Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-24
Title:	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
Publication Date(s):	April 2001
Withdrawal Date:	August 1, 2018
Withdrawal Note:	Does not address newer technologies, such as Voice Over IP (VOIP); includes references to "security controls" that pre-date SP 800-53.

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	
Title:	
Author(s):	
Publication Date(s):	
URL/DOI:	

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Laboratory)
Latest revision of the attached publication:	
Related information:	https://csrc.nist.gov/publications
Withdrawal announcement (link):	https://csrc.nist.gov/news/2018/nist-to-withdraw-eleven-outdated-sp-800-pubs

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Date updated: August 1, 2018

NIST Special Publication 800-24

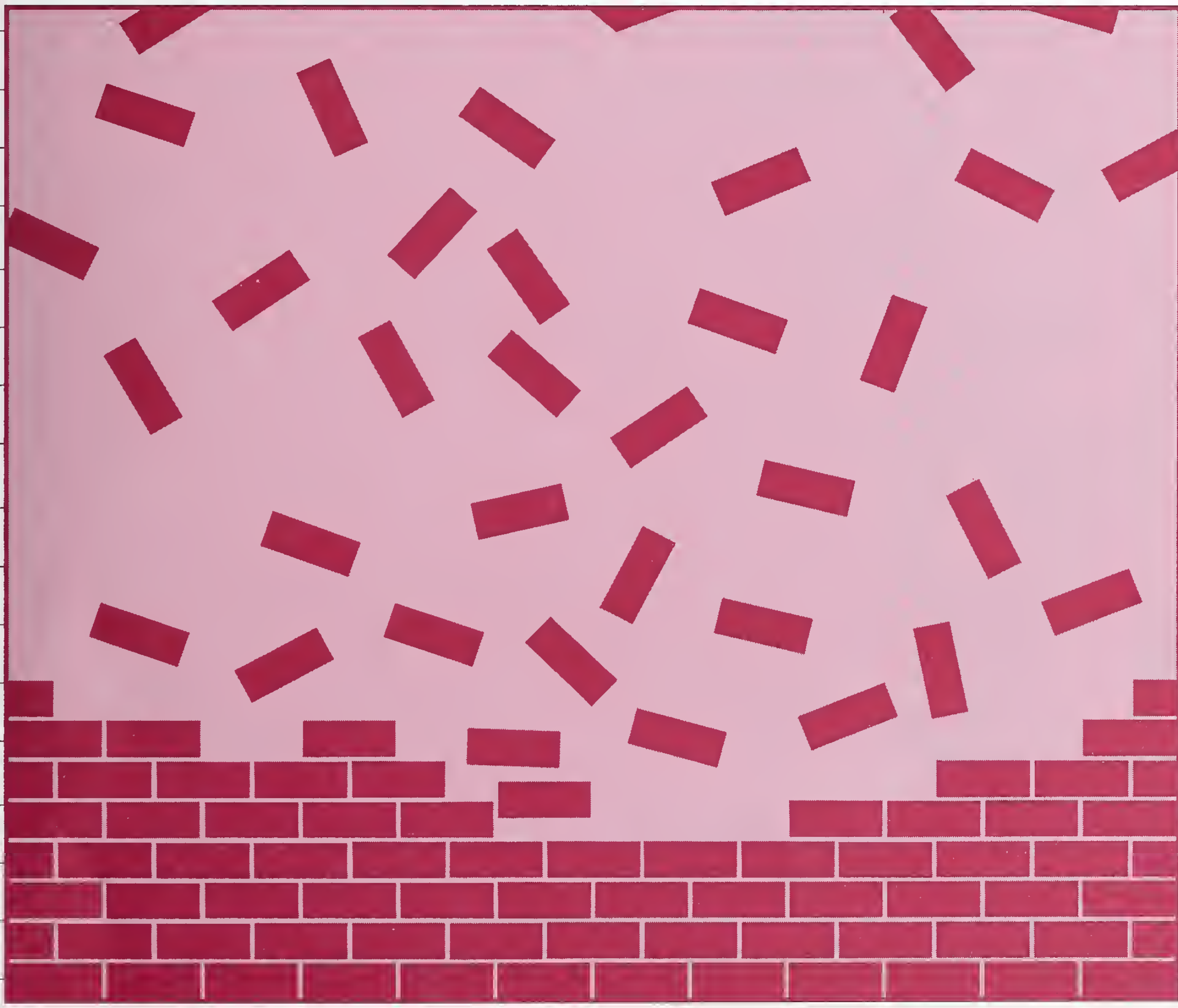
PBX Vulnerability Analysis

Finding Holes in Your PBX Before Someone Else Does

D. Richard Kuhn

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

COMPUTER SECURITY



NIST CENTENNIAL 1901-2001

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

Office of the Director
- National Quality Program
- International and Academic Affairs

Technology Services
- Standards Services
- Technology Partnerships
- Measurement Services
- Information Services

Advanced Technology Program
- Economic Assessment
- Information Technology and Applications
- Chemistry and Life Sciences
- Materials and Manufacturing Technology
- Electronics and Photonics Technology

Manufacturing Extension Partnership Program
- Regional Programs
- National Programs
- Program Development

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Radio-Frequency Technology[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- NIST Center for Neutron Research

Chemical Science and Technology Laboratory
- Biotechnology
- Physical and Chemical Properties[2]
- Analytical Chemistry
- Process Measurements
- Surface and Microanalysis Science

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Optical Technology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Manufacturing Metrology
- Intelligent Systems
- Fabrication Technology
- Manufacturing Systems Integration

Building and Fire Research Laboratory
- Applied Economics
- Structures
- Building Materials
- Building Environment
- Fire Safety Engineering
- Fire Science

Information Technology Laboratory
- Mathematical and Computational Sciences[2]
- Advanced Network Technologies
- Computer Security
- Information Access
- Convergent Information Systems
- Information Services and Computing
- Software Diagnostics and Conformance Testing
- Statistical Engineering

[1]At Boulder, CO 80303.
[2]Some elements at Boulder, CO.

NIST Special Publication 800-24

PBX Vulnerability Analysis

Finding Holes in Your PBX Before Someone Else Does

D. Richard Kuhn

COMPUTER SECURITY

Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Karen H. Brown, Acting Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Karen H. Brown, Acting Director

Reports on Information Security Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology. ITL develops tests, test methods, reference data, proof of concept implementations and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-24
Natl. Inst. Stand. Technol. Spec. Publ. 800-24, 64 pages (April 2001)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402-9325

Foreword

This publication is issued by the National Institute of Standards and Technology as part of its program to promulgate security standards for information systems as well as standards for test procedures for assessing the level of conformance to these standards. This document is intended for use primarily by system administrators of PBX systems, but may also be useful for security evaluators. Where possible, countermeasures are described that can be applied by system administrators. In some cases vulnerabilities may be discovered that require software patches from the manufacturer.

Comments on this document should be directed to:

Richard Kuhn
NIST/Computer Security Division
Gaithersburg, MD 20899-8930

INTRODUCTION

The Private Branch Exchange (PBX) is an essential element that supports the critical infrastructure of both government agencies and U.S. industry. A PBX is a sophisticated computer-based switch that can be thought of as essentially a small, in-house phone company for the organization that operates it. Protection of the PBX is thus a high priority. Failure to secure a PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, and loss of revenue or legal entanglements.

This report presents a generic methodology for conducting an analysis of a Private Branch Exchange (PBX) in order to identify security vulnerabilities. The report focuses on digital-based PBXs and addresses the following areas for study:

- System Architecture
- Hardware
- Maintenance
- Administrative Database/Software
- User Features

This report is not intended to provide a step-by-step process, but rather a guideline for what specific areas should be studied for the existence of possible vulnerabilities. This process must be customized for each specific PBX, depending upon the actual switch features as well as the perceived threat. We do not identify known vulnerabilities in particular switches because doing so may encourage attacks by unsophisticated hackers or "script kiddies." However, this report does provide information on vulnerabilities that are not well known to many system administrators, as well as procedures for penetration testing, i.e., determining the existence of these vulnerabilities and if they can be exploited. Sophisticated hackers and foreign intelligence organizations should be assumed to know of these vulnerabilities already. System administrators need to be able to find them before an attacker does. Note that some of the analysis methods described here may require instruments or expertise not available in all organizations. Individual judgment will be required to determine if the organization's risk is sufficient to warrant obtaining additional assistance.

A second reason for conducting penetration tests is to determine what countermeasures should receive priority. Not all of the vulnerabilities described in this report will appear on every PBX system. Depending on the system architecture and the set of active user features, the risk of some security weaknesses being exploited will be considerably less than for others. Given a limited budget for security, protecting against the higher risk vulnerabilities will require giving less attention to others. To establish whether the potential exists for a particular attack on a PBX, testing will normally be needed. The methods described in this report are designed to assist administrators in conducting this type of testing. Computer based telephony systems and new techniques such as voice over IP (VOIP) present an entirely new collection of vulnerabilities and are not addressed in this report. However, some of the evaluation methods described here may be applied to these systems as well.

BACKGROUND

Digital PBXs are widespread throughout government and industry, having replaced their analog predecessors. The advent of software-based PBXs has provided a wealth of communications capabilities within these switches. Today, even the most basic PBX systems have a wide range of capabilities that were previously available only in large-scale switches. These new features have opened up many new opportunities for an adversary to attempt to exploit the PBX, particularly by using the features as designed for a purpose that was never intended. The threats to PBX telephone systems are many, depending on the goals of attackers. Threats include:

- *Theft of service* – i.e., toll fraud, probably the most common of motives for attackers.
- *Disclosure of information* - data disclosed without authorization, either by deliberate action or by accident. Examples include both eavesdropping on conversations or unauthorized access to routing and address data.
- *Data modification* - data altered in some meaningful way by reordering, deleting or modifying it. For example, an intruder may change billing information, or modify system tables to gain additional services.
- *Unauthorized access* - actions that permit an unauthorized user to gain access to system resources or privileges.
- *Denial of service* - actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.
- *Traffic analysis* - a form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g. from the source and destination numbers, or frequency and length of the messages. For example, an intruder observes a high volume of calls between a company's legal department and the Patent Office, and concludes that a patent is being filed.

PBXs are sophisticated computer systems, and many of the threats and vulnerabilities associated with operating systems are shared by PBXs. But there are two important ways in which PBX security is different from conventional operating system security:

- *External access/control.* Like larger telephone switches, PBXs typically require remote maintenance by the vendor. Instead of relying on local administrators to make operating system updates and patches, organizations normally have updates installed remotely by the switch manufacturer. This of course requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.

- *Feature richness.* The wide variety of features available on PBXs, particularly administrative features and conference functions, provide the possibility of unexpected attacks. A feature may be used by an attacker in a manner that was not intended by its designers. Features may also interact in unpredictable ways, leading to system compromise even if each component of the system conforms to its security requirements and the system is operated and administrated correctly.

Although most features are common from PBX to PBX, the implementation of these features may vary. For example, many PBX vendors have proprietary designs for the digital signaling protocol between the PBX and the user instruments. This is the reason digital instruments usually cannot be interchanged between PBXs of different manufacturers. The methodology outlined in this report will assist in the investigation of PBX features that are known to be susceptible to adversarial attack. However, the degree of vulnerability, if any, will depend on how each feature is implemented.

EVALUATION APPROACH

This report provides suggestions for areas of investigation. In practice, the evaluator may discover many other avenues of investigation. For some aspects of the PBX, specific steps are suggested to attempt to investigate a vulnerability (especially User Features). For others, the approach is necessarily architecture-dependent and must be discussed more generally.

The type of skills and number of evaluators required, as well as the length of time required to perform the evaluation cannot be fixed since these depend on the size and complexity of the PBX under study. The type of perceived threat and the seriousness of any discovered vulnerabilities must be decided by the evaluating organization. Consequently, any corrective actions must also be decided upon based on the cost of the loss compared with the cost of the corrective action. It is recommended that at least two individuals perform the evaluation in order to share observations and gain the advantage of multiple insights.

SYSTEM ARCHITECTURE

This section addresses the ways in which an adversary may be able to exploit vulnerabilities that are inherent in the system architecture.

SEPARATION OF SWITCHING AND ADMINISTRATIVE FUNCTIONS

All modern PBXs have central computer processors that are controlled from a software-driven stored program (see Figure 1). In addition, most PBXs have microprocessors dispersed throughout the switch that provide real-time signaling and supervision control as instructed from the central processor. One or more terminals and their associated port(s) provide computer operating system, database management, and maintenance access to the PBX processor. Access to these functions gives the administrator or maintenance personnel total control of the PBX. Depending on the size of the PBX, these functions may be separate or combined.

Administrative Terminals. The switch should be examined to determine whether the administrative functions are performed on terminals that are connected to the PBX via the same type of ports that switch the voice and data traffic, or if the terminals are connected via dedicated ports. If they are connected via the same type of voice and data ports, these terminals could be surreptitiously switched to an unauthorized user. This may or may not require a modem. If the ports are dedicated for use by these terminals, this vulnerability is reduced. However, it may be possible for an adversary to gain access through the use of a modem coupled with an unauthorized connection to a switched port, enabling the adversary to dial in and make database modifications. Tests should be conducted to see if these functions can be rerouted to other physical terminals through configuration options or other changes to the administrative database.

In smaller PBXs, these functions are often combined. For example, the attendant (operator) terminal may also be the database terminal, or the database terminal may also be the maintenance terminal. Attempts should be made to use these terminals to modify the database or gain access to unauthorized functions. For example, investigate whether the attendant or maintenance personnel can gain access and modify the database.

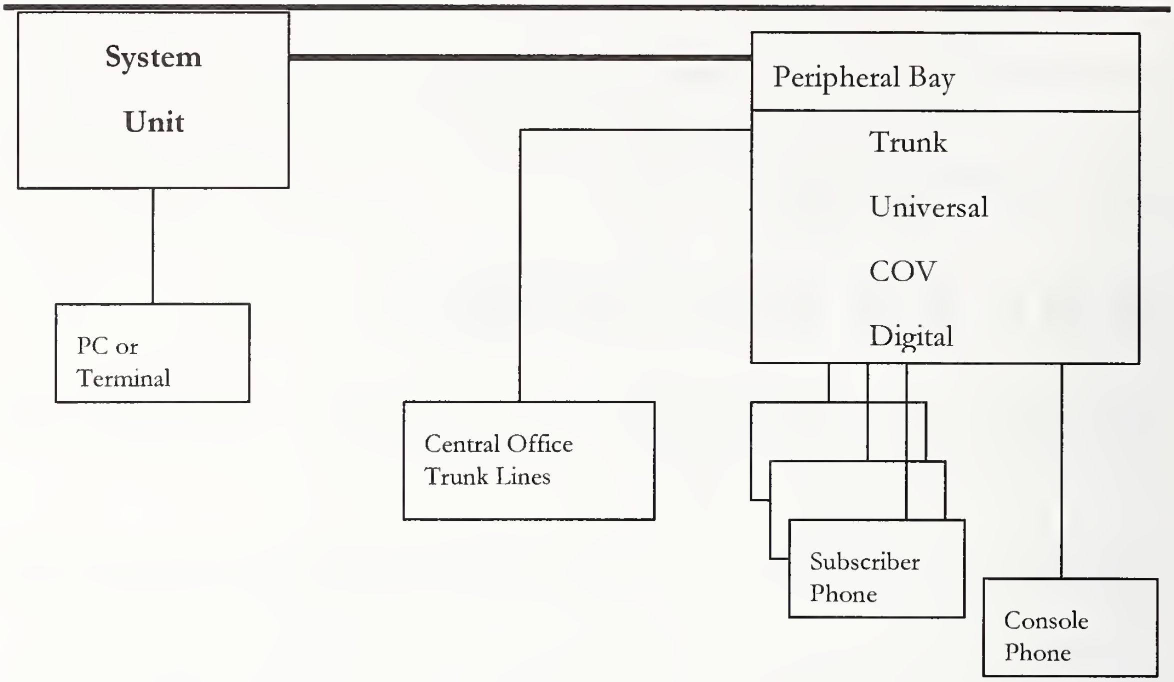


Figure 1. PBX Block Diagram

SWITCHING ALGORITHM

Switching is performed using time division multiplexing techniques where each voice (digitized) and data port is assigned a time slot. Under control of the call processing routines, incoming time slots are connected to outgoing time slots. If the number of incoming slots does not exceed the number of outgoing slots, there will be no contention for switching resources. This is commonly known as non-blocking switching.

Dual Connections. To investigate for vulnerabilities, attempts should be made to route another incoming time slot to an outgoing time slot in addition to the intended time slot. This might be accomplished by a database entry or by a modification to the PBX control software. After accomplishing this, test calls should be made to verify the dual connection and to determine whether the calling or called party can detect the false connection. If the PBX under study has status or maintenance query features, attempts should be made to detect the modification.

The documentation accompanying the PBX forms the basis for learning its structure and operation. The manufacturer may have additional documentation that will be useful during the course of the evaluation. It may be beneficial to have technical discussions with the manufacturer to fully understand how PBX functions are implemented. Since this information is usually proprietary, it may be necessary to negotiate a non-disclosure agreement between the evaluating organization and the manufacturer to protect this data.

Also, the manufacturer may provide training as to the operation and maintenance of the PBX for customers that purchase their products.

Function Allocation

Although most PBX functions are software driven, the PBX under study should be examined to determine how specific features are implemented so that potential vulnerabilities can be explored. For example, conferencing can be implemented in hardware or software. Knowing the design implementation will aid in determining if an adversary may be able to exploit the function. Figure 2 shows a typical PBX functional architecture.

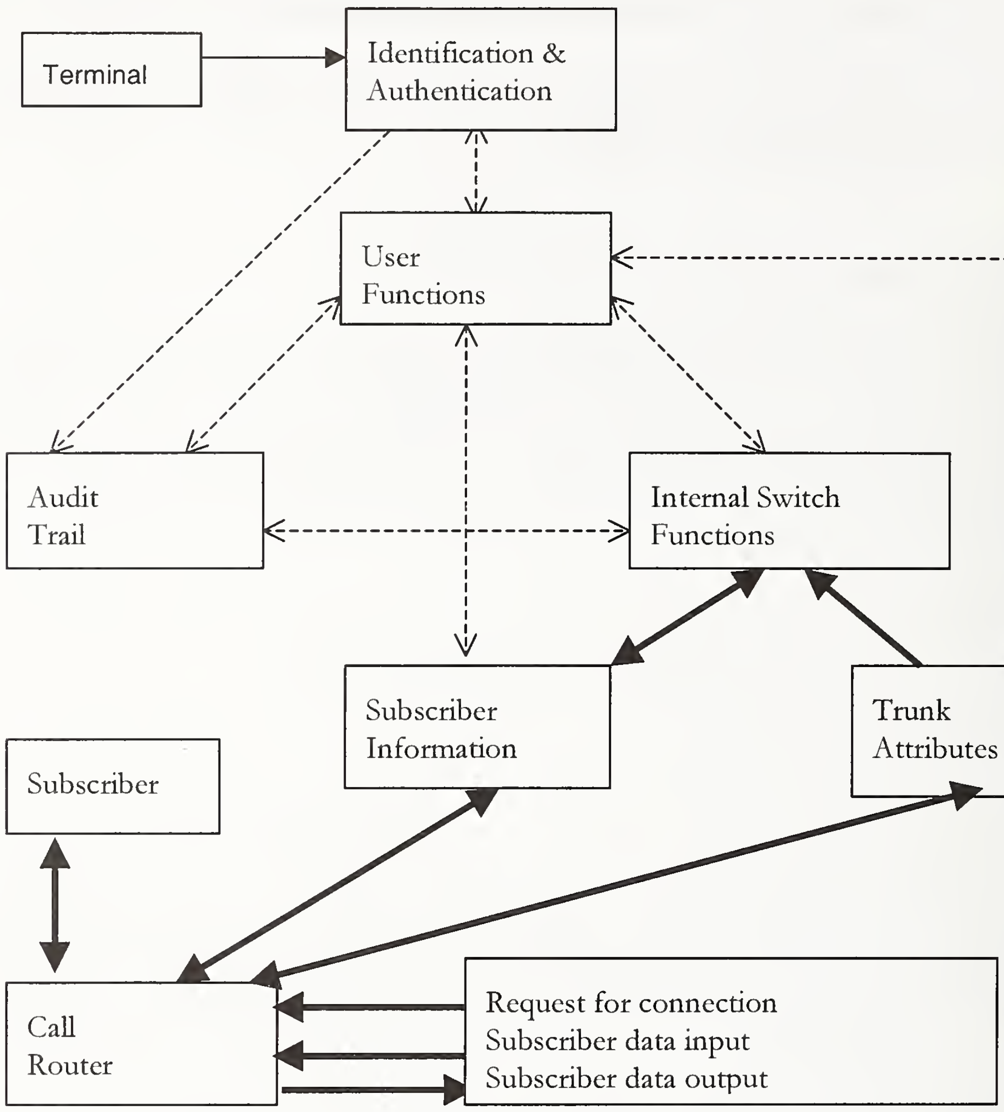


Figure 2. PBX Functional Architecture

HARDWARE

This section addresses the ways in which an adversary could exploit vulnerabilities that are inherent in the system hardware to gain unwanted access to information passing through the switch.

SUSCEPTIBILITY TO TAPPING

A PBX's susceptibility to tapping depends on the methods used for communication between the PBX and its instruments. This communication may include voice, data, and signaling information. The signaling information is typically commands to the instrument (turn on indicators, microphones, speakers, etc.) and status from the instrument (hook status, keys pressed, etc.). Three general communications methods are discussed below.

Analog Voice with or without Separate Control Signals

This is the simplest of the three methods discussed here. Analog voice information is passed between the PBX and the instrument on either a single pair of wires or two pairs (one for transmit and one for receive). If there is any additional signaling communication (other than the hook switch) between the PBX and the instrument, it is done on wires that are separate from the voice pair(s).

The voice information is transmitted essentially as it is picked up by a microphone. It is in a form that can be directly reproduced by a speaker. The voice line can be easily tapped by connecting a high impedance differential amplifier to the pair of voice wires. The amplified voice signal can then be heard directly with a speaker or headphones, or it can be recorded for later playback.

If signaling data is transmitted on a separate set of wires, it is normally in proprietary formats. An adversary with physical access can gain useful information by hooking an oscilloscope up to each wire and observing the effects when the instrument is taken on and off hook, keys are pressed, etc. For example, in one common format the voltage present on each data wire reflects the on/off status of a control or indicator.

Another possible format is one in which information is passed as bytes of digital data in a serial asynchronous bit stream similar to that of a PC's or a terminal's serial data port. Each data byte being transmitted would appear in a pattern similar to the following: Start Bit, Data Bits (5..8, frequently 8), optional Parity Bit, Stop Bits (1, 1.5, or 2). The Start Bit and Stop bits are of opposite polarity. The bit rate could be measured with an oscilloscope. A device such as a PC or terminal could then be configured to capture the serial data and perhaps store it for some later use.

Analog Voice with Inclusive Control Signals

In this scheme, analog voice and control signaling is passed between the PBX and the instrument on either a single pair of wires or two pairs (one pair for transmit and another for receive). This can be done if the signal path is of a high enough bandwidth to pass voice information (less than 4 KHz) plus additional data information. For example, voice information can be combined with data information modulated onto a carrier tone that is centered outside of the voice band.

This type of line is vulnerable to tapping by connecting a high impedance differential amplifier to the pair and passing the signal through filters to separate the voice and data information. Data information could be recovered by demodulating the carrier tone. The methods outlined in the section above could then be used to determine the format of the data being transmitted.

Digital Voice with Inclusive Control Signals

With this method, voice and control signaling data are passed across the same pair of wires. There may be two pairs of wires, one for each direction, or both directions could be combined onto one pair of wires using echo cancellation as is done with ISDN. Conventional tapping techniques would not work against most types of digital lines. The format and type of digital signals that pass between the PBX and its instruments vary widely between switch types.

If separate pairs are used for transmit and receive, each pair could be tapped to provide access to the transmit and receive digital bit streams by first determining in what digital format the data is being transmitted. Then a digital to analog converter could be used to convert the digital data back into analog voice that can be listened to or recorded. A great deal of information useful to an attacker could be gained by disassembling the telephone models of interest and determining what types of parts are used for CODECs, UARTs, A/Ds, D/As, etc. Published information on these parts can generally be obtained from the manufacturers.

Echo Cancellation

If both transmit and receive are combined on one pair using echo cancellation, the previously described methods would not be useful for tapping. This is because each transmit end of the link can only determine what is being received by subtracting out what it is transmitting from the total signal. An outside observer tapping the line somewhere between the two ends would only have access to the total signal and would therefore find it very difficult to reproduce either end. An attack would depend on a known initial condition on both ends (such as silence) in order to be able to subtract the correct information from the total signal. The technical difficulty of this attack probably makes systems using echo cancellation most resistant to attack among those described here. Protecting against this attack requires ensuring that lines are not physically compromised.

Analysis of Signaling Methods

It may be possible to discover information about the method of communication between the PBX and its instruments by disassembling and examining them. Most digital instruments are designed around a microcontroller that handles the PBX communication, controls the displays, and responds to key presses and hook status changes. There may be a PROM device in the instrument, or the microcontroller may have built-in PROM that stores the microcontroller's software. With access to the PROM and/or microcontroller, the software could be disassembled, providing information about the PBX communication. If the software is stored directly in the microcontroller, it may not be accessible since some microcontrollers have a security feature that can make it difficult if not impossible to read its contents once it is programmed. An approach to investigating these vulnerabilities is the following:

- Disassemble an instrument.
- Note the integrated circuits (ICs) that are used and look up unfamiliar ICs in the corresponding vendors' data books. This provides knowledge as to the signaling protocols.
- Determine if the instrument contains a PROM device. If so, a detailed investigation would require attempting to remove and read the device with a PROM programmer.
- Locate the microcontroller and determine its part number. Look it up in the microcontroller manufacturer's data books. Determine if it has a security feature

and if so, how it works. A detailed investigation would require attempting to read the microcontroller's contents with a PROM programmer or a test circuit and a PC or workstation.

- If the PROM or microcontroller code is readable, it may be desirable to try to disassemble the code to learn how the instrument communicates with the PBX. Some reverse engineering may be required.

Instrument Modification Risks

- Methods to prevent eavesdropping on an on-hook analog telephone by using telephone instruments that are known to resist such attacks have been documented in the Telephone Security Group (TSG) standards [TSG]. However, digital instruments offer a similar vulnerability. An adversary interested in eavesdropping on a particular user instrument has three goals:
- Create a condition so that the voice information will be transmitted to the PBX while giving the appearance that the instrument is on-hook.
- Modify the instrument to keep the microphone live while in an on-hook condition.
- Ensure that this condition is transparent to the user and the PBX.

The circuitry of the digital instrument under study must be analyzed to determine the conditions that must exist to allow the digitized voice information to continue to transmit to the PBX. This may include having the handset off-hook electrically. Also, since the instrument would normally include a CODEC to convert the analog voice to digital data, this function must be enabled. In order to create the necessary conditions, it may be necessary to cut traces on the circuit board and/or insert jumpers to bypass certain safeguards within the instrument itself. One could also modify the on-board PROM containing the program that controls the instruments to create this condition. The key condition is that the instrument still appear to be on-hook to the user and the PBX so that normal calls can be made and received.

Once the conditions are created, make calls to and from the modified instrument to assure normal operation. Also, if diagnostic tests are available, test the line in question to be sure that no abnormal conditions are detected.

Having successfully modified an instrument now creates the opportunity for an adversary to exploit. As mentioned earlier, the line cannot simply be "tapped" to gain access to the voice data. An active device may be required to "tap" the line between the instrument and the PBX and convert the bit stream to analog form. Also, this condition may be exploited in conjunction with one or more feature vulnerabilities to allow undetected access to the telephone line of interest.

CONFERENCING (HARDWARE)

When implemented in hardware, the conferencing feature may employ a circuit card known as a conference bridge or a signal processor chip. This allows multiple lines to be "bridged" to create a conference where all parties can both speak and listen. Some PBXs have a feature where all parties can hear, but only certain parties can speak. This is a type of broadcast conference. An adversary would desire a connection to the bridge where the conference could be overheard. A hardware modification to the bridge itself may make it possible to cause the "output" of the bridge to be available to a specific port. As in instrument modifications, some additional steps must be taken to receive this information. This may include modifying the database to have the adversary be a permanent member of the bridge so that any conference on that bridge could be overheard.

COUNTERMEASURES

- Physical security to prevent unauthorized access to telephone closets and PBX facilities is important. Whenever possible, the PBX should be kept in a locked room with restricted access.
- Critical hardware components may be locked with anti-tamper devices.
- Periodic integrity checks should be made to ensure that components have note been tampered with.

MAINTENANCE

Maintenance procedures are among the most commonly exploited functions in networked systems, and the problem is even more acute with PBXs because PBX maintenance frequently requires the involvement of outside personnel. This section addresses the ways in which an adversary could exploit vulnerabilities in maintenance features to gain unwanted access to the switch.

REMOTE ACCESS

Remote access is frequently an unavoidable necessity, but it can represent a serious vulnerability. The maintenance features may be accessible via a remote terminal with a modem, an Attendant Console or other instrument, or even over an outside dial-in line. This allows for systems to be located over a large area (perhaps around the world) and have one central location from which maintenance can be performed. Often it is necessary for the switch manufacturer to have remote access to the switch to install software upgrades or to restart a switch that has experienced a service degradation.

Dial-back modem vulnerabilities.

Unattended remote access to a switch clearly represents a vulnerability. Many organizations have employed dial-back modems to control access to remote maintenance facilities. This access control method works by identifying the incoming call, disconnecting the circuit, and dialing the identified person or computer at a predetermined telephone number. Although helpful, this form of access control is weak because methods of defeating it are well known. For example, if the local telephone company central office uses originator control for phone lines, the attacker can stay on the line, send a dial tone when the modem attempts to disconnect, then wait for the modem to dial out again on the same line. A more sophisticated means of defeating dial-back modems has also been used in attacks reported in the open literature. In this method, the local phone company switch is penetrated and its databases modified to forward the returned calls directly to the attacker's computer.

Social engineering attacks.

Even if the organization requires some action by local operators to provide access to the remote maintenance connection, serious vulnerabilities may still exist. For example, modems on lines used by remote maintenance may be kept off, and only turned on when a call is received from the switch manufacturer. Often the only form of authentication used by the organization may be ensuring that the manufacturer remote maintenance personnel requesting access are listed among legitimate remote users. This form of authentication is clearly inadequate. It is easy for attackers to contact the switch manufacturer on the pretext of needing help with a particular type of switch, obtain the names of the manufacturer's remote maintenance personnel, and then masquerade as these personnel to obtain access to the victim's switch.

Maintenance Feature Vulnerabilities

A common maintenance feature is Maintenance-Out-of-Service (MOS). This feature allows maintenance personnel to place a line out of service for maintenance. It is typically used when a problem is detected with a line or when it is desired to disable a line. However, if a line is placed MOS while it is in operation, the PBX may terminate its signaling communication with the instrument and leave the instrument's voice channel connection active even after the instrument is placed on-hook. If the MOS feature were to function in this manner, the potential exists for someone to use the MOS feature to establish a live microphone connection to a user's location without the user's knowledge, and thereby eavesdrop on the area surrounding the user's instrument.

Line Testing Capabilities

Another common maintenance feature is the ability to connect two lines together in order to transmit data from one line to the other and verify whether or not the second line receives the data properly. This feature would allow someone with maintenance access to connect a user's instrument to an instrument at another location in order to eavesdrop on the area surrounding the user's instrument without the user's knowledge.

Undocumented Maintenance Features

The PBX may support some maintenance features that are not normally accessible to the owner/operator of the PBX for several reasons. These types of utilities vary greatly from one PBX to another so that a general approach to finding them cannot be detailed. Some suggested courses of action are listed below:

- Ask the manufacturer or maintenance company if any such features exist.
  - Attempt to learn about undocumented usernames/passwords.
  - Attempt to search the system PROMS or disks for evidence of such features.
  - Viewing the system load files with a binary editor will sometimes reveal the names of undocumented commands among a list of known maintenance commands that can be recognized in the binaries.

SPECIAL MANUFACTURER'S FEATURES

There may be features that the manufacturer considers useful in the event a customer's PBX becomes disabled to such a point that on-site maintenance personnel cannot resolve the problems. The manufacturer could then instruct the maintenance personnel to configure and connect a modem to the maintenance port. The manufacturer may then be able to dial-in and use certain special features to resolve the problems without sending a representative to the customer's location. The potential cost savings is a likely reason for adding such special features. The manufacturer would not want the special features to be well known because of their potential vulnerability. These types of features would most likely be accessible via undocumented username/password access to the maintenance and/or administrative tools. Some possible undocumented features are listed below:

- *Database upload/download utility:* Such a utility allows the manufacturer to download the database from a system that is malfunctioning and examine it at their location to try to determine the cause of the malfunction. It would also allow the manufacturer to upload a new database to a PBX in the event that the database became so corrupted that the system became inoperable. Compromise of such a utility could allow an adversary to download a system's database, insert a trojan horse or otherwise modify it to allow special features to be made available to the adversary, and upload the modified database back into the system.

- *Database examine/modify utility:* Such a utility allows the manufacturer to remotely examine and modify a system's database to repair damage caused by incorrect configuration, design bugs, or tampering. This utility could also provide an adversary with the ability to modify the database to gain access to special features.

- *Software debugger/update utility:* This type of utility gives the manufacturer the ability to remotely debug a malfunctioning system. It also allows the manufacturer to remotely update systems with bug fixes and software upgrades.

Such a utility could also grant an adversary the same abilities. This is perhaps the most dangerous vulnerability because access to the software would give an adversary virtually unlimited access to the PBX and its associated instruments.

MANUFACTURER'S DEVELOPMENT & TEST FEATURES

There may be features that were added to the system during its development phase that were forgotten and not removed when production versions were released. There also may be hidden features that were added by a person on the development team with the intent of creating a backdoor into customers' systems. Left-over debugging code, binary editors, and even a "battleship" game have been discovered in commercial PBX system load modules.

These types of features potentially create extreme vulnerabilities for the PBX system if an adversary has detailed knowledge of the software and its structure. This is because there is generally little or no protection given to test features that are expected to be removed. The test features are probably easy to access for ease of development and have few restrictions in order to reduce development time. These types of features could come in many forms, such as:

- Undocumented username/passwords
- Entering out-of-range values in database fields
- Dialing undocumented access codes on instruments
- Pressing certain key sequences on instruments

It may be possible to discover some of these undocumented features during the normal course of the evaluation. If open technical discussions are held with the manufacturer, this area should be discussed, although they may only be known to the original designers/developers. Lastly, some "shortcuts" may be described in vendor training courses as an aid to maintenance people.

COUNTERMEASURES

- Ensure that remote maintenance access is normally blocked unless unattended access is required. Whenever possible, require some involvement of local personnel in opening remote maintenance ports.
- Install two-factor (i.e., two different mechanisms) strong authentication on remote maintenance ports. Smart-card based systems or one-time password tokens, in addition to conventional login/password functions, make it much more difficult for attackers to breach your system's security.
- Keep maintenance terminals in a locked, restricted area.
- Turn off maintenance features when not needed, if possible.

ADMINISTRATIVE DATABASES

Administrative databases represent "the keys to the kingdom" for a PBX. Among the most critical security tasks for PBX owners are administration of the PBX, the creation and modification of its user databases, and the operating software controlling the switch.

Software Loading and Update Tampering

When software is initially loaded onto a PBX and when any software updates/patches are loaded, the PBX is particularly vulnerable to software tampering. A software update sent to a PBX administrator could be intercepted by an adversary. The update could be modified to allow special access or special features to the adversary. The modified update would then be sent to the PBX administrator who would install the update and unknowingly give the adversary unwanted access to the PBX.

Tamper and Error Detection

The ability of an adversary to intercept and modify the software can be reduced by several means. The software could be encrypted by the manufacturer and decrypted by the PBX during the install/update process using unique keys only possessed by the manufacturer and PBX administrator (or the PBX itself). This method would work well unless the adversary were to discover the key and encryption method. The presence of such an encryption scheme could be detected by looking through the software with an ASCII dump utility on a PC or workstation. The software will almost definitely contain words and phrases that are recognizable to people such as messages, variable and function names used by debuggers, etc. If no readily recognizable words or phrases are found, it is very likely that the software is encrypted.

The software manufacturer could also use error detection methods in order to detect tampered software before installation. Various cyclical redundancy checks and checksums can be performed on the software before it is installed. The results can be compared with known correct results stored with the software or in ROM on the PBX to determine whether or not the software is valid. This scheme is useful against hardware or other unintentional errors, but only marginally effective against a skilled attacker. Software can be intentionally modified in such a way that the modification will not be detectable by standard error detection algorithms. A PC or workstation could be used to read the PBX software, make changes, and place the modified software on media used by the PBX. The installation or update process can then be attempted with the modified software. If an error detection scheme is in fact used, it is very unlikely that the installation process will allow the modified software to be installed.

Countermeasures

Many software packages use error detection codes to protect against transmission or disk copying errors. Conventional error detection codes such as checksums or cyclical redundancy checks (CRC) are not sufficient to ensure tamper detection. Strong error detection based on cryptography must be used. These methods use cryptographic algorithms that guarantee detection of even a single bit modification.

CRASH-RESTART ATTACKS

System crashes primarily present a denial-of-service vulnerability. The means by which a system may be crashed vary significantly from one system to another. The following list suggests a few features and conditions that can sometimes trigger a system crash:

- Call Forwarding.
- Voice mail.
- Physical removal of hardware or media from the PBX.
- Use of administrative/maintenance terminal functions.
- Direct modification of the system or the database may be possible if the media can be read by utilities typically found on a PC or workstation.
- Normal system Shutdown procedures.

These approaches should be tested as possible ways of exposing the weaknesses discussed in the remainder of this section.

Live Microphone Vulnerabilities

Although denial-of-service is the primary vulnerability of a system crash, it is not the only possibility. A system may in some cases be crashed in such a way as to disable the interaction between the PBX and its instruments without terminating the calls in progress.

When a user then attempts to terminate a call, the PBX may be unable to command the instruments to disable their microphones thereby causing voice data to continue to be received by the microphone and transmitted to a destination that may be accessible to an adversary. The adversary could then eavesdrop on areas around the target instrument until normal operation of the PBX is restored. While attempting to cause various system crashes as described above, try to determine if any connections remain active after the crash and the users attempt to terminate the connections.

Embedded Login IDs and Passwords

Passwords are normally stored in the system database and can be changed by administrators and users, as in any computer operating system. However, testing has shown that some PBXs have embedded login IDs and passwords that are restored on rebooting the system. These may be needed to allow manufacturer personnel to bring up a system remotely after a failure that has corrupted the local database. However, they also make it possible for an attacker to gain administrator privileges on a system by crashing the system, then applying a known embedded login ID/password combination.

Countermeasures

- Test for crash-restart vulnerabilities. If present develop and document restart procedures that eliminate the vulnerability. This may require doing a cold start (complete shutdown, power-off, and restart) in event of a system crash.
- If embedded passwords are found, consider patching the load module to replace them. Authorized manufacturer personnel can be given the new password if needed.

PASSWORDS

Most PBXs grant administrative access to the system database through an Attendant Console or a generic dumb terminal. Username/password combinations are often used to protect the system from unwanted changes to the database. If remote access to the maintenance features is available, it is usually restricted by some form of password protection. There may be a single fixed maintenance account, multiple fixed maintenance accounts, or general user defined maintenance accounts. The documentation provided with the PBX should state what type of maintenance access is available. The documentation should also indicate how passwords function.

Password Types

Passwords may be set at the factory to predetermined permanent values. If this is the case, the passwords should be provided by the manufacturer. They may also be determined by searching the contents of the system media (ROM, PROM, EPROM, EEPROM, FLASH, floppy/hard disk, CD-ROM) for the user or account names. Passwords may be stored in a look-up table near the account names. However, some form of encryption may be used to make it difficult to determine the passwords.

Passwords may also be set to factory default values that can be changed by the user. Default values are typically published in the documentation provided with the PBX. If there are multiple maintenance accounts and only one is used by maintenance personnel, the others may remain at their published factory settings. This would grant maintenance access to anyone who knows the factory default settings. Tables where passwords are stored may be readily found by making a copy of likely storage media (EEPROM, FLASH, floppy disk), changing a password, and comparing the updated media with the older copy. Any differences are likely to indicate where passwords are stored. Even if the passwords are encrypted, the encrypted versions of known passwords could be placed into the password locations of other accounts to set the password of an account without having prior access to that account. This scenario could be used by an adversary to seize control of the PBX since the passwords would only be known by the adversary.

In addition to published or user defined usernames/passwords, there may be additional combinations that are intended only for use by the manufacturer. If a table containing usernames or passwords can be found in the load module, comparing the number of entries in the table with the number of known combinations could lead to the discovery of additional combinations. If additional passwords are found but the usernames associated with them are unknown, it may be possible to determine correct combinations as follows:

- Change the password to one that is known. Then try logging in using the known password with various reasonable guesses at the username such as ADMIN, MAINT, SYSTEM, SUPERUSER, ROOT, etc.
- If a valid username can be determined without a password, it would be useful to try logical guesses at the password.
- The maximum allowable length of a password would be useful to know when guessing passwords. If not published, it could be determined by using the

system to set the password of an accessible account to longer and longer passwords until perhaps the password is not accepted.

- If a very long password is accepted, the system may only use part of it. The useful part could be determined by first setting a very long password and then trying to log in using only the first few characters.
- Try longer and longer parts of the password until a part is found that works. The length of the successful part is likely to be the maximum password length.

Password Login Timeouts

A potential vulnerability of the password access system is that an authentic user may log onto the system and at some point leave the active terminal unattended without intentionally logging-off of the system. An adversary with access to the terminal could then have access to the maintenance system and its features.

The PBX may provide protection from such a vulnerability in the form of a timeout period. The system could measure the amount of inactive time on the terminal and automatically terminate the login session. If the timeout period is set to a short enough time, the chances of an adversary gaining access to an unattended terminal are significantly reduced. However, the timeout period cannot be so short that an authentic user becomes annoyed by frequent automatic logouts during normal use. The timeout can be tested as follows:

- Log into the system.
- Wait a while without pressing any keys or moving the mouse. A timeout should occur in about 5 - 10 minutes. Watch for any warning messages that indicate that a timeout has occurred.
- Try to access the system to determine if the login session has been terminated. There may not have been a warning message displayed when the timeout occurred.
- If no timeout is observed, try longer waiting times - up to perhaps 30 minutes. A timeout this long or longer would not be very useful.

A system without a timeout feature that has dial-up maintenance capabilities could allow an adversary access to remote maintenance capabilities. For example, an authentic user may dial-up and log-into the maintenance system, perform maintenance tasks, and disconnect without logging-off. If an adversary were then to dial-up the maintenance system, access to the system may be available without the use of a username/password to gain access.

Multi-Level Password Access

The password system may employ a scheme where the level of access granted to a user is dependent on the username or password that is used. For example, there may be a "super user" that has virtually unlimited access to the database and maintenance features while an "attendant" may only be able to adjust a limited set of database parameters.

If there are multiple levels of access, try to determine if they are user selectable (perhaps by the "super user") or if they are predetermined by the manufacturer. Look for a feature that allows a higher level user to determine the access level of those below it. If the levels of access are adjustable, a user with a low level of access may be able to increase their access levels by modification of the system database.

Countermeasures

Perhaps the most important task for password security is to make passwords resistant to cracking by automated tools. A password generator that creates random passwords can go a long way in defeating password crackers. Both free and commercial random password generation tools are available. Commercial products are available that can generate passwords of user-selectable length that are very resistant to cracking.

Physical Security

Physical access to the PBX hardware grants access to the software, the configuration database, and all calls going in and out of the PBX. With easy access to the PBX, practically any conceivable vulnerability could be exploited by an adversary.

The type of media on which the software and databases are stored is important to a PBX's physical security. If these are stored on ROM type devices or on an internal hard disk, it is more difficult to gain access to them than if they are stored on floppy disks or CD-ROM. ROM devices are mounted on circuit boards and may be soldered in rather than socketed, making removal and replacement difficult. Likewise, an internal hard disk is probably mounted behind something and is bolted into the chassis making removal and replacement difficult. However, floppy disks are easily removable and replaceable. An adversary with access to the floppy disks could easily conceal a disk containing modified software/databases, gain access to the PBX, and replace the original disk with the modified disk. Similarly, CD-ROMs can be easily removed and replaced. Since equipment for creating CD-ROMs is as readily available as for floppy disks, an adversary may find it as equally easy to copy and modify a CD-ROM based system.

If the PBX supports configuration and maintenance via a dumb terminal, the terminal may be located near the PBX. If the terminal is not at the same location as the PBX, the terminal port is still available and could be used by an adversary with a PC acting as a terminal.

Some PBXs may be configured as a central system unit with peripheral units at remote locations. The remote peripheral units may also support configuration/maintenance via a dumb terminal and therefore provide the same vulnerabilities as the system unit's terminal. Also, all calls routed through a particular peripheral unit are accessible to someone with physical access to the peripheral unit.

Attendant Consoles may offer access to PBX maintenance and configuration software. Special features may also be available to Attendant Consoles such as Override, Forwarding, and Conferencing. If any of these features are available to the user of an Attendant Console, physical access to it should be restricted to prevent giving an adversary unwanted access to these features.

Most PBXs have an attached system printer. Various information may be output to the printer including source and destination of calls that are made or received (possibly every call), access codes used to access certain features, account or authorization codes used for making special calls, etc. Access to these printouts could provide information enabling toll fraud or other compromises.

Countermeasures

Because of the potential for exploitation by intruders, PBX boot disks and utilities must be given more protection than usually afforded typical office software such as word processing packages. Strong physical security should be provided for PBX software. Audit reports from the PBX should be shredded or destroyed in the same way as confidential memos or financial information.

REMOTE ACCESS

A very useful but potentially vulnerable feature of many PBXs is remote administrative access. The PBX may allow an administrator to make changes to the system configuration database through an Attendant Console or from a terminal that is not physically located near the PBX, perhaps over a dial-in line with a modem.

Remote Access via an Attendant Console

The degree of the vulnerability created by remote access via an Attendant Console is determined by several factors: password access, physical connection of the Attendant Console to the PBX, and availability of administrative features through the Attendant Console.

If there is no password protection or if the password protection is not very good, physical access to the Attendant Console becomes very important. If the Attendant console connects to the PBX in the same manner as the telephone instruments, an adversary could connect their own Attendant Console in place of any other instrument to gain access to the administrative features.

Remote Access via a Terminal

If a standard dumb terminal can be used for access to the administrative features, more opportunities become available for an adversary to gain unwanted access. A modem could be connected to a terminal port and an outside dial-in line allowing easy access for the PBX administrator to do remote configuration and maintenance. Unfortunately, it also gives easy remote access to an adversary. By setting up remote access in this manner, a poor password protection system, the existence of "backdoors" (e.g., a special key sequence that would bypass required authorization levels), or the use of easy-to-guess passwords would seriously undermine the security of the system.

Some PBX systems may even support multiple terminal ports. For example, a system with multiple remote switching components (nodes) may have a terminal port for each node. If all of the terminal ports were considered to be one access point by the PBX, an unused port could be used by an adversary to copy the communications of a port that is used. This may allow an adversary to gain password information that could then be used to gain full access to the system's administrative and maintenance features. Testing for remote access can be done as follows:

- Connect a modem to the administrative or maintenance terminal port. Make sure the modem is configured correctly (baud rate, parity, stop bits, DTE/DCE). Also connect the modem to a line that is accessible from the PSN.
- Connect a similar modem to a terminal and a line on the PSN.
- From the remote terminal, dial into the administrative/maintenance port. Determine the extent of access that is available with this configuration.
- While logged into the system, disconnect the line and call back. Determine if the login session was automatically terminated after the hang-up. If not, this could present a vulnerability similar to a timeout vulnerability.

Countermeasures

- Vulnerabilities can be minimized if the Attendant Console connects to the PBX with a different physical and/or electrical connection than that of the telephone instruments.
- If the Attendant console connects to the PBX in the same manner as the telephone instruments, vulnerabilities can be reduced by having some sort of line configuration feature. Such a feature could reduce vulnerabilities by requiring that a line be specifically configured for use with an Attendant Console. With such a configuration requirement, a telephone instrument could not be easily replaced with an Attendant Console to gain access to the administrative features.

Alarms and Audit Trails

Alarms occur within the PBX for many reasons: hardware failure, thresholds exceeded, etc. They are usually categorized as either major or minor depending on whether a function is lost or just operating in a degraded mode. The evaluator must observe these alarms when attempting to modify the system to exploit a vulnerability and, in some cases, attempt to defeat them to determine if it is possible to avoid detection of the modification.

Similarly, a system administrator can use these alarms to detect such modifications. An audit of the database may also detect a modification such as a user line enabled for Silent Monitoring that was not authorized for it. The success of such an audit is only as good as the amount of configuration management applied during switch operation.

The PBX may maintain a history of significant system events to provide a system administrator a means to determine what activity has occurred on a PBX. The audit trail or system log may contain information about various events such as: database changes, power failures, hardware failures, card changes, disk changes, etc. Stored with the event type may be information such as: time and date of occurrence, type of database change, the user that made the change, the line on which remote maintenance was performed, etc.

The level of detail stored in the audit trail determines how effective it is in protecting the PBX from an adversary. For instance, if a system does not log the time and date of an event, it may be difficult for an administrator to pinpoint an adversary's actions. Also, if the system provides a means of editing, erasing, or replacing the audit trail, an adversary could use that feature to mask changes that were made. Such a feature would present a vulnerability to the system.

In researching the vulnerabilities in a particular audit trail system, it is useful to determine the level of detail stored to determine if an adversary can make changes that go unnoticed or hide changes that have been made. You should try various events such as those suggested above to determine the level of vulnerability allowed in the audit trail system.

USER FEATURES

An adversary may be able to exploit vulnerabilities in a system's features and the way in which features can interact. As with many aspects of information technology, the proliferation of features that make PBXs easy to configure and use has also led to an expansion of vulnerabilities. Many of these are inherent in the features themselves, or arise out of feature interactions, making them difficult to avoid. This discussion illustrates some of these vulnerabilities so that administrators will be able to weigh the risks of features against their benefits.

ATTENDANT CONSOLE

Attendant Consoles typically have more function keys and a larger alphanumeric display that standard instruments to support the extra features available to the Attendant Console. The Attendant Console may be used for access to maintenance and administrative functions. Some typical features available with an Attendant Console are Override, Forwarding, and Conferencing.

Attendant Override

Attendant Override is intended to allow the Attendant to break into a busy line to inform a user of an important incoming call. This feature could be used by an adversary with access to an Attendant Console to eavesdrop on conversations. The PBX should provide for some protection against such uses of Override by providing visual and/or audible warnings that an Override is in progress. The vulnerability of the Override feature can be tested as follows:

- If necessary, configure the Attendant Console to permit the Attendant to use Override.
- Place a call between two extensions.
- Use the Override feature of the Attendant Console to attempt to break into the call in progress.

- Note whether both parties can be heard by the Attendant and whether both parties can hear the Attendant. Also look and listen for indications on the target instruments that reveal that an Override is in progress. Audible warnings may come in the form of a single tone when the Override is initiated, periodic warning tones while Override is active, or a combination of the two.

- If any warnings are observed, look to see if there is any way of disabling them via the administrative tools.

- Try using Override with various combinations of inside and outside lines. There may be differences in the amount and type of warnings given between inside and outside lines.

Attendant Forwarding

A common feature granted to the Attendant is the ability to control the forwarding of other instruments. An adversary with access to the Attendant Console could use this feature to forward any instrument's incoming calls to a long distance number. The adversary could then call the target instrument and be forwarded to the long distance number, thereby gaining free long distance access. This can be tested as follows:

- Use the Attendant Console to forward a different instrument to a long distance number.

- From another instrument, or from an outside line, call the forwarded instrument. Note whether or not the long distance call is successful.

An adversary could also use Attendant Forwarding to forward a user's instrument to an unused or disabled number. As a result, the normal user of the target instrument may be denied incoming calls. This can be tested as follows:

- Use the Attendant Console to forward a different instrument to another extension, perhaps one that is not connected to an instrument.

- From another instrument, or from an outside line, call the forwarded instrument. Observe the forwarded instrument to see if 1) there is any indication that Forwarding is active, and 2) that an incoming call has been forwarded. A visual or audible warning may indicate that a call has been made to the forwarded instrument and/or forwarded to a different location.

Look for something in the administrative tools that would allow an administrator to disable the use of Attendant Forwarding to prevent an adversary from exploiting any vulnerabilities related to Attendant Forwarding.

Attendant Conferencing

Attendants may also have the ability to initiate a conference or join an existing conference. If this feature is available, the potential exists for an Attendant to eavesdrop on a conversation or add an additional party to a conference without the knowledge of the other parties. Potential vulnerabilities can be examined as follows:

- Use the Attendant Console to initiate a conference between two parties. Attempt to leave the Attendant in the conference.

- Set up an ordinary call between two parties. Attempt to use the Attendant Console to join into the call in progress. Also try to add a third party to the call in progress.

- If any of the above cases are possible, observe the instruments in the conference and look for visual or audible indications that a conference is in progress. For example, if any of the affected instruments have alphanumeric displays, the number of conference members may be displayed. There may also be a single tone heard when a member is added to the conference.

- Inside and outside lines may respond differently. If the PBX supports both digital and analog instruments, there may also be different responses between the two line types.

AUTOMATIC CALL DISTRIBUTION (ACD)

ACD allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on hold until an agent becomes available. Agents may be grouped together with each group having a supervisor. The group of supervisors may then even have a higher-level supervisor. The number of supervisors and number of levels of supervisors is dependent on the type of PBX being used.

Most ACD systems grant a supervisor the ability to monitor the calls of the group they are supervising. The system may allow this monitoring to be done without the knowledge of the parties being monitored (although laws may require consumers to be notified of monitoring.)

Because of this feature, ACD systems are a potential vulnerability to the users of a PBX. If an adversary could gain access to the configuration tools or the system database, they could set up an ACD supervisor and an ACD group. The supervisor could then monitor the calls of any of the users in the Group. The ability of an adversary to do this could be tested as follows:

- Using the system configuration tools, create an ACD Agent and assign the Agent to a specific line.
- Then create an ACD Supervisor that has the newly created Agent in its supervisory Group and assign the Supervisor to a specific line.
- On the Agent's line, place a call to another extension or outside line. Alternately, place a call from another extension or outside line into the Agent's line.
- From the Supervisor's line, access the monitoring feature for the desired Agent.
- The Silent Monitoring feature msy allow the Supervisor to monitor both sides of the Agent's call without either party having any visual or audible warning. To verify this, look for any indicators or messages on the target instruments and listen for any warning tones. Also listen to verify that the Supervisor cannot be heard on either of the target instruments.

Depending on the way the ACD system works, the Agents and Supervisors may need to be permanently assigned to specific lines. A more flexible method may also be used where the Agents and Supervisors are assigned ID codes and can be logged into any line. The type of method used will affect how the first two steps are performed. In either case it is useful to closely observe the monitored instruments to see if there are any indications that the line is being used as an ACD Agent.

Call Forwarding

Call Forwarding is a common feature that allows a user to specify an alternate number to which calls are to be forwarded based on certain conditions. Common conditions are: forward all calls, forward only when line is busy, forward when there is no answer after a certain number of rings, or forward when the line is busy or there is no answer.

Forwarding Loops. One potential problem with Call Forwarding is the ability to set up forwarding loops. This occurs when one line is forwarded through any number of intermediary lines and back to itself. If such a loop is set up, it may cause the entire system to crash or stop processing calls. This may require that one of the lines in the loop be called in order to initiate the failure. This can be tested as follows:

- If necessary, configure several lines with the ability to use Call Forwarding.
- Set up the forwarding loop by forwarding the first line to the second, the second to the third, and so on until the last line is reached. Then forward the last line back to the first. There may be a forwarding button on the instrument or you may have to dial a forwarding Access Code.
- Using a line that is not in the forwarding loop, call one of the numbers in the loop and observe what happens.
- Also try using a line that is in the forwarding loop to call another line in the loop and observe what happens.
- Try the same type of test using different forwarding methods. Also try with only one instrument forwarded directly to itself.

User Tracking. Another potential use of Call Forwarding by an adversary is to learn the whereabouts of a PBX user. Many PBXs can use instruments that possess alphanumeric displays which display messages to users. These displays may be used by the Call Forwarding feature to inform a caller that the called line has been forwarded to another line. If any instruments possessing an alphanumeric display are available, this feature can be tested as follows:

- If necessary, configure a line with the ability to use Call Forwarding.
- Forward a line to another extension.
- From an instrument possessing an alphanumeric display, call the forwarded line. Observe the display and look for messages that indicate that the dialed line has been forwarded to another extension.
- Repeat after adding other forwards.

ACCOUNT CODES/AUTHORIZATION CODES

Account Codes are normally used for tracking calls made by certain people or projects so that bills can be charged appropriately. For example, a user may be required to enter an Account Code prior to placing a long distance call. Depending on the configuration of the PBX, the Account Code may have to be on a list of approved codes for the call to be successful. If this is the case, the Account Code may be considered an Authorization Code because the user must dial a specific Account Code that is authorized for making long distance calls.

Another important use for Access Codes is for Dial In System Access (DISA). DISA typically allows a user to dial in to the PBX system from an outside line and gain access to the normal features of the PBX, almost as if they were a subscriber on the PBX instead of an outside caller. This feature is typically used to allow employees to make long distance calls from the corporate PBX while out of the office by dialing in to the switch, then entering a code to make long distance calls. It is easily abused by anyone with the authorization code, possibly leading to large fraudulent long-distance charges.

Certain Account Codes may also be allocated for changing a user's Class of Service (COS). When the COS is changed, the user may have access to a different set of features. For example, most instruments may be assigned a COS that does not permit the use of an Override feature, but a special COS that is only accessible by using an Account Code may be created that does permit the use of Override. By using the Account Code, an adversary could then gain access to the Override feature.

Since the Account Codes are used for billing, there are records kept of the calls that are made for the various Account Codes. These records generally include the source, destination, Account Code, and time/date of the call. The records may be stored as files on one of the system's disks, or they may be printed out on a system printer. If the records are printed, an adversary who is able to gain access to the printer will have access not only to traffic information, but the printed Account Codes. Once the codes are known, the adversary will be able to use the codes for toll fraud, additional feature access, etc.

Testing for vulnerabilities with Account Codes may be performed as follows:

- Allow the use of Account Codes.
- Restrict an instrument so that long-distance calls cannot be made from it.
- Assign an Account Code that permits dialing long-distance.
- From the restricted instrument, attempt to dial a long distance number. The connection should not be made.

- From the restricted instrument, dial the Account Code set above and then dial the long distance number. This time the connection should be made. If the system has a printer attached, check to see if traffic information for the call is printed (possibly including the Account Code). Also check to see if records are kept on the system that may 'be accessible from the maintenance or administration terminal, or the Attendant Console.

- Attempt the same procedure as above, but intentionally dial an incorrect Account Code. Do this several times with various placements of the first incorrect digit. This will allow you to determine if the entire code must be entered before the code is rejected. A system that rejects incorrect codes at the first wrong digit allows the codes to be guessed more easily. This will also allow you to determine the length of an Account Code. The documentation may also provide information on the Account Code length and whether or not it is variable.

- Attempt to set up a DISA line that requires an Account Code. Dial into the DISA line and enter a valid Account Code. Attempt to use features such as Override, Silent Monitoring, Conferencing, etc. from the DISA line. Determine how much control is granted by the administrative tools for restricting/allowing the use of such features.

ACCESS CODES

Access Codes are frequently assigned to features so that users with simple instruments (e.g., traditional analog phones) may have access to these features. In determining vulnerabilities due to Access Codes, it is useful to determine to which features Access Codes can and cannot be assigned. For those that can have Access Codes assigned, determine from what types of lines and instruments the features are accessible. For example, allowing a Silent Monitoring feature to be accessed from an outside line can be a significant vulnerability.

SILENT MONITORING

A Silent Monitoring feature may be available that allows a user, given special access to this feature, to monitor other calls without the knowledge of the parties being eavesdropped upon. If such a feature exists, its use should be limited to as few people as possible to prevent unauthorized use. Potential vulnerabilities of a Silent Monitoring feature can be examined as follows:

- Enable Silent Monitoring for an extension or Access Code. Also ensure that any Silent Monitoring blocking features are disabled for at least two more extensions.
- Place a call between two unblocked extensions.
- Use the Silent Monitoring feature to monitor the call in progress. Observe the target instruments for visual/audible warnings that indicate that the call is being monitored. Also listen to verify that the Monitoring party cannot be heard.
- Look for ways in the administrative tools that Silent Monitoring can be disabled.
- Determine how Silent Monitoring is assigned. If the feature is assigned to a feature key on an instrument, physical access to such an instrument would grant an adversary access to this feature. Access to the database would allow the adversary to assign such a feature key to most other instruments.
- If an Access Code is assigned to the Silent Monitoring feature, determine the minimum and maximum lengths of the codes. Determine if the system allows "easy to guess" codes to be used such as all of 1 digit (e.g., 55555), a simple sequence (e.g., 12345), the user's extension, etc. If such limitations are not used, an adversary could guess the Access Code in a relatively short time. Also determine how invalid Access Codes are rejected. If an invalid code is rejected when the first incorrect digit is pressed, guessing Access Codes becomes a relatively easy task.

Conferencing

The common Conferencing feature could allow an adversary to eavesdrop on a conversation or add an additional party to a conference without the knowledge of the other parties. Potential vulnerabilities can be examined as follows:

- If necessary, permit several instruments the use of the Conference feature.
- Set up an ordinary call between two parties. Attempt to use the Conference feature to add another user to the call in progress.
- Once a conference is in progress, attempt to add parties to the conference from other instruments besides the conference initiator.

- If any of the above cases are possible, observe the instruments in the conference and look for visual or audible indications that a conference is in progress. For example, if any of the affected instruments have alphanumeric displays, the number of conference members may be displayed. There may also be an audible tone heard when a member is added to the conference.

- Different responses may occur with inside and outside lines. If the PBX supports both digital and analog instruments, there may also be different responses between the two line types.

It may also be possible to use a maintenance feature to establish a direct connection between the adversary's line and the conference bridge. If so, the adversary may become a permanent member of this bridge and able to monitor any conference call that uses this particular bridge.

- Take the adversary's line out of service.

- Attempt to directly connect this line to a line assigned to a conference bridge (preferably the "last" line).

- Establish a conference call using this bridge.

- Determine whether the adversary can overhear the conferees or be heard by them.

- If the adversary cannot hear the conference, try putting the line

- back in service and observe whether the direct connection is

- maintained and whether the conference can now be heard.

Additional steps may be necessary to ensure that the adversary cannot be heard. Using maintenance and administrative functions, try to detect the adversary's presence on the bridge.

OVERRIDE (INTRUDE)

An Override or Intrude feature is common to many PBXs. Due to its potential vulnerability, it is commonly selectable as a feature that can be allowed/disallowed on a single instrument or a group of instruments. Override is intended to allow one user (perhaps a supervisor) to break into a busy line to inform another user of an important message. This feature could be used by an adversary with access to any instrument permitted to use the Override feature to eavesdrop on conversations. The PBX should provide for some protection against such uses of Override by providing visual and/or audible warnings that an Override is in progress. The vulnerability of the Override feature can be tested as follows:

- If necessary, configure an instrument to permit the use Override.
- Place a call between two other extensions.
- Use the Override feature on the first instrument to attempt to break in to the call in progress.
- Note whether both parties can be heard by the Overrider and whether both parties can hear the Overrider. Also look and listen for indications on the target instruments that reveal that an Override is in progress. Audible warnings may come in the form of a single tone when the Override is initiated, periodic warning tones while Override is active, or a combination of the two.
- If any warnings are observed, look to see if there is any way of disabling them via the administrative tools.
- Try using Override with various combinations of inside and outside lines. There may be differences in the amount and type of warnings given between inside and outside lines.
- Look for any settings in the administrative tools that may disable the use of Override on an instrument or group of instruments.

AUTO ANSWER

Auto Answer is a common feature that allows an instrument to automatically go off-hook when called. The instrument is generally equipped with a speaker and microphone in addition to the handset. It is intended for use by people who may frequently not have their hands free to answer an incoming call (e.g., a hospital nursing station).

An adversary could use this feature to gain information that would not normally be available. For example, an instrument in a conference room could be set up for Auto Answer. Since the microphone in the room would be live, the adversary could then monitor a meeting remotely by simply calling that extension.

The degree to which this is possible depends on the specific configuration of the PBX and instruments evaluated. There is typically some warning given to a user that a call has come in and been answered by their instrument. The warning may be in the form of a light or other visual indicator on the instrument, or a ring from the instrument's ringer or speaker, or a combination.

The audible warning may be easily defeated by turning off the ringer or by turning down the speaker/ringer volume so that the warning is very quiet. The on/off or volume control may be a physical control on the instrument, or a remote control under the configuration of the system database. If it is remotely controlled, it could be changed without direct access to the instrument via access to the PBX configuration tools.

The ability of an adversary to make use of Auto Answer could be tested as follows:

- If necessary, configure an instrument and line for Auto Answer.
- From another instrument, call the instrument that has Auto Answer turned on. Look for visual warnings on the instrument and listen for audible warnings.
- Sounds in the room with the Auto Answer instrument should now be heard at the calling extension.
- If any warnings were noted, look for ways that they can be defeated. Try turning off/down the ringer and/or speaker volume.

If any warnings can be defeated, determine if the configuration is stored in the instrument or the PBX. Do this by configuring two of the same type instruments in different ways (e.g., one instrument set to high volume and one to low). Then swap the instruments between lines and note whether the configuration moved with the instrument or not. If not, it is likely that the configuration is stored in the PBX and not the instrument.

TENANTING

Tenanting is a feature commonly used to limit subscriber access to only those subscribers that belong to the same Tenant group. It would be used in a situation where one company owns a building or group of buildings and leases out parts of the buildings to other companies. The building owner may also own a PBX that is used to provide voice/data service to the tenants of the buildings. The tenants would all share the resources of a common PBX, but each would like to have its own configuration, Attendants, Trunk lines, etc. The Tenanting feature can be used to divide the resources of the PBX in this manner.

The operation of the Tenanting feature will vary from one PBX to another. The PBX may restrict the Tenant groups so that to each group, there appear to be no other users of the PBX. Alternately, the PBX may allow for adjustments in the restrictions placed between groups. Reducing the limitations between groups may be useful, but it introduces a potential vulnerability into the system.

If an adversary were to gain access to the PBX administrative tools, or access to the configuration database, the limitations between Tenant groups could be intentionally reduced. The adversary could create an additional Tenant group that has unrestricted access to all other groups. Instruments and/or trunk lines could be assigned to the new group that would allow the adversary to access the instruments and trunk lines of the other groups. Testing for Tenanting vulnerabilities can be done as follows:

- Create three different Tenant groups, each with some instruments and trunk lines assigned to it.
- If the restrictions between groups are adjustable, maximize the restrictions between the first two groups and minimize the restrictions between the third group and both of the others.
- Try to determine the level of restriction between the first two groups by placing calls between groups, setting up conferences between groups, combining members of both groups into the same ACD group, using an Override or Intrude feature between groups, and using one group's Attendant Console to access the other group's instruments (forwarding, messages, configuration, etc.).
- Perform tests as above between the third group and either of the first two groups.
- Compare the results of the above tests. If Tenant restrictions can be reduced, the Tenanting feature is a potential vulnerability.

VOICE MAIL

The voice mail feature of many PBXs can be a particularly vulnerable feature. This is because voice mail is typically used to let someone store voice messages at a central location by calling in from any inside or outside line and then retrieve the messages from any inside or outside line. It also grants the general public access to the PBX system.

Unauthorized Access to Stored Messages

In retrieving messages, the target extension and a password are usually required to gain access to the messages. Since the target extension is usually easy to determine, the only significant restriction to an adversary is the password. Once an adversary determines a target user's password, all messages left for the target user are accessible to the adversary. The adversary could also delete messages from the target user's mailbox to prevent an important message from getting to the target user. Some weaknesses of voice mail and answering machine passwords include the following:

- Default and obvious passwords. Once the target user's extension is known, try obvious passwords such as birth dates, other significant dates, and names that may be significant to the user. Default passwords (e.g., voice mail box number, '9999', '1000', etc.) established at system initialization time may never have been changed.

- Fixed length passwords. Check if a password entry can be terminated by a special key such as the # or * key. If not, the passwords may be of fixed length. Try to determine if the passwords have a fixed length and, if so, what that length is. This may be done by entering a known incorrect password slowly while listening to determine when the password is rejected. If such a limitation can be found, it reduces the number of random combinations that may be tried before a correct password is found.

- Non-terminated password entry. Some systems accept a continuous string of digits, granting entry when the correct password sequence is entered. For example, if the password is '896', and the sequence '1935896' is entered, the password is accepted and access granted. Attackers could use a simple algorithm to overlap digit sequences. By not requiring a password entry to be terminated, the length of the average sequence needed to guess a four-digit password is reduced by a factor of five.

- Check to determine if a complete password must be entered before an incorrect password is rejected. Do this by entering several correct digits followed by an incorrect digit. Does the system reject the password as soon as the first incorrect digit is entered or must the entire password be entered? If it is rejected on the first incorrect digit, sequential guessing becomes much more practical. For example, on such a system that has a fixed password length of four and uses the digits 0-9, it would take at most 40 sequential attempts to guess a password. On a system that required all four digits to be entered, at most 10,000 guesses would be required.

Denial of Service

An adversary may be able to use a PBX's voice mail system to damage the system in such a way that other users cannot access the voice mail system or even the entire switch.

Lengthy Messages

The amount of message time that can be stored on a voice mail system is typically limited by the size and number of hard disks allocated to voice mail. By leaving a user an excessively long message full of random noise, much if not all of the total message time can be used. The system may not be able to deal with a situation like this and crash, causing access to voice mail or the PBX to be limited. The system may impose a per-message time limit. If this is the case, multiple lengthy messages can still be left and have the same effect.

- Try to determine if the switch has a per-message time limit by attempting to leave a message so long that it uses all of the available space. You should use a message that consists of some sort of noise since most systems don't record silence.

- If the entire message space cannot be used in a single message or set of messages to a single user, try to determine if there is a per-user message space limit. Even if general access to the system cannot be denied in this manner, an individual user may still be denied incoming messages by filling the user's message space to its limit.

Embedding Codes in Messages

Many voice mail systems have playback features such as: Fast Forward, Rewind, Skip, Send a Copy, etc. These are typically accessed by pressing various digit keys during playback. It may be possible for an adversary to insert these codes into a message during recording in order to cause undesirable results if they are interpreted during playback. A few examples are listed below:

- An adversary could send a message to a target user that contains a Rewind code at the immediate beginning of the message. When the user plays back the message, it immediately rewinds to the beginning of the message and gets stuck in a loop playing back that message continuously.

- An adversary could send a message to a target user that contains a Send a Copy code and an extension for the copy's destination. If the target user's same extension is used as the destination, this may create a message that is duplicated every time it is played, thereby making a message that seemingly cannot be deleted. Even if the destination extension cannot be added to the message, during playback the system may still enter the Send a Copy mode requiring the user to enter a destination. This may create an annoying situation where a user must send the message to another user in order to delete it, causing the message to "float" around from one user to another until perhaps a system administrator can delete it.

- Try embedding playback codes into a voice mail message. If this is possible, try ideas similar to the examples above and determine how the system acts upon playback. The details will depend on the playback options available on each specific voice mail system.

Access to Outgoing Lines

- Some systems may allow access to the PBX via the Voice Mail system in a similar manner as a DISA line. If this can be done, an adversary may be able to gain access to many of the switch's features. Depending on which features are accessible, toll fraud and theft of information are possible. Checking for these types of vulnerabilities can be done as follows:

- Configure an extension for Voice Mail.

- From another extension, call the extension configured above and leave a message. Search through the available menu options for any options that may grant access to another line.

- Dial in to the Voice Mail system to retrieve the message. Search through the available menu options for any options that may grant access to another line.

- If any access to another line is possible when leaving or retrieving a message, further investigation is required.

- After getting access to another line, try using various Access Codes to attempt to use their associated switch features. Also try using Account Codes or Authorization codes to make long distance calls.

PRIVACY RELEASE

Privacy Release is a feature that may be used when more than one instrument shares the same extension. Frequently, instruments can be configured to support multiple extensions where some or all of the extensions are shared with other instruments. The PBX normally ensures the security of each line by allowing each extension to be used by only one instrument at a time. The Privacy Release feature disables this security by allowing instruments to connect to an extension that is already in use. Testing for vulnerabilities in the Privacy Release feature can be done as follows:

- Configure several instruments to have access to the same extension. Each instrument may only be able to have a unique primary extension. If this is the case, the redundant extensions may be able to be configured using programmable line keys on the instruments.

- Place a call between one of the extensions configured above and another extension or outside line.

- From one of the other extensions configured above, attempt to connect to the in-use extension. This should not yet be possible.

- Activate the Privacy Release feature on the instrument used in step two. This time the connection should be permitted. Look for any visual/audible indications on the three instruments that an additional party has connected to the call in progress.

- Check to see if the Privacy Release is specific to a single instrument or if it is global to all instruments sharing a particular extension by activating Privacy

Release on one instrument and then using two different instruments to test other's ability to use the same extension.

- Examine the additional features accessible from the Attendant Console and the maintenance/administrative terminal (if applicable). Attempt to determine if a feature exists that could allow an adversary to remotely control the status of an instrument's Privacy Release, or if it is only controllable at the instrument itself.
- If possible, examine the configuration database to try to determine if the status of Privacy Release is stored in the database or in the instrument. If it is stored in the database, an adversary with access to the database could remotely change the Privacy Release status of an instrument.

NON-BUSY EXTENSIONS

The Non-Busy Extensions feature typically allows calls to an in-use extension to be added to a conference with the existing parties when the extension is already off-hook. An adversary could configure a target instrument as a Non-Busy Extension and then call that extension to eavesdrop on a call in progress. The PBX should provide some form of warning to the user of the Non-Busy Extension that another party has joined the call in progress. Testing for vulnerabilities in the Non-Busy Extensions feature could be done as follows:

- Configure an extension as a Non-Busy Extension.
- Place a call between the Non-Busy Extension and another extension or outside line.
- From another instrument, place a call to the Non-Busy extension. Look and listen for visual and audible indications on the Non-Busy Extension that would indicate that another caller has been added to the call in progress. Types of warnings may include messages on an alphanumeric display, conference indicator lamps, and warning tones.
- Also observe the instrument to which the Non-Busy Extension was initially connected. Look for the same types of warnings as above.
- Try the above procedure using different model instruments as the Non-Busy Extension and its initial connection instrument. Also try various combinations

of digital, analog, and outside lines. There may be warnings that are present on one instrument or line that are not used on another.

DIAGNOSTICS

In addition to the major diagnostic features available at a maintenance terminal or Attendant Console, many PBXs provide diagnostics that can be initiated from any instrument. These diagnostic features may permit a user to make connections through the PBX by bypassing normal call processing restrictions. An adversary with access to these diagnostic features may be able to deny service or make undetected connections allowing for the monitoring of other calls. These features are commonly vulnerable when used in combinations with other feature vulnerabilities. Diagnostic vulnerabilities may be researched as follows:

- Study the PBX documentation to determine if there are any documented diagnostic key sequences. If so, try to exploit them to gain access to other lines what would not normally be permitted.

- Look for documented restrictions such as extensions that cannot be used. These may be used for undocumented diagnostics.

CAMP-ON

The Camp-On or Call Waiting feature allows a party to call into a busy extension and indicate to the busy party that someone is calling. The party wanting to Camp-On may be required to press a key that activates Camp-On, or Camp-On may be automatically activated when the calling party waits on the line. When activated, the called party may receive a visual and/or audible warning indicating that another party is Camped-On. Some typical options available are Forward, Trade to, and Conference with the Camped-On party.

If the calling party is brought into a conference, other parties on the call may or may not receive a visual or audible indication that another party is added to the conference. By using this feature, an adversary may be able to Camp-On to a party in a conference and be brought into the conference without the knowledge of some of the conference members. Testing the Camp-On feature can be performed as follows:

- If necessary, enable the Camp-On feature.

- Place a call between one instrument (A) and another (B).

- From another instrument (C) that is permitted to use Camp-On, call one of the other instruments (e.g., A). Camp-On to (A) by waiting or pressing a feature key as appropriate.
- Instrument (A) should receive an indication of the Camp-On. Connect to the Camped-On party (C).
- Try to bring instrument (B) into a conference with (A) and (C) perhaps with a Camp-On key, Conference key or FLASH.
- Check the instruments for visual or audible indications that a conference is now in progress.
- Try this procedure with different types of instruments, different lines (analog, digital, outside), and DISA lines.

Dedicated Connections

The use of Dedicated Connections allows connections to be made through the PBX without need for normal dialing sequences. Dedicated Connections may be used for creating a voice hot line between two instruments so that when one instrument goes off-hook, the other immediately rings. Another example is for a dedicated data line between a subscriber's PC or terminal and a central server or mainframe.

This can create a vulnerability in which an adversary could make a dedicated connection to a user's line and thereby eavesdrop on that line. Such changes may be possible if an adversary has access to the system's software, configuration tools, or database.

Feature Interaction Attacks

With the advent of the digital PBX and its wealth of features, the interaction between features presents a significant possibility for vulnerabilities. With such a large number of features available, it becomes difficult for the manufacturer to consider all of the combinations in which different features may interact. Because of this, vulnerabilities may exist that allow an adversary unwanted access to the PBX and its instruments.

Since the actual Feature Interaction vulnerabilities found on a specific system depend heavily on the particular implementation of the features, it would be nearly impossible to describe every possibility for a generic system. Listed below are a few examples that involve common features. In testing for Feature Interaction vulnerabilities, one should examine the features available, look for commonalities between features (keys, database configuration, etc.), and then test combinations you suspect may prove vulnerable. It is useful to try combinations that do not appear to have obvious potential for vulnerability because many Feature Interaction vulnerabilities are results of quirks in the implementation of the features.

In construction of a COS, Feature Interaction should be given much thought. Many of the feature vulnerabilities discussed involve Feature Interaction since several COS items or system options may have to be enabled/disabled to allow them to occur.

Call Forwarding/Return Call

A possible Feature Interaction vulnerability is the use of Call Forwarding to defeat the Return Call feature. Normally, if an adversary were to call a target user (perhaps harassment via the telephone), after the call is terminated, the target user could use the Return Call feature to call back the adversary and/or discover the adversary's extension (the returned extension may be displayed on an alphanumeric display when the call is returned). The adversary probably would not want the target user to discover this information. The adversary may be able to hide their extension from the target user by using Call Forwarding. The following procedure could be used to test for this vulnerability:

- Place a call from one extension (A) to another (B). The (B) instrument should have an alphanumeric display.
- Terminate the call at both ends.
- Attempt to use Return Call on (B) to call back (A). Observe the display on (B) for information about the extension being called back.
- If extension information is displayed, the adversary may be able to be located; if not, the adversary's call may still be returned.
- Forward (A) to another extension (C).
- Again place a call from (A) to (B) and terminate the call on both ends after (B) has picked up.
- Attempt to use Return Call on (B) to call back (A). Observe the display on (B) for information about the extension being called back.

- If the display shows (A)'s extension, then Call Forwarding cannot be used to mask the adversary's extension from Return Call.

- If the display shows (C)'s extension, then Call Forwarding can be used to mask the adversary's extension from Return Call.

- In any case, check to see which extension (A) or (C) is actually called back. The display on (B) may not agree with the extension that is actually called back.

Conference/Call Park

An adversary may be able to use the Call Park feature to intrude into a target user's Conference. Call Park is typically used to transfer a call to a busy extension. The busy user is informed of the parked call and can connect to it if desired. Conferencing may use the same key to bring a party into a conference as Call Park uses to connect to a parked call. This could allow an adversary to park a call onto an extension that is setting up a conference. When the conference is connected, the parked call may also be connected thereby unknowingly bringing the adversary into the conference. Testing for this vulnerability can be done as follows:

- Place a call from one extension (A) to another (B).

- At (A), place (B) on hold and connect to another extension (C).

- Place a call from extension (D) to (E).

- Use the Call Park feature to park the incoming call to (E) from (D) onto (A).

- Complete (A)'s conference with (B) and (C).

- Determine if the parked call onto (A) was brought into the conference with (B) and (C). If so, observe (A)'s instrument for information about the number of parties in the conference to determine if (A) is given any indication that there is an extra party in the conference.

Return Call/Camp-On/Caller-ID Blocking

The Return Call, Camp-On, and Caller-ID Blocking features may be combined to cause unwanted disclosure of telephone numbers. In the example below, caller (A) attempts to call (B) using Caller-ID Blocking so as not to disclose (A)'s telephone number. The example below illustrates how (B) can use Return Call and Camp-On to defeat Caller-ID Blocking and discover (A)'s telephone number:

- Using Caller-ID Blocking, place a call from (A) to (B).
- Do not answer the call at (B); hang up at (A).
- Use Return Call at (B) at to call (A) back.
- Answer the call at (A).
- Hang up at (B) and immediately use Return Call again to call (A) back a second time. Since (A) is still off-hook, Camp-On may be invoked (automatically or manually). Hang up at (B).
- Hang up at (A). The Camp-On takes effect and the switch rings both (A) and (B). Caller-ID information may be transmitted to both (A) and (B) at this time, disclosing (A)'s telephone number to (B).

COUNTERMEASURES

Because the vulnerabilities described in this section are inherent in feature implementation, they are difficult to defend against. In some cases not all features are needed, or may be turned off without major inconvenience to users. The most effective strategy is to ensure that only essential features are activated.

COMPUTER TELEPHONY

One of the biggest new developments in telecommunications is the advent of computer based telephony systems (CT). As microprocessor speeds have increased and memory prices dropped, it has become possible to implement a PBX on little more than a high-end PC. A CT system typically requires only the addition of specialized voice processing boards to an ordinary office PC with 64 MB of memory, a 3 GB disk, and 300 MHz processor. Some CT systems use specialized real-time operating systems, but the trend is toward commercial off-the-shelf systems such as Windows, Linux, or other versions of UNIX. This development has brought great reductions in the cost of PBX systems, but means the possibility of enormously increased security risks. Two factors in particular can increase exposure: greatly expanded integration of telephony with the computer network, and implementation of PBX functions over operating systems with widely known vulnerabilities. Some of the features appearing in new CT systems include:

- Voice over IP.
- Browser-based call handling and administration.
- Integration of IP PBX with legacy PBXs and voicemail systems.
- Integration of wireless networks with office network systems.
- Virtual private networks.

A complete exposition of the risks of CT systems is beyond the scope of this document. The safest course of action is to assume that most or all of the vulnerabilities described here apply to CT systems as well as traditional PBXs. CT systems may also have added vulnerabilities resulting from well-known weaknesses of PC operating systems. Future NIST publications may address CT security issues in more depth.

Selected Bibliography

NIST GCR 93-635 Private Branch Exchange (PBX) Security Guideline, September 1993

NS/EP Telecom News:
http://www.ncs.gov/n5_hp/Customer_Service/PTelecomNews.html

TSG Standard No. 1 - *Introduction to Telephone Security*

TSG Standard No. 2 - *TSG Guidelines for Computerized Telephone Systems*

TSG Standard No. 3 - *TSG Type-Acceptance Program for Telephones Used with the Conventional Central Office Interface*

TSC Standard No. 4 - *TSG Type-Acceptance Program for Electronic Telephones Used in Computerized Telephone Systems*

TSG Standard No. 5 - *On-Hook Telephone Audio Security Performance Specifications*

TSG Standard No. 6 - *TSG Approved Equipment*

TSG Standard (Interim) No. 7 - *Guidelines for Cellular Telephones*

Appendix A ABBREVIATIONS/ ACRONYMS

A/D	-	Analog to Digital Converter
ACD	-	Automatic Call Distribution
CODEC	-	Coder Decoder
COS	-	Class of Service
D/A	-	Digital to Analog Converter
DCE	-	Data Communications Equipment
DISA	-	Dial In System Access
DTE	-	Data Terminal Equipment
DTMF	-	Dual Tone Multi-Frequency
EEPROM	-	Electrically Erasable Programmable Read Only Memory
EPROM	-	Erasable Programmable Read Only Memory
ISDN	-	Integrated Services Digital Network
MOS	-	Maintenance-Out-of-Service
PBX	-	Private Branch Exchange
PROM	-	Programmable Read Only Memory
PSN	-	Public Switched Network
ROM	-	Read Only Memory
UART	-	Universal Asynchronous Receiver Transmitter

Appendix B
EXAMPLE SECURITY POLICY

This policy concerns the digital switching equipment (PBX) configuration, switch data, and maintenance and administration functions. This policy deals mainly with constraints that are enforceable through system software manipulation. Policy statements concerning physical, procedural, or administrative functions are discussed in Appendix B, Baseline Security Controls.

1. The switch will route all calls only to their intended authorized destinations.

2. The switch will prevent unauthorized access to, or tampering with existing connections or conversations.

3. The switch will prevent unauthorized disconnection of calls and support positive disconnection.

4. The switch will prevent unauthorized observation or manipulation of the subscriber database within the switch memory.

5. The switch will restrict the use of its resources and features to authorized users and subscribers, and will allow only authorized users to modify switch database attributes. The switch will log all unauthorized user access attempts as well as authorized user attempts to do unauthorized functions.

6. The switch will implement valid identification and authentication procedures for physical access to switch hardware and software.

7. The switch will maintain an audit trail of all security related incidents occurring within the switch and the audit information will be protected from unauthorized access, modification, or destruction.

8. The switch will exercise the option of providing control of privileged user access to switch functions, with each user only allowed access to its specific functions necessary to perform his/her duties.

access or use. Sensitive areas within the PBX area should be made physically secure during unattended time using such methods as locked doors, automatic detection devices, and positive identification and authentication controls. Personnel traffic and access to work areas should be minimized to authorized personnel only. Sensitive areas (e.g. switchroom, file storage area, and cross-connect terminal) should be placed or positioned in low traffic areas if traffic can not be controlled.

OPERATIONS SECURITY

The objective is to prevent compromise of PBX data. Applications, patches, supplements, and test programs are usually needed to test and upgrade the PBX system. In this regard, the PBX administrator will sometimes need to provide accurate real-time data to the firmware software developers or programmers. Sensitive data should be properly handled in a manner befitting its classification. Proper care should be exercised to minimize exposure of all PBX data not needed for the specific problems. Operations security also involves protection against unauthorized software or hardware modifications. ,It also involves prevention of trouble calls being overlooked, especially the ones that deals directly to PBX integrity (e.g. network integrity, memory mismatches, and carrier loss). All activity initiated within the PBX system should be logged and a record kept of this log. This log will encompass not only normal daily operational routines but also maintenance and trouble shooting procedures. If a problem was found and subsequently fixed, the steps involved in the whole procedure should be put in the log. Another objective is to detect unauthorized system use. Most PBX systems have within its security parameters the method to record, in memory, items such as system activity logs, journal files, exception reports, software errors, hardware errors, and operations and measurements parameters. These parameters or files should be constantly checked and updated, both manually and automatically. Back-ups of system configuration and database should be kept and maintained at least daily. Such back-up files should be kept in a secure area allowing access only by authorized personnel.

MANAGEMENT INITIATED CONTROLS

The objectives are to prevent loss of security support; prevent disclosure, taking, or unauthorized use of documents; and prevent inadequate PBX system controls. Personnel accountable for the security of the PBX should require that these areas are explicitly defined. PBX administration requires the use and filing of reports and other documents which includes security reviews, audits, PBX traffic reports, subscriber trouble reporting logs, and maintenance logs. These reports are sensitive and should be protected. Management should also be aware that there are other PBX owners/users and that they may have devised other ways of protecting their investments.

PBX System Control

The objectives are to avoid inadequacy of controls, to detect PBX systems and operations failures, and to prevent loss, modification, disclosure, or destruction of switch data assets. Third party vendor supplied PBX support programs (e.g. call detail recording systems) should be used without modification. Many of these programs have been developed with the controls and integrity built into them. Any modifications may possibly compromise its built in capabilities. Whenever changes are to be made in the PBX switch database or operating system, a review of the change should be made to make sure the new changes are necessary and will not compromise controls and integrity of the switch, have an unanticipated impact on some other part of the system, and/or interfere excessively with the existing system. Exception reporting on a periodic basis should be activated to report any deviations from the normal activity that may indicate errors or unauthorized acts. Exception reporting should occur when a specific control is violated, or may constitute a warning of possible undesirable events. Exception reporting should be recorded in a recoverable form within the system and when required, displayed to the PBX security administrator. Validation of all inputs to the PBX system should be performed, if it is not already automatic within the PBX, to assist in the assurance of correct and proper data entry. Validation should include checking for out-of-range values, invalid characters, and excess in upper/lower limits of possible entry.

PBX System Terminal Access Control

The objective is to prevent and avoid PBX system access exposure and control access to the PBX system database. Limiting the access to the PBX system and its database is an important means of security. It may be possible to control dial-up access to the PBX for maintenance and administration purposes. A PBX port interfaced to the Public Switched Telephone Network is exposed to access from telephones anywhere in the world. There may be a trade-off between PBX security and maintenance and administration accessibility. One alternative is to restrict access to the dial-up line to certain times of the day. Dial-up modem lines should be password or access code protected. Once access is given, whether via dial-up modem lines or on-site operations, administration, and maintenance terminals, care should be taken so that only authorized personnel are allowed access to data assigned to them. Users and others who have access to the PBX database should only be allowed to view, change, or manipulate the data that pertain to their specific job functions. Different types of database read and write privileges should be given to users with different job functions. Passwords to the PBX should be kept secret. It should be set up so that each user has a distinct and separate password of their own. This is to keep positive track of their activities. Access to the use of all terminals should be restricted to authorized users. This can be done by physically securing areas in which the terminals are located.

Password Management - Password control is essential to good security. Passwords should be controlled so that they expire after a period of time (e.g. 30 days). This type of password is considered reusable and is vulnerable if the password is seen (watched being entered) or monitored. To prevent this type of vulnerability, a device to generate a password based on some information (e.g. time, date, and personal identification number) that is valid for only a brief period (e.g. 1 minute). This type of device mitigates the reusable password problems but can isolate the user if the 'token device' is lost, stolen, broken, or the batteries expire (the batteries can not be changed by the user).

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Institute of Physics (AIP). Subscription orders and renewals are available from AIP, P.O. Box 503284, St. Louis, MO 63150-3284.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency or Internal Reports (NISTIR)—The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). In general, initial distribution is handled by the sponsor; public distribution is handled by sales through the National Technical Information Service, Springfield, VA 22161, in hard copy, electronic media, or microfiche form. NISTIR's may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

U.S. Department of Commerce
National Institute of Standards
and Technology
Gaithersburg, MD 20899–0001