area Network
Gateway: MAILER@CUVMA

Domain: CONNCOLL.EDU
Name: Connecticut College Local Area Network
Gateway: MAILER@CONNCOLL

Domain: CORNELL.EDU
Name: Cornell University
Gateway: MAL@CORNELLC

Domain: CUN.EDU
Name: University of Puerto Rico
Gateway: SMTPUSER@UPRENET

Domain: CUNY.EDU
Name: City University of New York
Gateway: SMTP@CUNYVM

Domain: DARTMOUTH.EDU
Name: Dartmouth College Local Area Network
Gateway: MAILER@DARTCMS1

Domain: GATECH.EDU
Name: Georgia Institute of Technology Local Area Network
Gateway: MAILER@GITVM1

Domain: HAMPSHIRE.EDU
Name: Hampshire College Local Area Network
Gateway: MAILER@HAMPVMS

Domain: HARVARD.EDU
Name: Harvard University Local Area Network
Gateway: MAILER@HARVARDA

Domain: HAWAII.EDU
Name: University of Hawaii Local Area Network
Gateway: MAILER@UHCCUX

Domain: IASTATE.EDU
Name: Iowa State University Local Area Network
Gateway: MAILER@ISUMVS

Domain: KSU.EDU
Name: Kansas State University
Gateway: MAILER@KSUVM

Domain: LEHIGH.EDU
Name: Lehigh University Campus Network
Gateway: SMTPUSER@LEHIIBM1

Domain: LSU.EDU
Name: Louisiana State University local area network
Gateway: SMTPUSER@LSUVAX

Domain: MAINE.EDU
Name: University of Maine System
Gateway: MAILER@MAINE

Domain: MAYO.EDU
Name: Mayo Clinic LAN, Minnesota Regional Network
Gateway: SMTPUSER@UMNACVX

Domain: MIT.EDU
Name: MIT Local Area Network
Gateway: MAILER@MITVMA

Domain: NCSU.EDU
Name: North Carolina State University
Gateway: MAILER@NCSUVM

Domain: CCCC.NJIT.EDU
Name: NJIT Computer Conferencing Center
Gateway: MAILER@ORION
Comments: In process of establishing a single NJIT.EDU domain

Domain: NWU.EDU
Name: Northwestern University Local Area Network
Gateway: SMTPUSER@NUACC

Domain: NYU.EDU
Name: New York University/Academic Computing Facility LAN
Gateway: SMTP@NYUCCVM

Domain: OBERLIN.EDU
Name: Oberlin College
Gateway: SMTPUSER@OBERLIN

Domain: PEPPERDINE.EDU
Name: Pepperdine University
Gateway: MAILER@PEPVAX

Domain: PRINCETON.EDU
Name: Princeton University Local Area Network
Gateway: VMMAIL@PUCC

Domain: PURDUE.EDU
Name: Purdue University Campus Network
Gateway: MAILER@PURCCVM

Domain: RICE.EDU
Name: Rice University Local Area Network
Gateway: MAILER@RICE

Domain: ROSE-HULMAN.EDU
Name: Rose-Hulman Institute of Technology Local Area Network
Gateway: SMTPUSER@RHIT

Domain: SDSC.EDU
Name: San Diego Supercomputer Center
Gateway: MAILER@SDSC

Domain: STANFORD.EDU
Name: Stanford University Local Area Network
Gateway: MAILER@STANFORD

Domain: STOLAF.EDU
Name: St. Olaf College LAN, Minnesota Regional Network
Gateway: SMTPUSER@UMNACVX

Domain: SWARTHMORE.EDU
Name: Swarthmore College Local Area Network
Gateway: MAILER@SWARTHMR

Domain: SYR.EDU
Name: Syracuse University Local Area Network (FASTNET)
Gateway: SMTP@SUVM

Domain: TORONTO.EDU
Name: University of Toronto local area Network
Gateway: MAILER@UTORONTO

Domain: TOWSON.EDU
Name: Towson State University Network
Gateway: MAILER@TOWSONVX

Domain: TRINCOLL.EDU
Name: Trinity College - Hartford, Connecticut
Gateway: MAILER@TRINCC

Domain: TRINITY.EDU
Name: Trinity University
Gateway: MAILER@TRINITY

Domain: TULANE.EDU
Name: Tulane University local area Network
Gateway: MAILER@TCSVM

Domain: UAKRON.EDU
Name: University of Akron Campus Network
Gateway: MAILER@AKRONVM

Domain: UCAR.EDU
Name: National Center for Atmospheric Research Bldr CO
Gateway: SMTPSERV@NCARIO

Domain: UCHICAGO.EDU
Name: University of Chicago Local Area Network
Gateway: MAILER@UCHIMVS1

Domain: UCLA.EDU
Name: University of California Los Angeles
Gateway: MAILER@UCLAMVS

Domain: UCOP.EDU
Name: University of California, Office of the President
Gateway: BSMTP@UCBJADE

Domain: UCSB.EDU
Name: University of California, Santa Barbara
Gateway: MAILER@SBITP

Domain: UCSD.EDU
Name: University of California at San Diego Campus Mail Network
Gateway: MAILER@UCSD

Domain: UCSF.EDU
Name: Univ of California San Francisco Network
Gateway: BSMTP@UCSFCCA

Domain: UFL.EDU
Name: University of Florida, Gainesville, FL
Gateway: MAILER@NERVM

Domain: UGA.EDU
Name: University of Georgia Campus Network
Gateway: MAILER@UGA

Domain: UIC.EDU
Name: University of Illinois at Chicago
Gateway: MAILER@UICVM

Domain: UIUC.EDU
Name: University of Illinois at Urbana-Champaign Local Area Network
Gateway: SMTP@UIUCVMD

Domain: UKANS.EDU
Name: University of Kansas
Gateway: SMTPUSER@UKANVAX

Domain: UKY.EDU
Name: University of Kentucky
Gateway: MAILER@UKCC

Domain: UMN.EDU
Name: University of Minnesota LAN, Minnesota Regional Network
Gateway: SMTPUSER@UMNACVX

Domain: UNL.EDU
Name: University of Nebraska Lincoln
Gateway: SMTPUSER@UNLVAX1

Domain: UOREGON.EDU
Name: University of Oregon
Gateway: SMTPUSER@OREGON

Domain: URICH.EDU

```
Name:       University of Richmond network
Gateway:    SMTPUSER@URVAX

Domain:     UPENN.EDU
Name:       University of Pennsylvania Campus Network
Gateway:    SMTPUSER@PENNLRSM

Domain:     USC.EDU
Name:       University of Southern California, Los Angeles
Gateway:    SMTP@USCVM

Domain:     UTAH.EDU
Name:       University of Utah Computer Center
Gateway:    SMTPUSER@UTAHCCA

Domain:     UVCC.EDU
Name:       Utah Valley Community College
Gateway:    SMTPUSER@UTAHCCA

Domain:     VCU.EDU
Name:       Virginia Commonwealth University Internetwork
Gateway:    SMTPUSER@VCURUBY

Domain:     WASHINGTON.EDU
Name:       University of Washington Local Area Network
Gateway:    MAILER@UWAVM

Domain:     WESLEYAN.EDU
Name:       Wesleyan University Local Area Network
Gateway:    MAILER@WESLEYAN

Domain:     WISC.EDU
Name:       University of Wisconsin Local Area Network
Gateway:    SMTPUSER@WISCMAC3

Domain:     WVNET.EDU
Name:       West Virginia Network for Educational Telecomputing
Gateway:    MAILER@WVNVAXA

Domain:     YALE.EDU
Name:       Yale University Local Area Network
Gateway:    SMTP@YALEVM

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

United States Of America Government Domains
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Domain:     GOV
Name:       Internet - Government clients
Gateway:    SMTP@INTERBIT

Domain:     JPL.NASA.GOV
Name:       Jet Propulsion Laboratory
Gateway:    MAILER@HAMLET

Domain:     LBL.GOV
Name:       Lawrence Berkeley Laboratory
Gateway:    MAILER@LBL

Domain:     NBS.GOV
```

```
Name:       National Institute of Standards and Technology
Gateway:    SMTPUSER@NBSENH

Domain:     NSESCC.GSFC.NASA.GOV
Name:       NASA Space and Earth Sciences Computing Center
Gateway:    MAILER@SCFVM
```

- -
-

Italian National Network (IT)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

```
Domain:     IT
Name:       Italian national network
Gateway:    MAILER@ICNUCEVX

Domain:     TO.CNR.IT
Name:       CNR (Italian Research Council) Network
Gateway:    CNRGATE@ITOPOLI

Domain:     INFN.IT
Name:       Italian Research Network
Gateways:   MAILER@IBOINFN
            INFNGW@IPIVAXIN
Comments:   IPIVAXIN is to only be used as a backup gateway in the event that
            IBOINFN is broken.
```

- -
-

Other Standard Domains Not Previously Detailed
%%

```
Domain:     ARPA
Name:       Advanced Research Projects Agency - US DOD
Gateway:    SMTP@INTERBIT

Domain:     AT
Name:       University Network of Austria
Gateway:    MAILER@AWIUNI11

Domain:     BE
Name:       Belgian Research Network
Gateway:    MAILER@BEARN

Domain:     CA
Name:       Canadian mail domain
Gateway:    MAILER@UTORGPU

Domain:     CDN
Name:       Canadian University X.400 Research Network
Gateway:    MAILER@UWOCC1
Comments:   The gateway at CERNVAX is no longer supported due to
            the high cost of X.25 transfer over public data networks.

Domain:     CERN
Name:       Center for Nuclear Research Network
Gateways:   1) MAILER@UWOCC1
            2) MAILER@CERNVAX

Domain:     CH
Name:       Swiss University Mail Network(s)
Gateway:    MAILER@CEARN
```

Domain: CHUNET
Name: Swiss University pilot X.400 Network
Gateway: MAILER@CERNVAX

Domain: DBP.DE
Name: German X.400 National Network
Gateway: MAILER@DFNGATE

Domain: DE
Name: EARN view of German academic networks
Gateway: MAILER@DEARN

Domain: DK
Name: Denmark's Internet Domain
Gateway: MAILER@NEUVM1

Domain: ES
Name: Spanish Internet Domain
Gateway: MAILER@EB0UB011

Domain: FI
Name: Finland's Internet Domain
Gateway: MAILER@FINHUTC

Domain: FR
Name: French University pilot X.400 Network
Gateway: MAILER@CERNVAX

Domain: HEPnet
Name: High Energy Physics network
Gateway: MAILER@LBL

Domain: IE
Name: Ireland Academic X25 Network
Gateway: MAILER@IRLEARN

Domain: IL
Name: Israeli Academic Research Network
Gateway: MAILER@TAUNIVM

Domain: IS
Name: Icelands Internet Domain
Gateway: MAILER@NEUVM1

Domain: JP
Name: Japanese network
Gateway: MAILER@JPNSUT00

Domain: MFENET
Name: Magnetic Fusion Energy Network
Gateway: MFEGATE@ANLVMS

Domain: MIL
Name: Internet - Military clients
Gateway: SMTP@INTERBIT

Domain: NET
Name: Internet - Network gateways
Gateway: SMTP@INTERBIT

```
Domain:     NL
Name:       Netherlands Internet Domain
Gateway:    MAILER@HEARN

Domain:     NO
Name:       Norwegian Internet domain
Gateway:    MAILER@NORUNIX

Domain:     ORG
Name:       Internet - Organizational clients
Gateway:    SMTP@INTERBIT

Domain:     PT
Name:       National Scientific Computation Network (of Portugal)
Gateway:    MLNET@PTIFM

Domain:     SE
Name:       SUNET, Swedish University NETwork
Gateway:    MAILER@SEKTH

Domain:     SG
Name:       Singapore National Network
Gateway:    MAILER@NUSVM

Domain:     SUNET
Name:       Swedish University X.400 Network
Comments:   The gateways at CERNVAX and UWOCC1 are no longer supported
            due to the high cost of X.25 transfer over public data
            networks -- see domain SE

Domain:     UK
Name:       United Kingdom University/Research Network (Janet)
Gateway:    MAILER@UKACRL
Comments:   NRSname is basically a reversal of the domain address.
            Example: user@GK.RL.AC.UK becomes user%UK.AC.RL.GK@AC.UK

Domain:     UNINETT
Name:       Norwegian University pilot X.400 Network
Gateway:    MAILER@NORUNIX

Domain:     US
Name:       Internet - USA clients
Gateway:    SMTP@INTERBIT

Domain:     UTORONTO
Name:       University of Toronto local area Network
Gateway:    MAILER@UTORONTO

Domain:     UUCP
Name:       Unix Network
Gateways:   1) MAILER@PSUVAX1   (USA)
            2) MAILER@UWOCC1    (Canada)
            3) BSMTP@UNIDO      (Germany)
            4) MAILER@MCVAX     (Netherlands)
Alternate addressing: user%node.UUCP@HARVARD.HARVARD.EDU
                      user%node.UUCP@RUTGERS.EDU
Comments:   Only users in Germany are allowed to send to UNIDO.  All
            European users are recommended to use MCVAX.

Domain:     WUSTL
Name:       Washington University local area Network
```

Gateway: GATEWAY@WUNET

- -
-

Bitnet - Internet Regional Gateways
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Below is a list of those sites that will handle regional traffic between Bitnet and the Internet:

SMTP@CUNYVM
SMT@CORNELLC
MAILER@MITVMA
MAILER@ICNUCEVM - available only for Italian nodes

You should *ALWAYS* use the generic address of SMTP@INTERBIT and never any of the addresses mentioned above. The addresses stated above are for informational and debugging purposes ONLY. Failure to abide by this rule will cause the owners of the gateway to close their service to all Bitnet and EARN users.

Indirect Domains
%%%%%%%%%%%%%%%%
Domains that are unreachable directly, but that the Internet exit of Mailer knows how to translate:

```
Domain:     DEC
Name:       Digital Equipment Internal Network (Easynet)
Gateway:    SMTP@INTERBIT
Sample:     user@domain.DEC
Translated to: user%node.DEC@DECWRL.DEC.COM

Domain:     OZ (soon to become OZ.AU)
Name:       Australian University Network
Gateway:    SMTP@INTERBIT
Sample:     user@node.OZ
Translated to: user%node.OZ@UUNET.UU.NET
```

Domains that are unreachable directly but that are accessible by specifying the
address explicitly:

```
Name:       Xerox Internal Use Only Network (Grapevine)
Sample:     user.Registry@Xerox.Com

Name:       IBM Internal Use Only Network (VNET)
Sample:     user@Vnet

Comments:   1) Mail must be sent directly to user and not via a 3rd party
               mailer (i.e. VM Mailer server)
            2) User within Vnet must first receive approval within IBM to
               establish a circuit and then initiate a virtual circuit.  A
user
               within Bitnet may not establish communications with a VNET
user,
               without the above requirement.
            3) This gateway is only open to selected nodes within IBM which
               have ties with academia (i.e. ACIS).
```

_

==Phrack Inc.==

Volume Three, Issue 26, File 9 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        %%%%%%%%%%%   %%%%%%%%%   %%%%%%%        PWN
PWN                Issue XXVI/Part 1                PWN
PWN                                                 PWN
PWN                 April 25, 1989                  PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Welcome to Issue XXVI of Phrack World News. This issue features articles on Robert Tappen Morris, ITT, Telenet, PC Pursuit, a hacker's convention in Holland, government wiretapping, viruses, social security numbers, a rivalry between two different factions of TAP Magazine and much more.

As we are getting closer to SummerCon '89, it is becoming increasingly more important for us to get an idea of who to be expecting and who we need to contact to supply with further information.

Since we only communicate directly with a select group of people at this time, we recommend that you contact Red Knight, Aristotle, or Violence (or other members of the VOID hackers). These people will in turn contact us and then we can get back to you. Keep in mind that only people who are able to contact us will be receiving the exact location of SummerCon '89.

Please do not wait till the last minute as important information and changes can occur at any time.

:Knight Lightning

_

Cornell Panel Concludes Morris Responsible For Computer Worm   April 6, 1989
%%
By Dennis Meredith (Cornell Chronicle)

Graduate student Robert Tappen Morris Jr., working alone, created and spread the "worm" computer program that infected computers nationwide last November, concluded an internal investigative commission appointed by Provost Robert Barker.

The commission said the program was not technically a "virus" -- a program that inserts itself into a host program to propagate -- as it has been referred to in popular reports. The commission described the program as a "worm," an independent program that propagates itself throughout a computer system.

In its report, "The Computer Worm," the commission termed Morris's behavior "a juvenile act that ignored the clear potential consequences." This failure constituted "reckless disregard of those probable consequences," the commission

stated.

Barker, who had delayed release of the report for six weeks at the request of both federal prosecutors and Morris's defense attorney, said, "We feel an overriding obligation to our colleagues and to the public to reveal what we know about this profoundly disturbing incident."

The commission had sought to determine the involvement of Morris or other members of the Cornell community in the worm attack. It also studied the motivation and ethical issues underlying the release of the worm.

Evidence was gathered by interviewing Cornell faculty, staff, and graduate students and staff and former students at Harvard University, where Morris had done undergraduate work.

Morris declined to be interviewed on advice of counsel. Morris had requested and has received a leave of absence from Cornell, and the university is prohibited by federal law from commenting further on his status as a student.

The commission also was unable to reach Paul Graham, a Harvard graduate student
who knew Morris well. Morris reportedly contacted Graham on November 2 1988, the day the worm was released, and several times before and after that.

Relying on files from Morris's computer account, Cornell Computer Science Department documents, telephone records, media reports, and technical reports from other universities, the commission found that:

- Morris violated the Computer Sciences Department's expressed policies against computer abuse. Although he apparently chose not to attend orientation meetings at which the policies were explained, Morris had been given a copy of them. Also, Cornell's policies are similar to those at Harvard, with which he should have been familiar.

- No member of the Cornell community knew Morris was working on the worm. Although he had discussed computer security with fellow graduate students, he did not confide his plans to them. Cornell first became aware of Morris's involvement through a telephone call from the Washington Post to the science editor at Cornell's News Service.

- Morris made only minimal efforts to halt the worm once it had propagated, and did not inform any person in a position of responsibility about the existence or content of the worm.

- Morris probably did not intend for the worm to destroy data or files, but he probably did intend for it to spread widely. There is no evidence that he intended for the worm to replicate uncontrollably.

- Media reports that 6,000 computers had been infected were based on an initial rough estimate that could not be confirmed. "The total number of affected computers was surely in the thousands," the commission concluded.

- A computer security industry association's estimate that the worm caused
about $96 million in damage is "grossly exaggerated" and "self-serving."

- Although it was technically sophisticated, "the worm could have been created by many students, graduate or undergraduate ... particularly if forearmed with knowledge of the security flaws exploited or of similar

flaws."

The commission was led by Cornell's vice president for information technologies, M. Stuart Lynn. Other members were law professor Theodore Eisenberg, computer science Professor David Gries, engineering and computer science Professor Juris Hartmanis, physics professor Donald Holcomb, and Associate University Counsel Thomas Santoro.

Release of the worm was not "an heroic event that pointed up the weaknesses of operating systems," the report said. "The fact that UNIX ... has many security flaws has been generally well known, as indeed are the potential dangers of viruses and worms."

The worm attacked only computers that were attached to Internet, a national research computer network and that used certain versions of the UNIX operating system. An operating system is the basic program that controls the operation of a computer.

"It is no act of genius or heroism to exploit such weaknesses," the commission said.

The commission also did not accept arguments that one intended benefit of the worm was a heightened public awareness of computer security.

"This was an accidental by-product of the event and the resulting display of media interest," the report asserted. "Society does not condone burglary on the grounds that it heightens concern about safety and security."

In characterizing the action, the commission said, "It may simply have been the unfocused intellectual meandering of a hacker completely absorbed with his creation and unharnessed by considerations of explicit purpose or potential effect."

Because the commission was unable to contact Graham, it could not determine whether Graham discussed the worm with Morris when Morris visited Harvard about two weeks before the worm was launched. "It would be interesting to know, for example, to what Graham was referring to in an Oct. 26 electronic mail message to Morris when he inquired as to whether there was 'Any news on the brilliant project?'" said the report.

Many in the computer science community seem to favor disciplinary measures for Morris, the commission reported.

"However, the general sentiment also seems to be prevalent that such disciplinary measures should allow for redemption and as such not be so harsh as to permanently damage the perpetrator's career," the report said.

The commission emphasized, that this conclusion was only an impression from its investigations and not the result of a systematic poll of computer scientists.

"Although the act was reckless and impetuous, it appears to have been an uncharacteristic act for Morris" because of his past efforts at Harvard and elsewhere to improve computer security, the commission report said.

Of the need for increased security on research computers, the commission wrote, "A community of scholars should not have to build walls as high as the sky to

protect a reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information."

The trust between scholars has yielded benefits to computer science and to the world at large, the commission report pointed out.

"Violations of that trust cannot be condoned. Even if there are unintended side benefits, which is arguable, there is a greater loss to the community as a whole."

The commission did not suggest any specific changes in the policies of the Cornell Department of Computer Science and noted that policies against computer
abuse are in place for centralized computer facilities. However, the commission urged the appointment of a committee to develop a university-wide policy on computer abuse that would recognize the pervasive use of computers distributed throughout the campus.

The commission also noted the "ambivalent attitude towards reporting UNIX security flaws" among universities and commercial vendors. While some computer
users advocate reporting flaws, others worry that such information might highlight the vulnerability of the system.

"Morris explored UNIX security amid this atmosphere of uncertainty, where there
were no clear ground rules and where his peers and mentors gave no clear guidance," the report said.

"It is hard to fault him for not reporting flaws that he discovered. From his viewpoint, that may have been the most responsible course of action, and one that was supported by his colleagues."

The commission's report also included a brief account of the worm's course through Internet. After its release shortly after 7:26 p.m. on November 2, 1988, the worm spread to computers at the Massachusetts Institute of Technology, the Rand Corporation, the University of California at Berkeley and others, the commission report said.

The worm consisted of two parts -- a short "probe" and a much larger "corpus." The problem would attempt to penetrate a computer, and if successful, send for the corpus.

The program had four main methods of attack and several methods of defense to avoid discovery and elimination. The attack methods exploited various flaws and features in the UNIX operating systems of the target computers. The worm also attempted entry by "guessing" at passwords by such techniques as exploiting computer users' predilections for using common words as passwords.

The study's authors acknowledged computer scientists at the University of California at Berkeley for providing a "decompiled" version of the worm and other technical information. The Cornell commission also drew on analyses of the worm by Eugene H. Spafford of Purdue University and Donn Seeley of the University of Utah.

People Vs. ITT Communications Services, Inc. March 29, 1989

%%

NOTICE OF CLASS ACTION AND PROPOSED SETTLEMENT TO CERTAIN CURRENT

AND FORMER CUSTOMERS OF UNITED STATES TRANSMISSION SYSTEMS, INC.
(NOW KNOWN AS ITT COMMUNICATIONS SERVICES, INC.)

By order of the United States District Court for the Eastern District of Michigan, PLEASE TAKE NOTICE THAT:

A class action lawsuit has been filed on behalf of certain former and current customers against United States Transmission Systems, Inc., now known as ITT Communications Services, Inc., hereinafter referred to as "USTS." The Court has preliminarily approved a settlement of this lawsuit.

YOU ARE URGED TO READ THIS NOTICE CAREFULLY BECAUSE IT AFFECTS YOUR RIGHTS AND WILL BE BINDING ON YOU IN THE FUTURE.

I. NOTICE OF A PENDING CLASS ACTION

A. Description of the Lawsuit

Plaintiffs have sued USTS, alleging that USTS charged customers for certain unanswered phone calls, holding time, busy signals, and central office recorded messages, hereinafter referred to as "unanswered calls," without adequately disclosing such charges to their customers or the public. Plaintiffs seek to present their own claims for charges for unanswered calls, as well as the claims of other current and former USTS customers for similar charges.

USTS denies the violations alleged by plaintiffs, and contends that at all times, USTS has charged its subscribers fairly and properly and has disclosed fully and fairly the basis for its long distance charges. USTS has agreed to settle plaintiff's suit solely to avoid the expense, inconvenience and disruption of further litigation.

This notice is not an expression of any opinion by the Court of the merits of this litigation or of the Settlement Agreement. The Complaint, the Settlement Agreement and other pleadings in this case may be inspected during normal business hours at the office of the Clerk of the United States District Court for the Eastern District of Michigan, 231 West Lafayette Boulevard, Detroit, MI 48226.

B. The Settlement Class

Plaintiffs and USTS have entered into a Settlement Agreement, which has been preliminarily approved by the Court. Under the terms of the Settlement Agreement, the parties have agreed, for purposes of settlement only, that this suit has been brought on behalf of the following class of persons similarly situated to Plaintiffs, hereinafter known as "the Class":

All persons and entities that subscribed to and utilized the long distance telephone service of USTS or its predecessor ITT Corporate Communication Services, Inc., referred to collectively hereinafter as "USTS," at any time during the period January 1, 1979 through December 31, 1985.

C. How to Remain a Class Member

If you were a subscriber to and utilized USTS' long distance service at any time during this period, you are a member of the Class. You need do nothing to remain a member of the Class and participate in the benefits this settlement will provide. If you remain in the Class, you will be bound by

the results of the settlement and/or the lawsuit.

D. How to Exclude Yourself From the Class

You are not required to be a member of the Class. Should you decide that you do not want to me a member of the Class, you must send an Exclusion Notice that states your name, your current address, and your desire to be excluded from the Class to the Clerk of the United States District Court for the Eastern District of Michigan at the address given at the end of this Notice, postmarked no later than April 20, 1989. If you choose to be excluded from the Class, you may not participate in the settlement. You will not, however, be bound by any judgment dismissing this action and you will be free to pursue on your own behalf any legal rights you may have.

II. TERMS OF THE SETTLEMENT

The Settlement Agreement requires USTS to provide to Class members up to 750,000 minutes of long distance telephone credits having a maximum value, at 30 cents per minute, of $225,000, hereinafter known as the "Settlement Credits," and cash refunds up to a maximum of $50,000. These benefits are available to Class members who file a proof of claim in a timely manner as described in Section III below. Class members may choose one benefit from the following options:

A. A *standardized credit* toward USTS long distance telephone service of $1.50 for each year from 1979 through 1985 in which the Class member (i) was a USTS customer, and (ii) claims that s/he was charged by USTS for unanswered calls; or

B. A *standardized cash refund* of 90 cents for each year from 1979 through 1985 in which the Class member was (i) was a USTS customer and (ii) claims that s/he was charged by USTS for unanswered calls; or,

C. An *itemized credit* toward USTS long distance service of 30 cents for each minute of unanswered calls for which the Class member was charged during the Class period (January 1, 1979 through December 31, 1985) and for which the Class member has not been previously reimbursed or credited; or,

D. An *itemized cash refund* of 30 cents for each minute of unanswered calls for which the Class member charged during the Class period (January 1, 1979 through December 31, 1985) and for which the Class member has not been previously reimbursed or credited.

To obtain an *itemized* credit or cash refund, the Class member must itemize and attest to each unanswered call for for which a refund or credit is claimed. If the total credits claimed by Class members exceed 750,000 credit minutes, each Class member claiming Settlement Credits will receive his/her/its pro rata share of the total Settlement Credits available.

Class members need not be current USTS customers to claim the standardized and itemized credits. USTS will automatically open an account for any Class member who requests credits and executes an authorization to open such an account. If a Class member incurs a local telephone company service charge in connection with the opening of a USTS account, USTS will issue a credit to the Class member's account for the full amount of such

service charge upon receipt of the local telephone company's bill for the service charge. USTS is not responsible for any other service charge that a local telephone company may impose for ordering, using or terminating USTS service.

The Settlement Agreement requires USTS to pay the costs of giving this Notice (up to a maximum of $120,000) and of administering the settlement described above.

The Settlement Agreement further provides that upon final approval of the settlement, the Court will enter a judgment dismissing with prejudice all claims of plaintiffs and members of the Class that have been or might have been asserted in this action and that relate to USTS' billing practices and disclosure practices for unanswered calls.

Counsel for the Class have investigated the facts and circumstances regarding the claims against USTS and their defenses. In view of those circumstances, counsel for the Class have concluded that this Settlement Agreement is fair and reasonable, and in the best interests of the Class.

III. HOW TO FILE A CLAIM

To receive Settlement Credits or a Cash Refund, you must first obtain a Proof of Claim Notice; then provide all the information requested and return it to the Clerk of the Court postmarked no later than June 30, 1989.

To obtain claim forms:	To file completed claim form:
USTS Class Action Claim Administrator ITT Communication Services, Inc. 100 Plaza Drive Secaucus, NJ 07096	Clerk of the United States Court ATTN: USTS Settlement 231 W. Lafayette Blvd. Room 740 Detroit, MI 48226

If you have any further questions about this Notice, or the filing of Proof of Claim, *write* to the USTS Action Claim Administrator at the above address. If you have any questions about this lawsuit or your participation therein as a member of the Class, *write* to lead counsel for plaintiffs --

Sachnoff Weaver & Rubenstein, Ltd.
ATTN: USTS Settlement
30 South Wacker Drive, Suite 2900
Chicago, IL 60606

Always consult your own attorney for legal advice and questions which concern you about your rights in any class action matter.

DO NOT telephone the Court.

DO NOT telephone the attorneys for plaintiff.

DO NOT telephone the Claims Administrator; any office of USTS or any of its employees.

DO NOT telephone any Telephone Company asking for information on this matter. Only *written correspondence filed in a timely manner will be considered

by the Court.

Telenet Announces New PC Pursuit Terms April 9, 1989

%%

Earlier this year, Telenet announced new terms for the PC Pursuit program, which placed time limits on the use of the service, and set new rates for usage of the service.

***** Most of the deal has been called OFF *****

In a letter dated March 29, 1989 from Floyd H. Trogdon, Vice President and General Manager of Network Services announced several revisions in the earlier plans. His latest letter supersedes all previous memos and usage agreements, and becomes effective July 1, 1989.

There will be THREE membership plans:

- REGULAR membership will be $30 per month for up to 30 hours of non-prime time (evenings and weekend) use. This can be used by the subscriber only. No others allowed to use it.

- FAMILY membership will be $50 per month for up to 60 hours of non-prime time (evenings and weekend) use. This can be used by the subscriber and any immediate family members in the same household. If a single person expected to use more than 30 hours per month, s/he would still buy this "family" plan, even if the entire "family" consisted of just one person.

- HANDICAPPED membership will be $30 per month for up to 90 hours of non-prime time (evening and weekend) use. To qualify for these terms, proof of physical handicap must be provided. Ask Telenet for the exact terms.

EXCESS HOURS over 30 (or 60/90) per month during non-prime time hours will be billed at $3.00 per hour. This is a decrease from the earlier proposed charge of $4.50 per hour.

PRIME-TIME USAGE will be billed at $10.50 per hour, regardless of how much time may be remaining on the PCP membership plan.

The billing will be in arrears each month. That is, the July usage will be billed in August, etc. Call detail will be automatically provided to any subscriber going over thirty hours per month.

GRACE PERIOD/FORGIVENESS: All calls will be given a one minute grace period for the purpose of establishing the connection. There will never be a charge for calls lasting one minute or less. If you disconnect promptly when you see that your call will not complete for whatever reason, there will be no charge.

There will be a two minute minimum on all connections (after the first minute has passed). Otherwise, times will be rounded to the *nearest* minute for billing purposes.

NEW PASSWORDS AND USER I.D.'s FOR EVERYONE: During April, 1989, all current subscribers to PC Pursuit will be issued new passwords and new user identities.

On May 1, 1989, all existing passwords and ID's will be killed.

New users after July 1, 1989 will pay $30 to set up an account. Password changes will be $5.00. *Existing* users will never have to pay a fee to adjust their account upward or downward from regular < == > family plans. Call detail will be provided in June, 1989 to users with more than 30 hours of usage to help them determine which plan they should use; however there will be no charge for extra hours until July.

Because of the confusion and lack of good communication between Telenet and its users over the past few months, the official change in terms from unlimited use to measured use has been postponed from its original starting date in June to July 1.

These are just excerpts from the letter to subscribers posted on the Net Exchange BBS. If you subscribe to PC Pursuit, I recommend you sign on and read the full memo, along with the accompanying Terms and Conditions and price schedules.

Remember, any changes you may have made in February/March in anticipation of the changeover originally planned for May/June are now void. Telenet has stated all users will be defaulted to REGULAR memberships effective July 1 unless they specifically make changes to this during the months of May and June.

Telenet Customer Service: 1-800-336-0437
Telenet Telemarketing: 1-800-TELENET

Sign up via modem with credit card number handy: 1-800-835-3001.

To read the full bulletins, log onto Net Exchange by calling into your local Telenet switcher and connecting to '@pursuit'.

_

==Phrack Inc.==

Volume Three, Issue 26, File 10 of 11

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN
PWN P h r a c k W o r l d N e w s PWN
PWN %%%%%%%%%% %%%%%%%% %%%%%%% PWN
PWN Issue XXVI/Part 2 PWN
PWN PWN
PWN April 25, 1989 PWN
PWN PWN
PWN Created, Written, and Edited PWN
PWN by Knight Lightning PWN
PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

Reach Out And TAP Someone April 3, 1989

%%%%%%%%%%%%%%%%%%%%%%%%

Two former employees of Cincinnati Bell, who were fired by the company for "good cause" according to Cincinnati Bell Chairman Dwight Hibbard are claiming they installed more than 1200 illegal wiretaps over a 12 year period from 1972 - 1984 at the request of their supervisors at the telco and the local police.

Among the alleged targets of the snooping were past and present members of Congress, federal judges, scores of the city's most prominent politicians, business executives, lawyers and media personalities.

Leonard Gates and Robert Draise say they even wiretapped the hotel room where President Gerald Ford stayed during two visits to Cincinnati; and this part of their story, at least, has been verified by the now retired security chief at the hotel.

As more details come out each day, people in Cincinnati are getting a rare look
at a Police Department that apparently spied on itself, and at a grand jury probe that has prompted one former FBI official to suggest that the Justice Department seems more interested in discrediting the accusers than in seeking the truth.

Cincinnati Bell executives says Gates and Draise are just trying to "get even" with the company for firing them. But disclosures thus far seem to indicate there is at least some truth in what the two men are saying about the company they used to work for.

According to Gates and Draise, they were just employees following the orders given to them by their superiors at Cincinnati Bell. But Dwight Hibbard, Chairman of the Board of Cincinnati Bell has called them both liars, and said their only motive is to make trouble for the company.

Cincinnati Bell responded to allegations that the company had specifically participated in illegal wiretapping by filing a libel suit against Gates and Draise. The two men responded by filing a countersuit against the telco. In addition to their suit, four of the people who were allegedly spied on have filed a class action suit against the telco.

In the latest development, Cincinnati Bell has gone public with (according to them) just recently discovered sordid details about an extramarital affair by Gates. A federal grand jury in Cincinnati is now trying to straighten out the

tangled web of charges and countercharges, but so far no indictments have been returned.

Almost daily, Gates and Draise tell further details about their exploits, including taps they claim they placed on phones at the Cincinnati Stock Exchange and the General Electric aircraft engine plant in suburban Evendale.

According to Draise, he began doing these "special assignments" in 1972, when he was approached by a Cincinnati police officer from that city's clandestine intelligence unit. The police officer wanted him to tap the lines of black militants and suspected drug dealers, Draise said.

The police officer assured him the wiretapping would be legal, and that top executives at the phone company had approved. Draise agreed, and suggested recruiting Gates, a co-worker to help out. Soon, the two were setting several wiretaps each week at the request of the Intelligence Unit of the Cincinnati Police Department.

But by around 1975, the direction and scope of the operation changed, say the men. The wiretap requests no longer came from the police; instead they came from James West and Peter Gabor, supervisors in the Security Department at Cincinnati Bell, who claimed *they were getting the orders from their superiors*.

And the targets of the spying were no longer criminal elements; instead, Draise and Gates say they were asked to tap the lines of politicians, business executives and even the phone of the Chief of Police himself, and the personal phone lines of some telephone company employees as well.

Draise said he "began to have doubts about the whole thing in 1979" when he was told to tap the private phone of a newspaper columnist in town. "I told them I wasn't going to do it anymore," he said in an interview during the week of April 2, 1989.

Gates kept on doing these things until 1984, and he says he got cold feet late that year when "the word came down through the grapevine" that he was to tap the phone lines connected to the computers at General Electric's Evendale plant. He backed out then, and said to leave him out of it in the future, and he claims there were hints of retaliation directed at him at that time; threats to "tell what we know about you..."

When Dwight Hibbard was contacted at his office at Cincinnati Bell and asked to comment on the allegations of his former employees, he responded that they were both liars. "The phone company would not do things like that," said Hibbard, "and those two are both getting sued because they say we do." Hibbard has refused to answer more specific questions asked by the local press and government investigators.

In fact, Draise was fired in 1979, shortly after he claims he told his superiors he would no longer place wiretaps on lines. Shortly after he quit handling the "special assignments" given to him he was arrested, and charged with a misdemeanor in connection with one wiretap -- which Draise says he set for a friend who wanted to spy on his ex-girlfriend. Cincinnati Bell claims they had nothing to do with his arrest and conviction on that charge; but they "were forced to fire him" after he pleaded guilty.

Gates was fired in 1986 for insubordination. He claims Cincinnati Bell was retaliating against him for taking the side of two employees who were suing the company for sexual harassment; but his firing was upheld in court.

The story first started breaking when Gates and Draise went to see a reporter at [Mount Washington Press], a small weekly newspaper in the Cincinnati suburban area. The paper printed the allegations by the men, and angry responses started coming in almost immediately.

At first, police denied the existence of the Intelligence Unit, let alone that such an organization would use operatives at Cincinnati Bell to spy on people. Later, when called before the federal grand jury, and warned against lying, five retired police officers, including the former chief, took the Fifth Amendment. Finally last month, the five issued a statement through their attorney, admitting to 12 illegal wiretaps from 1972 - 1974, and implicated unnamed operatives at Cincinnati Bell as their contacts to set the taps.

With the ice broken, and the formalities out of the way, others began coming forward with similar stories. Howard Lucas, the former Director of Security for Stouffer's Hotel in Cincinnati recalled a 1975 incident in which he stopped Gates, West and several undercover police officers from going into the hotel's phone room about a month before the visit by President Ford.

The phone room was kept locked, and employees working there were buzzed in by someone already inside, recalled Lucas. In addition to the switchboards, the room contained the wire distribution frames from which phone pairs ran throughout the hotel. Lucas refused to let the police officers go inside without a search warrant; and they never did return with one.

But Lucas said two days later he was tipped off by one of the operators to look in one of the closets there. Lucas said he found a voice activated tape recorder and "a couple of coils they used to make the tap." He said he told the Police Department and Cincinnati Bell about his findings, but "...I could not get anyone to claim it, so I just yanked it all out and threw it in the dumpster..."

Executives at General Electric were prompted to meet with Draise and Gates recently to learn the extent of the wiretapping that had been done at the plant. According to Draise, GE attorney David Kindleberger expressed astonishment when told the extent of the spying; and he linked it to the apparent loss of proprietary information to Pratt & Whitney, a competing manufacturer of aircraft engines.

Now all of a sudden, Kindleberger is clamming up. I wonder who got to him? He admits meeting with Draise, but says he never discussed Pratt & Whitney or any competitive situation with Draise. But an attorney who sat in on the meeting supports Draise's version.

After an initial flurry of press releases denying all allegations of illegal wiretapping, Cincinnati Bell has become very quiet, and is now unwilling to discuss the matter at all except to tell anyone who asks that "Draise and Gates are a couple of liars who want to get even with us..." And now, the telco suddenly has discovered information about Gates' personal life.

- -

FBI/Bell Wiretapping Network? April 3, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

[Edited For This Presentation]

Bob Draise/WB8QCF was an employee of Cincinnati Bell Telephone between 1966 and 1979. He, and others, are involved in a wiretapping scandal of monumental proportions. They say they have installed more than 1,000 wiretaps on the phones of judges, law enforcement officers, lawyers, television personalities, newspaper columnists, labor unions, defense contractors, major corporations (such as Proctor & Gamble and General Electric), politicians (even ex-President Gerald Ford) at the request of Cincinnati police and Cincinnati Bell security supervisors who said the taps were for the police. They were told that many of the taps were for the FBI.

Another radio amateur, Vincent Clark/KB4MIT, a technician for South-Central Bell from 1972 to 1981, said he placed illegal wiretaps similar to those done by Bob Draise on orders from his supervisors -- and on request from local policemen in Louisville, Kentucky.

When asked how he got started in the illegal wiretap business, Bob said that a friend called and asked him to come down to meet with the Cincinnati police. An intelligence sergeant asked Bob about wiretapping some Black Muslims. He also told Bob that Cincinnati Bell security had approved the wiretap -- and that it was for the FBI. The sergeant pointed to his Masonic ring which Bob also wore -- in other words, he was telling the truth under the Masonic oath -- something that Bob put a lot of stock in.

Most of the people first wiretapped were drug or criminal related. Later on, however, it go out of hand -- and the FBI wanted taps on prominent citizens. "We started doing people who had money. How this information was used, I couldn't tell you."

The January 29th "Newsday" said Draise had told investigators that among the taps he rigged from 1972 to 1979 were several on lines used by Wren Business Communications, a Bell competitor. It seems that when Wren had arranged an appointment with a potential customer, they found that Bell had just been there without being called. Wren's president is a ham radio operator, David Stoner/K8LMB.

When spoken with, Dave Stoner said the following;

> "As far as I am concerned, the initial focus for all of this began with the FBI. The FBI apparently set up a structure throughout the United States using apparently the security chiefs of the different Bell companies. They say that there have been other cases in the United States like ours in Cincinnati but they have been localized without the realization of an overall pattern being implicated."
>
> "The things that ties this all together is if you go way back in history to the Hoover period at the FBI, he apparently got together with the AT&T security people. There is an organization that I guess exists to this day with regular meetings of the security people of the different Bell companies. This meant that the FBI

would be able to target a group of 20 or 30 people that represented the security points for all of the Bell and AT&T connections in the United States. I believe the key to all of this goes back to Hoover. The FBI worked through that group who then created the activity at the local level as a result of central planning."

"I believe that in spite of the fact that many people have indicated that this is an early 70's problem -- that there is no disruption to that work to this day. I am pretty much convinced that it is continuing. It looks like a large surveillance effort that Cincinnati was just a part of."

"The federal prosecutor Kathleen Brinkman is in a no-win situation. If she successfully prosecutes this case she is going to bring trouble down upon her own Justice Department. She can't successfully prosecute the case."

About $200 million in lawsuits have already been filed against Cincinnati Bell and the Police Department. Several members of the police department have taken
the Fifth Amendment before the grand jury rather than answer questions about their roles in the wiretapping scheme.

Bob Draise/WB8QCF has filed a suit against Cincinnati Bell for $78 for malicious prosecution and slander in response to a suit filed by Cincinnati Bell against Bob for defamation. Right after they filed the suit, several policemen came forward and admitted to doing illegal wiretaps with them. The Cincinnati police said they stopped this is 1974 -- although another policeman reportedly said they actually stopped the wiretapping in 1986.

Now the CBS-TV program "60 Minutes" is interested in the Cincinnati goings-on and has sent in a team of investigative reporters. Ed Bradley from "60 Minutes" has already interviewed Bob Draise/WB8QCF and it is expected that sometime during this month (April) April, we will see a "60 Minutes" report on spying by the FBI. We also understand that CNN, Ted Turner's Cable News Network, is also working up a "Bugging of America" expose.

Crackdown On Hackers Urged April 9, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%

Taken From the Chicago Tribune (Section 7, Page 12b)

"Make Punishment Fit The Crime," computer leaders say.

DALLAS (AP) -- The legal system has failed to respond adequately to the threat that hackers pose to the computer networks crucial to corporate America, a computer expert says.

Many computer hackers "are given slaps on the wrist," Mark Leary, a senior analyst with International Data Corp., said at a roundtable discussion last week.

"The justice system has to step up...to the fact that these people are malicious and are criminals and are robbing banks just as much as if they walked up with a shotgun," he said.

Other panelists complained that hackers, because of their ability to break into
computer systems, even are given jobs, sometimes a security consultants.

The experts spoke at a roundtable sponsored by Network World magazine, a publication for computer network users and managers.

Computer networks have become crucial to business, from transferring and compiling information to overseeing and running manufacturing processes.

The public also is increasingly exposed to networks through such devices as automatic teller machines at banks, airline reservation systems and computers that store billing information.

Companies became more willing to spend money on computer security after last year's celebrated invasion of a nationwide network by a virus allegedly unleased by a graduate student [Robert Tappen Morris], the experts said.

"The incident caused us to reassess the priorities with which we look at certain threats," said Dennis Steinaur, manager of the computer security management group of the National Institute of Standards and Technology.

But computer security isn't only a matter of guarding against unauthorized entry, said Max Hopper, senior vice president for information systems as American Airlines.

Hopper said American has built a "a Cheyenne mountain-type" installation for its computer systems to guard against a variety of problems, including electrical failure and natural disaster. Referring to the Defense Department's underground nerve center in a Colorado mountain, he said American's precautions even include a three-day supply of food.

"We've done everything we can, we think, to protect the total environment," Hopper said.

Hopper and Steinaur said that despite the high-tech image of computer terrorism, it remains an administrative problem that should be approached as a routine management issue.

But the experts agreed that the greatest danger to computer networks does not come from outside hackers. Instead, they said, the biggest threat is from disgruntled employees or others whose original access to systems was legitimate.

Though employee screening is useful, Steinaur said, it is more important to build into computer systems ways to track unauthorized use and to publicize that hacking can be traced.

Steinaur said growing computer literacy, plus the activities of some non-malicious hackers, help security managers in some respects.

Expanded knowledge "forces us as security managers not be dependent on ignorance," Steinaur said.

"Security needs to be a part of the system, rather than a 'nuisance addition,'" Steinaur said, "and we probably have not done a very good job of making management realize that security is an integral part of the system."

IDC's Leary said the organization surveys of Fortune 1000 companies surprisingly found a significant number of companies were doing little to protect their systems.

The discussion, the first of three planned by Network World, was held because computer sabotage "is a real problem that people aren't aware of," said editor John Gallant. Many business people sophisticated networks."

It also is a problem that many industry vendors are reluctant to address, he said, because it raises questions about a company's reliability.

Typed For PWN by Hatchet Molly

Ex-Worker Charged In Virus Case -- Databases Were Alleged Target Apr 12, 1989

%%

by Jane M. Von Bergen (Philadelphia Inquirer)

A former employee was charged yesterday with infecting his company's computer database in what is believed to be the first computer-virus arrest in the Philadelphia area.

"We believe he was doing this as an act of revenge," said Camden County Assistant Prosecutor Norman Muhlbaier said yesterday, commenting on a motive for the employee who allegedly installed a program to erase databases at his former company, Datacomp Corp. in Voorhees, New Jersey.

Chris Young, 21, of the 2000 block of Liberty Street, Trenton, was charged in Camden County with one count of computer theft by altering a database. Superior Court Judge E. Stevenson Fluharty released Young on his promise to pay $10,000 if he failed to appear in court. If convicted, Young faces a 10-year prison term and a $100,000 fine. Young could not be reached for comment.

"No damage was done," Muhlbaier said, because the company discovered the virus before it could cause harm. Had the virus gone into effect, it could have damaged databases worth several hundred thousand dollars, Muhlbaier said.

Datacomp Corp., in the Echelon Mall, is involved in telephone marketing. The company, which has between 30 and 35 employees, had a contract with a major telephone company to verify the contents of its white pages and try to sell bold-faced or other special listings in the white pages, a Datacomp company spokeswoman said. The database Young is accused of trying to destroy is the list of names from the phone company, she said.

Muhlbaier said that the day Young resigned from the company, October 7, 1988 he used fictitious passwords to obtain entry into the company computer, programming the virus to begin its destruction December 7, 1988 -- Pearl Harbor Day. Young, who had worked for the company on and off for two years -- most recently as a supervisor -- was disgruntled because he had received some unfavorable job-performance reviews, the prosecutor said.

Eventually, operators at the company picked up glitches in the computer system. A programmer, called in to straighten out the mess, noticed that the program had been altered and discovered the data-destroying virus, Muhlbaier said. "What Mr. Young did not know was that the computer system has a lot of security features so they could track it back to a particular date, time and terminal," Muhlbaier said. "We were able to ... prove that he was at that terminal."

Young's virus, Muhlbaier said, is the type known as a "time bomb" because it is programmed to go off at a specific time. In this case, the database would have been sickened the first time someone switched on a computer December 7, he said

Norma Kraus, a vice president of Datacomp's parent company, Volt Information Sciences Inc, said yesterday that the company's potential loss included not only the databases, but also the time it took to find and cure the virus. "All the work has to stop," causing delivery backups on contracts, she said. "We're just fortunate that we have employees who can determine what's wrong and then have the interest to do something. In this case, the employee didn't stop at fixing the system, but continued on to determine what the problem was." The Volt company, based in New York, does $500 million worth of business a year with such services as telephone marketing, data processing and technical support. It also arranges temporary workers, particularly in the data-processing field, and installs telecommunication services, Kraus said.

Mexico's Phone System Going Private? April 17, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

By Oryan QUEST (Special Hispanic Corespondent)

The Mexico Telephone Company, aka Telefonos de Mexico, aka Telmex, is likely to go private in the next year or two. The Mexican government is giving serious consideration to selling its controlling interest in that nation's communications network, despite very stiff opposition from the local unions which would prefer to see the existing bureaucracy stay in place.

The proposed sale, which is part of a move to upgrade the phone system there -- and it *does* need upgrading -- by allowing more private investment, is part of a growing trend in Mexico to privatize heretofore nationalized industries.

The Mexico Telephone Company has spent more than a year planning a $14 billion, five-year restructuring plan which will probably give AT&T and the Bell regional holding companies a role in the improvements.

One plan being discussed by the Mexican government is a complete break-up of Telmex, similar to the court-ordered divestiture of AT&T a few years ago. Under this plan, there would be one central long distance company in Mexico, with the government retaining control of it, but privately owned regional firms providing local and auxiliary services.

Representatives of the Mexican government have talked on more than one occasion with some folks at Southwestern Bell about making a formal proposal. Likewise, Pacific Bell has been making some overtures to the Mexicans. It will be interesting to see what develops.

About two years ago, Teleconnect Magazine, in a humorous article on the divestiture, presented a bogus map of the territories assigned to each BOC,

with Texas, New Mexico and Arizona grouped under an entity called "Taco Bell."

Any phone company which takes over the Mexican system will be an improvement over the current operation, which has been slowly deteriorating for several years.

PS: I *Demand* To Be Let Back On MSP!

_

==Phrack Inc.==

Volume Three, Issue 26, File 11 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        %%%%%%%%%%   %%%%%%%%   %%%%%%%    PWN
PWN                Issue XXVI/Part 3            PWN
PWN                                             PWN
PWN                 April 25, 1989              PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Galactic Hacker Party March 30, 1989
%%%%%%%%%%%%%%%%%%%%

GALACTIC HACKER PARTY
August 2-4, 1989
PARADISO, AMSTERDAM, HOLLAND

During the summer of 1989, the world as we know it will go into overload. An interstellar particle stream of hackers, phone phreaks, radioactivists and assorted technological subversives will be fusing their energies into a media melt-down as the global village plugs into Amsterdam for three electrifying days of information interchange and electronic capers.

Aided by the advanced communications technology to which they are accustomed, the hacker forces will discuss strategies, play games, and generally have a good time. Free access to permanently open on-line facilities will enable them
to keep in touch with home base -- wherever that is.

Those who rightly fear the threat of information tyranny and want to learn what
they can do about it are urgently invited to interface in Amsterdam in August. There will be much to learn from people who know. Celebrity guests with something to say will be present in body or electronic spirit.

The Force must be nurtured. If you are refused transport because your laptop looks like a bomb, cut off behind enemy lines, or unable to attend for any other reason, then join us on the networks. Other hacker groups are requested to organize similar gatherings to coincide with ours. We can provide low-cost international communications links during the conference.

[Despite the wishes of those planning the "Galactic Hacker]
[Party," there will be NO change in plans for SummerCon '89!]

For further information, take up contact as soon as possible with:

HACK-TIC
P.O. box 22953
1100 DL Amsterdam
The Netherlands

tel: +31 20 6001480

PARADISO
Weteringschans 6-8
1017 SG Amsterdam
The Netherlands

tel: +31 20 264521 / +31 20 237348

Subversive Bulletin Boards March 26, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%

An article in a newspaper from the United Kingdom had an article relating to a computer bulletin board being run by a 14-year-old boy in Wilmslow, Cheshire, England. It contained information relating to such things as making plastic explosives.

Anti-terrorist detectives are said to be investigating for possible breaches of the Obscene Publications Act. Apparently reporters were able to easily gain access to this bulletin board and peruse articles on such subjects as credit card fraud, making various types of explosives, street fighting techniques and dodging police radar traps.

One article was obviously aimed at children and described how to make a bomb suitable for use on "the car of a teacher you do not like at school," which would destroy the tire of a car when it was started.

The boy's parents did not seem to think that their son was doing anything wrong, preferring him to be working with his computer rather than roaming the streets.

A London computer consultant, Noel Bradford, is quoted as having seen the bulletin board and found messages discussing "how to crack British Telecom, how to get money out of people and how to defraud credit card companies. Credit card numbers are given, along with PIN numbers, names, addresses and other details."

Tale Of TWO TAP Magazines! April 24, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%

It seemed inevitable that the battle for the rights to TAP would come into play, but many wonder why it has taken so long.

The Renegade Chemist, long time member of Phortune 500 and one of its "Board Of Directors," has been talking about re-starting TAP Magazine for at least two years... nothing ever happened with it until now. TRC claims that the TAP Magazine crew in Kentucky is just a fraud and that he is putting on the "REAL McCoy."

For a free issue of The Renegade Chemist's TAP Magazine, send a self-addressed stamped envelope to:

Data Security Consultants, Inc.
TAP Magazine
P.O. Box 271
South Windam, CT 06266-0271

Now on the other hand, Aristotle of the Kentucky based TAP Magazine has shown an almost uncaring attitude about The Renegade Chemist's statements about TAP Magazine. He says that he does not "really mind if these people put out a magazine. Honestly I just want to help the community and the more magazines and information, the better."

The really big news about the Kentucky based TAP Magazine came Saturday, April 22, 1989. Apparently, because of problems with local banks and the Internal Revenue Service, TAP Magazine is now FREE!

The only catch is that if you want it, you have to send them a self-addressed stamped envelope to get each issue or "you can send cash, but only enough to pay for postage, 25 cents should cover it." Do not send any kinds of checks and/or money orders. Anyone who did will be receiving their checks back or at least those checks will not be cashed. The TAP Magazine staff will be taking care of the printing costs out of their own pocket.

So for the FREE TAP Magazine, send a self-addressed stamped envelope to:

P.O. Box 20264
Louisville, KY 40220

Issue 93 is due for the end of April 1989, but Aristotle also wanted me to let everyone know that he will be attending SummerCon '89 and bringing with him plenty of issues of all the TAPs that he, Olorin The White, and Predat0r have published.

As I have not seen TRC's TAP, I make no judgements. Instead, get a copy of both TAPs FREE and compare them yourself. The market will decide which TAP will continue.

Information Provided by
Aristotle and The Renegade Chemist

Computer Group Wary Of Security Agency April 11, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Taken from the San Francisco Chronicle

A public interest group said yesterday that the National Security Agency, the nation's biggest intelligence agency, could exert excessive control over a program to strengthen the security of computer systems throughout the federal government.

The group, Computer Professionals for Social Responsibility -- based in Palo Alto -- urged key members of Congress to focus "particularly close scrutiny" on
the agency's role in helping to implement legislation aimed at safeguarding sensitive but unclassified information in federal computers.

"There is a constant risk that the federal agencies, under the guise of enhancing computer security, may find their programs -- to the extent that they
rely upon computer systems -- increasingly under the supervision of the largest
and most secretive intelligence organization in the country," it said.

Verifying Social Security Numbers April 11, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Taken From The New York Times

Dorcas R. Hardy, Commisssioner of the Social Security Administration, told a

Congressional committee that the agency had verified millions of SSN's for private credit companies.

TRW, the nation's largest credit reporting company, recently proposed paying the Social Security Administration $1,000,000 to have 140 million numbers verified.

Phil Gambino, an agency spokesman, reported last month that the agency had verified social security numbers only at the request of beneficiaries or employers and had never verified more than 25 numbers at a time. He said such disclosures were required under the Freedom of Information Act.

At the hearing yesterday, Dorcas R. Hardy, denied any other verifications at first. However, she later admitted that in the early 1980s, 3,000,000 social security numbers were verified for CitiCorp and that last year 151,000 numbers were verified for TRW. Ms. Hardy said that the 151,000 numbers were just part of a "test run."

Senator David Pryor, a democrat from Arkansas and chairman of the Special Committee on Aging, said that previous commissioners; the Congressional Research Service of the Library of Congress, and Donald A. Gonya, chief counsel
for Social Security have all decided that such verification is illegal.

PWN Quicknotes

1. Prank Virus Warning Message (March 28, 1989) -- An individual placed a time
bomb message on a government service system in the San Francisco Bay Area saying, "WARNING! A computer virus has infected the system!" The individual is learning that such a prank is considered almost as funny as saying that you have a bomb in your carry-on luggage as you board a plane.
-- Bruce Baker, Information Security Program, SRI International

- -

2. Hackers' Dictionary In Japanese? (March 30, 1989) -- What is this you ask? This amusing compilation was put together a decade or so ago by artificial intelligence (AI) graduate students at Stanford, MIT, and Carnegie-Mellon and recorded the then-current vernacular of their shared cultures. They did it for fun, but it somehow ended up getting published.

   The Hackers' Dictionary contains more than a few puns, jokes, and other things that are hard to translate such as "moby," as in "moby memory", or "fubar" and its regional variants "foo bar" and "foo baz."

- -

3. AT&T's Air Force -- AT&T has an air force that patrols its cable routes, some routes 24 hours a day, 365 days a year. The AT&T air force includes helicopters and fixed-wing aircraft. For some areas, AT&T uses infantry and armored cars. AT&T's Sue Fleming says, "We hope NOT to find any activity. We don't want to 'catch' people. But if we do spot a digging crew, the usual procedure is for the pilot to radio the location back to a ground crew, who check it out. On occasion, they drop notes -- or even land -- but that depends on where the site is. In some areas -- like New Jersey -- unauthorized landings bring heavy penalties."

- -

4. Terrorist Threat? -- Scientific advisors to the government told a Senate panel that telecommunications networks are tempting targets for terrorist

activity. The experts said that advances in technology -- like fiber optics, which concentrates equipment and data -- and the fragmentation of the telecom industry after divestiture are reasons for the increased risk. Certainly the Hinsdale, Illinois CO fire and the recent severing of a fiber backbone in New Jersey have shown us all how vulnerable our country's telecom network is.

- -

5. FCC Rules On AOS -- The FCC has ruled on a complaint filed this summer by two consumer groups against five Alternative Operator Services (AOS) companies. The FCC found the complaint valid and has ordered the AOS companies to stop certain practices immediately.

   The ruling states that callers must be told when their calls are being handled by an AOS, operators must provide callers with rate information and hotel or payphone owners cannot block calls to other long distance carriers. (Callers who don't take any special action when making a call will still be routed to the pre-subscribed carrier.)

   The FCC has also ordered the companies to eliminate "splashing" whenever technically feasible. Splashing is transferring a call to a distant carrier point-of-presence and charging the caller for the call from that point.

- -

6. Cool New Service -- CompuServe (the world's biggest computer bulletin board) users can now dial in and search and find articles from a bunch of different technical trade magazines. The database was put together by an outfit called Information Access Company. It currently contains full-text articles for 50 publications and paraphrased abstracts for 75 more. Most coverage begins with the January 1987 issues.

   You can search the publications by magazine name, author, key word, key phrase, etc., then pull up the abstracts of the article of interest and, if needed and when available, get the full text of the article. And it's easy to use.

   Charge for the service is $24 per hour, $1 for each abstract, and $1.50 for each full-text article accessed. CompuServe charges $12.50 per hour for connect time. Both per hour charges are pro-rated, and, with the databases being so easy to use, you'll rarely be on the board for more than 10-15 minutes, so those costs will drop.

CompuServe	800-848-8199
Information Access	800-227-8431

- -

7. ISDN Calling Number Identification Services (April 7, 1989) -- Bellcore Technical Reference TR-TSY-000860, "ISDN Calling Number Identification Services" can be purchased for $46 from:

Bellcore
Customer Service
60 New England Ave
Piscataway, NJ 08854-4196

(201) 699-5800

This Technical Reference contains Bellcore's view of generic requirements for support of ISDN Calling Number Identification (I-CNIS). The I-CNIS feature extends the concepts of Calling Number Delivery and Calling Number Delivery Blocking to ISDN lines. I-CNIS also allows the customer to specify which Directory Number (DN) should be used for each outgoing call and provides network screening to ensure that the specified DN is valid. I-CNIS handles calling number processing for both circuit-mode and packet-mode ISDN calls and provides four component features: Number Provision, Number Screening, Number Privacy, and Number Delivery. Material on Privacy Change by the calling party and Privacy Override by the called party is also included.

- -

8. Founder of TAP Magazine, Abbie Hoffman, born in 1936, passed away on April 12, 1989. He was found dead in his apartment in New Hope, PA. He was fully dressed under the bedcovers. An autopsy was inconclusive. An article about him appears in the April 24, 1989 issue of Time Magazine, "A Flower in a Clenched Fist," page 23.

- -

9. Bill Landreth aka The Cracker, author of Out Of The Inner Circle, has reappeared. Supposedly, he is now working as a bookbinder in Orange County, California and living with the sysop of a bulletin board called the "Pig Sty." -- Dark Sorcerer (April 19, 1989)

- -

10. Hacker/Phreaker Gets "Stiff" Penalty (Green Bay, Wisconsin) -- David Kelsey, aka Stagehand, plead guilty to two counts of class "E" felonies and received a 90 day jail term. Once he has completed his jail term, he will serve three years probation and an unknown amount of community service hours.

In addition to these penalties, Stagehand must also pay restitution of $511.00 to Schneider Communications of Green Bay, Wisconsin. Stagehand was given all his computer equipment back as part of the plea bargain -- minus any materials considered to be "ill gotten" gains.

_
! r¢¢

1:30:22 p.m.   ARE YOU STILL THERE ?
! r¢¢

1:35:22 p.m.   RESPOND OR BE LOGGED OFF
!

y
supervisors who said the taps were for the police. They were told that many of the taps were for the FBI.

Another radio amateur, Vincent Clark/KB4MIT, a technician for South-Central Bell from 1972 to 1981, said he placed illegal wiretaps similar to those done by Bob Draise on orders from his supervisors -- and on request from local policemen in Louisville, Kentucky.

When asked how he got started in the illegal wiretap business, Bob said that a friend called and asked him to come down to meet with the Cincinnati police. An intelligence sergeant asked Bob about wiretapping some Black Muslims. He also told Bob that Cincinnati Bell security had approved the wiretap -- and that it was for the FBI. The sergeant pointed to his Masonic ring which Bob also wore -- in other words, he was telling the truth under the Masonic oath -- something that Bob put a lot of stock in.

Most of the people first wiretapped were drug or criminal related. Later on, however, it go out of hand -- and the FBI wanted taps on prominent citizens. "We started doing people who had money. How this information was used, I couldn't tell you."

The January 29th "Newsday" said Draise had told investigators that among the taps he rigged from 1972 to 1979 were several on lines used by Wren Business Communications, a Bell competitor. It seems that when Wren had arranged an appointment with a potential customer, they found that Bell had just been there without being called. Wren's president is a ham radio operator, David Stoner/K8LMB.

When spoken with, Dave Stoner said the following;

> "As far as I am concerned, the initial focus for all of this began with the FBI. The FBI apparently set up a structure throughout the United States using apparently the security chiefs of the different Bell companies. They say that there have been other cases in the United States like ours in Cincinnati but they have been localized without the realization of an overall pattern being implicated."
>
> "The things that ties this all together is if you go way back in history to the Hoover period at the FBI, he apparently got together with the AT&T security people. There is an organization that I guess exists to this day with regular meetings of the security people of the different Bell companies. This meant that the FBI would be able to target a group of 20 or 30 people that represented the security points for all of the Bell and AT&T connections in the United States. I believe the key to all of this goes back to Hoover. The FBI worked through that group who then created the activity at the local level as a result of central planning."
>
> "I believe that in spite of the fact that many people have indicated that this is an early 70's problem -- that there is no disruption to that work to this day. I am pretty much convinced that it is continuing. It looks like a large surveillance effort that Cincinnati was just a part of."
>
> "The federal prosecutor Kathleen Brinkman is in a no-win situation. If she successfully prosecutes this case she is going to bring trouble down upon her own Justice Department. She can't successfully prosecute the case."

About $200 million in lawsuits have already been filed against Cincinnati Bell and the Police Department. Several members of the police department have taken the Fifth Amendment before the grand jury rather than answer questions about their roles in the wiretapping scheme.

Bob Draise/WB8QCF has filed a suit against Cincinnati Bell for $78 for malicious prosecution and slander in response to a suit filed by Cincinnati Bell against Bob for defamation. Right after they filed the suit, several policemen came forward and admitted to doing illegal wiretaps with them. The Cincinnati police said they stopped this is 1974 -- although another policeman reportedly said they actually stopped the wiretapping in 1986.

Now the CBS-TV program "60 Minutes" is interested in the Cincinnati goings-on and has sent in a team of investigative reporters. Ed Bradley from "60 Minutes" has already interviewed Bob Draise/WB8QCF and it is expected that sometime during this month (April) April, we will see a "60 Minutes" report on spying by the FBI. We also understand that CNN, Ted Turner's Cable News Network, is also working up a "Bugging of America" expose.

Crackdown On Hackers Urged April 9, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%

Taken From the Chicago Tribune (Section 7, Page 12b)

"Make Punishment Fit The Crime," computer leaders say.

DALLAS (AP) -- The legal system has failed to respond adequately to the threat that hackers pose to the computer networks crucial to corporate America, a computer expert says.

Many computer hackers "are given slaps on the wrist," Mark Leary, a senior analyst with International Data Corp., said at a roundtable discussion last week.

"The justice system has to step up...to the fact that these people are malicious and are criminals and are robbing banks just as much as if they walked up with a shotgun," he said.

Other panelists complained that hackers, because of their ability to break into
computer systems, even are given jobs, sometimes a security consultants.

The experts spoke at a roundtable sponsored by Network World magazine, a publication for computer network users and managers.

Computer networks have become crucial to business, from transferring and compiling information to overseeing and running manufacturing processes.

The public also is increasingly exposed to networks through such devices as automatic teller machines at banks, airline reservation systems and computers that store billing information.

Companies became more willing to spend money on computer security after last year's celebrated invasion of a nationwide network by a virus allegedly unleased by a graduate student [Robert Tappen Morris], the experts said.

"The incident caused us to reassess the priorities with which we look at certain threats," said Dennis Steinaur, manager of the computer security management group of the National Institute of Standards and Technology.

But computer security isn't only a matter of guarding against unauthorized entry, said Max Hopper, senior vice president for information systems as American Airlines.

Hopper said American has built a "a Cheyenne mountain-type" installation for its computer systems to guard against a variety of problems, including electrical failure and natural disaster. Referring to the Defense Department's underground nerve center in a Colorado mountain, he said American's precautions even include a three-day supply of food.

"We've done everything we can, we think, to protect the total environment," Hopper said.

Hopper and Steinaur said that despite the high-tech image of computer terrorism, it remains an administrative problem that should be approached as a routine management issue.

But the experts agreed that the greatest danger to computer networks does not come from outside hackers. Instead, they said, the biggest threat is from disgruntled employees or others whose original access to systems was legitimate.

Though employee screening is useful, Steinaur said, it is more important to build into computer systems ways to track unauthorized use and to publicize that hacking can be traced.

Steinaur said growing computer literacy, plus the activities of some non-malicious hackers, help security managers in some respects.

Expanded knowledge "forces us as security managers not be dependent on ignorance," Steinaur said.

"Security needs to be a part of the system, rather than a 'nuisance addition,'" Steinaur said, "and we probably have not done a very good job of making management realize that security is an integral part of the system."

IDC's Leary said the organization surveys of Fortune 1000 companies surprisingly found a significant number of companies were doing little to protect their systems.

The discussion, the first of three planned by Network World, was held because computer sabotage "is a real problem that people aren't aware of," said editor John Gallant. Many business people sophisticated networks."

It also is a problem that many industry vendors are reluctant to address, he said, because it raises questions about a company's reliability.

Typed For PWN by Hatchet Molly

Ex-Worker Charged In Virus Case -- Databases Were Alleged Target Apr 12, 1989

%%

by Jane M. Von Bergen (Philadelphia Inquirer)

A former employee was charged yesterday with infecting his company's computer database in what is believed to be the first computer-virus arrest in the Philadelphia area.

"We believe he was doing this as an act of revenge," said Camden County Assistant Prosecutor Norman Muhlbaier said yesterday, commenting on a motive

for the employee who allegedly installed a program to erase databases at his former company, Datacomp Corp. in Voorhees, New Jersey.

Chris Young, 21, of the 2000 block of Liberty Street, Trenton, was charged in Camden County with one count of computer theft by altering a database. Superior Court Judge E. Stevenson Fluharty released Young on his promise to pay $10,000 if he failed to appear in court. If convicted, Young faces a 10-year prison term and a $100,000 fine. Young could not be reached for comment.

"No damage was done," Muhlbaier said, because the company discovered the virus before it could cause harm. Had the virus gone into effect, it could have damaged databases worth several hundred thousand dollars, Muhlbaier said.

Datacomp Corp., in the Echelon Mall, is involved in telephone marketing. The company, which has between 30 and 35 employees, had a contract with a major telephone company to verify the contents of its white pages and try to sell bold-faced or other special listings in the white pages, a Datacomp company spokeswoman said. The database Young is accused of trying to destroy is the list of names from the phone company, she said.

Muhlbaier said that the day Young resigned from the company, October 7, 1988 he used fictitious passwords to obtain entry into the company computer, programming the virus to begin its destruction December 7, 1988 -- Pearl Harbor Day. Young, who had worked for the company on and off for two years -- most recently as a supervisor -- was disgruntled because he had received some unfavorable job-performance reviews, the prosecutor said.

Eventually, operators at the company picked up glitches in the computer system. A programmer, called in to straighten out the mess, noticed that the program had been altered and discovered the data-destroying virus, Muhlbaier said. "What Mr. Young did not know was that the computer system has a lot of security features so they could track it back to a particular date, time and terminal," Muhlbaier said. "We were able to ... prove that he was at that terminal." Young's virus, Muhlbaier said, is the type known as a "time bomb" because it is programmed to go off at a specific time. In this case, the database would have been sickened the first time someone switched on a computer December 7, he said

Norma Kraus, a vice president of Datacomp's parent company, Volt Information Sciences Inc, said yesterday that the company's potential loss included not only the databases, but also the time it took to find and cure the virus. "All the work has to stop," causing delivery backups on contracts, she said. "We're just fortunate that we have employees who can determine what's wrong and then have the interest to do something. In this case, the employee didn't stop at fixing the system, but continued on to determine what the problem was." The Volt company, based in New York, does $500 million worth of business a year with such services as telephone marketing, data processing and technical support. It also arranges temporary workers, particularly in the data-processing field, and installs telecommunication services, Kraus said.

Mexico's Phone System Going Private? April 17, 1989
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
By Oryan QUEST (Special Hispanic Corespondent)

The Mexico Telephone Company, aka Telefonos de Mexico, aka Telmex, is likely to go private in the next year or two. The Mexican government is giving serious consideration to selling its controlling interest in that nation's communications network, despite very stiff opposition from the local unions which would prefer to see the existing bureaucracy stay in place.

The proposed sale, which is part of a move to upgrade the phone system there -- and it *does* need upgrading -- by allowing more private investment, is part of a growing trend in Mexico to privatize heretofore nationalized industries.

The Mexico Telephone Company has spent more than a year planning a $14 billion, five-year restructuring plan which will probably give AT&T and the Bell regional holding companies a role in the improvements.

One plan being discussed by the Mexican government is a complete break-up of Telmex, similar to the court-ordered divestiture of AT&T a few years ago. Under this plan, there would be one central long distance company in Mexico, with the government retaining control of it, but privately owned regional firms providing local and auxiliary services.

Representatives of the Mexican government have talked on more than one occasion with some folks at Southwestern Bell about making a formal proposal. Likewise, Pacific Bell has been making some overtures to the Mexicans. It will be interesting to see what develops.

About two years ago, Teleconnect Magazine, in a humorous article on the divestiture, presented a bogus map of the territories assigned to each BOC, with Texas, New Mexico and Arizona grouped under an entity called "Taco Bell."

Any phone company which takes over the Mexican system will be an improvement over the current operation, which has been slowly deteriorating for several years.

PS: I *Demand* To Be Let Back On MSP!

==Phrack Inc.==

Volume Three, Issue 26, File 11 of 11

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN
PWN P h r a c k W o r l d N e w s PWN
PWN %%%%%%%%%%% %%%%%%%%% %%%%%%% PWN
PWN Issue XXVI/Part 3 PWN
PWN PWN
PWN April 25, 1989 PWN
PWN PWN
PWN Created, Written, and Edited PWN

PWN by Knight Lightning PWN
PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

Galactic Hacker Party March 30, 1989
%%%%%%%%%%%%%%%%%%%%%

GALACTIC HACKER PARTY
August 2-4, 1989
PARADISO, AMSTERDAM, HOLLAND

During the summer of 1989, the world as we know it will go into overload. An interstellar particle stream of hackers, phone phreaks, radioactivists and assorted technological subversives will be fusing their energies into a media melt-down as the global village plugs into Amsterdam for three electrifying days of information interchange and electronic capers.

Aided by the advanced communications technology to which they are accustomed, the hacker forces will discuss strategies, play games, and generally have a good time. Free access to permanently open on-line facilities will enable them
to keep in touch with home base -- wherever that is.

Those who rightly fear the threat of information tyranny and want to learn what
they can do about it are urgently invited to interface in Amsterdam in August. There will be much to learn from people who know. Celebrity guests with something to say will be present in body or electronic spirit.

The Force must be nurtured. If you are refused transport because your laptop looks like a bomb, cut off behind enemy lines, or unable to attend for any other reason, then join us on the networks. Other hacker groups are requested to organize similar gatherings to coincide with ours. We can provide low-cost international communications links during the conference.

[Despite the wishes of those planning the "Galactic Hacker]
[Party," there will be NO change in plans for SummerCon '89!]

For further information, take up contact as soon as possible with:

HACK-TIC
P.O. box 22953
1100 DL Amsterdam
The Netherlands

tel: +31 20 6001480

PARADISO
Weteringschans 6-8
1017 SG Amsterdam
The Netherlands

tel: +31 20 264521 / +31 20 237348

Subversive Bulletin Boards March 26, 1989
%%%%%%%%%%%%%%%%%%%%%%%%%

An article in a newspaper from the United Kingdom had an article relating to a computer bulletin board being run by a 14-year-old boy in Wilmslow, Cheshire, England. It contained information relating to such things as making plastic explosives.

Anti-terrorist detectives are said to be investigating for possible breaches of
the Obscene Publications Act. Apparently reporters were able to easily gain

access to this bulletin board and peruse articles on such subjects as credit card fraud, making various types of explosives, street fighting techniques and dodging police radar traps.

One article was obviously aimed at children and described how to make a bomb suitable for use on "the car of a teacher you do not like at school," which would destroy the tire of a car when it was started.

The boy's parents did not seem to think that their son was doing anything wrong, preferring him to be working with his computer rather than roaming the streets.

A London computer consultant, Noel Bradford, is quoted as having seen the bulletin board and found messages discussing "how to crack British Telecom, how
to get money out of people and how to defraud credit card companies. Credit card numbers are given, along with PIN numbers, names, addresses and other details."

Tale Of TWO TAP Magazines! April 24, 1989

%%%%%%%%%%%%%%%%%%%%%%%%

It seemed inevitable that the battle for the rights to TAP would come into play, but many wonder why it has taken so long.

The Renegade Chemist, long time member of Phortune 500 and one of its "Board Of
Directors," has been talking about re-starting TAP Magazine for at least two years... nothing ever happened with it until now. TRC claims that the TAP Magazine crew in Kentucky is just a fraud and that he is putting on the "REAL McCoy."

For a free issue of The Renegade Chemist's TAP Magazine, send a self-addressed stamped envelope to:

Data Security Consultants, Inc.
TAP Magazine
P.O. Box 271
South Windam, CT 06266-0271

Now on the other hand, Aristotle of the Kentucky based TAP Magazine has shown an almost uncaring attitude about The Renegade Chemist's statements about TAP Magazine. He says that he does not "really mind if these people put out a magazine. Honestly I just want to help the community and the more magazines and information, the better."

The really big news about the Kentucky based TAP Magazine came Saturday, April 22, 1989. Apparently, because of problems with local banks and the Internal Revenue Service, TAP Magazine is now FREE!

The only catch is that if you want it, you have to send them a self-addressed stamped envelope to get each issue or "you can send cash, but only enough to pay for postage, 25 cents should cover it." Do not send any kinds of checks and/or money orders. Anyone who did will be receiving their checks back or at least those checks will not be cashed. The TAP Magazine staff will be taking care of the printing costs out of their own pocket.

So for the FREE TAP Magazine, send a self-addressed stamped envelope to:

P.O. Box 20264
Louisville, KY 40220

Issue 93 is due for the end of April 1989, but Aristotle also wanted me to let everyone know that he will be attending SummerCon '89 and bringing with him plenty of issues of all the TAPs that he, Olorin The White, and Predat0r have published.

As I have not seen TRC's TAP, I make no judgements. Instead, get a copy of both TAPs FREE and compare them yourself. The market will decide which TAP will continue.

Information Provided by
Aristotle and The Renegade Chemist

Computer Group Wary Of Security Agency April 11, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Taken from the San Francisco Chronicle

A public interest group said yesterday that the National Security Agency, the nation's biggest intelligence agency, could exert excessive control over a program to strengthen the security of computer systems throughout the federal government.

The group, Computer Professionals for Social Responsibility -- based in Palo Alto -- urged key members of Congress to focus "particularly close scrutiny" on
the agency's role in helping to implement legislation aimed at safeguarding sensitive but unclassified information in federal computers.

"There is a constant risk that the federal agencies, under the guise of enhancing computer security, may find their programs -- to the extent that they
rely upon computer systems -- increasingly under the supervision of the largest
and most secretive intelligence organization in the country," it said.

Verifying Social Security Numbers April 11, 1989

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Taken From The New York Times

Dorcas R. Hardy, Commisssioner of the Social Security Administration, told a Congressional committee that the agency had verified millions of SSN's for private credit companies.

TRW, the nation's largest credit reporting company, recently proposed paying the Social Security Administration $1,000,000 to have 140 million numbers verified.

Phil Gambino, an agency spokesman, reported last month that the agency had verified social security numbers only at the request of beneficiaries or employers and had never verified more than 25 numbers at a time. He said such disclosures were required under the Freedom of Information Act.

At the hearing yesterday, Dorcas R. Hardy, denied any other verifications at

first. However, she later admitted that in the early 1980s, 3,000,000 social security numbers were verified for CitiCorp and that last year 151,000 numbers were verified for TRW. Ms. Hardy said that the 151,000 numbers were just part of a "test run."

Senator David Pryor, a democrat from Arkansas and chairman of the Special Committee on Aging, said that previous commissioners; the Congressional Research Service of the Library of Congress, and Donald A. Gonya, chief counsel
for Social Security have all decided that such verification is illegal.

PWN Quicknotes

1. Prank Virus Warning Message (March 28, 1989) -- An individual placed a time bomb message on a government service system in the San Francisco Bay Area saying, "WARNING! A computer virus has infected the system!" The individual is learning that such a prank is considered almost as funny as saying that you have a bomb in your carry-on luggage as you board a plane.
   -- Bruce Baker, Information Security Program, SRI International

- -

2. Hackers' Dictionary In Japanese? (March 30, 1989) -- What is this you ask? This amusing compilation was put together a decade or so ago by artificial intelligence (AI) graduate students at Stanford, MIT, and Carnegie-Mellon and recorded the then-current vernacular of their shared cultures. They did it for fun, but it somehow ended up getting published.

   The Hackers' Dictionary contains more than a few puns, jokes, and other things that are hard to translate such as "moby," as in "moby memory", or "fubar" and its regional variants "foo bar" and "foo baz."

- -

3. AT&T's Air Force -- AT&T has an air force that patrols its cable routes, some routes 24 hours a day, 365 days a year. The AT&T air force includes helicopters and fixed-wing aircraft. For some areas, AT&T uses infantry and armored cars. AT&T's Sue Fleming says, "We hope NOT to find any activity. We don't want to 'catch' people. But if we do spot a digging crew, the usual procedure is for the pilot to radio the location back to a ground crew, who check it out. On occasion, they drop notes -- or even land -- but that depends on where the site is. In some areas -- like New Jersey -- unauthorized landings bring heavy penalties."

- -

4. Terrorist Threat? -- Scientific advisors to the government told a Senate panel that telecommunications networks are tempting targets for terrorist activity. The experts said that advances in technology -- like fiber optics, which concentrates equipment and data -- and the fragmentation of the telecom industry after divestiture are reasons for the increased risk. Certainly the Hinsdale, Illinois CO fire and the recent severing of a fiber backbone in New Jersey have shown us all how vulnerable our country's telecom network is.

- -

5. FCC Rules On AOS -- The FCC has ruled on a complaint filed this summer by two consumer groups against five Alternative Operator Services (AOS) companies. The FCC found the complaint valid and has ordered the AOS companies to stop certain practices immediately.

The ruling states that callers must be told when their calls are being handled by an AOS, operators must provide callers with rate information and hotel or payphone owners cannot block calls to other long distance carriers. (Callers who don't take any special action when making a call will still be routed to the pre-subscribed carrier.)

The FCC has also ordered the companies to eliminate "splashing" whenever technically feasible. Splashing is transferring a call to a distant carrier point-of-presence and charging the caller for the call from that point.

- -

6. Cool New Service -- CompuServe (the world's biggest computer bulletin board) users can now dial in and search and find articles from a bunch of different technical trade magazines. The database was put together by an outfit called Information Access Company. It currently contains full-text articles for 50 publications and paraphrased abstracts for 75 more. Most coverage begins with the January 1987 issues.

You can search the publications by magazine name, author, key word, key phrase, etc., then pull up the abstracts of the article of interest and, if needed and when available, get the full text of the article. And it's easy to use.

Charge for the service is $24 per hour, $1 for each abstract, and $1.50 for each full-text article accessed. CompuServe charges $12.50 per hour for connect time. Both per hour charges are pro-rated, and, with the databases being so easy to use, you'll rarely be on the board for more than 10-15 minutes, so those costs will drop.

CompuServe	800-848-8199
Information Access	800-227-8431

- -

7. ISDN Calling Number Identification Services (April 7, 1989) -- Bellcore Technical Reference TR-TSY-000860, "ISDN Calling Number Identification Services" can be purchased for $46 from:

Bellcore
Customer Service
60 New England Ave
Piscataway, NJ 08854-4196
(201) 699-5800

This Technical Reference contains Bellcore's view of generic requirements for support of ISDN Calling Number Identification (I-CNIS). The I-CNIS feature extends the concepts of Calling Number Delivery and Calling Number Delivery Blocking to ISDN lines. I-CNIS also allows the customer to specify which Directory Number (DN) should be used for each outgoing call and provides network screening to ensure that the specified DN is valid. I-CNIS handles calling number processing for both circuit-mode and packet-mode ISDN calls and provides four component features: Number Provision, Number Screening, Number Privacy, and Number Delivery. Material on Privacy Change by the calling party and Privacy Override by the called

party is also included.

\- -
\-

8. Founder of TAP Magazine, Abbie Hoffman, born in 1936, passed away on April 12, 1989. He was found dead in his apartment in New Hope, PA. He was fully dressed under the bedcovers. An autopsy was inconclusive. An article about him appears in the April 24, 1989 issue of Time Magazine, "A Flower in a Clenched Fist," page 23.

\- -
\-

9. Bill Landreth aka The Cracker, author of Out Of The Inner Circle, has reappeared. Supposedly, he is now working as a bookbinder in Orange County, California and living with the sysop of a bulletin board called the "Pig Sty." -- Dark Sorcerer (April 19, 1989)

\- -
\-

10. Hacker/Phreaker Gets "Stiff" Penalty (Green Bay, Wisconsin) -- David Kelsey, aka Stagehand, plead guilty to two counts of class "E" felonies and received a 90 day jail term. Once he has completed his jail term, he will serve three years probation and an unknown amount of community service hours.

    In addition to these penalties, Stagehand must also pay restitution of $511.00 to Schneider Communications of Green Bay, Wisconsin. Stagehand was given all his computer equipment back as part of the plea bargain -- minus any materials considered to be "ill gotten" gains.

! r¢¢

1:30:22 p.m.   ARE YOU STILL THERE ?
! r¢¢

1:35:22 p.m.   RESPOND OR BE LOGGED OFF
!