Global Information Assurance Certification Paper

Securing the Other System: Basic PBX Functionality and Vulnerabilities

Brian L. Waldrop

GSEC Practical v1.2

April 24, 2001

Introduction

Hacking into a computer or data network is a well-known phenomenon and most organizations spend a great deal of time and money protecting the confidentiality, integrity, and availability of these resources. However, telecommunications fraud, in particular PBX and voice mail hacking, is relatively unknown to many organizations. According to research by Siemens Communications Limited (UK), "one of the main weapons that the [telecomm] hacking community exploits is the general lack of awareness of the problem within the UK [and the world]." In fact, their research showed that the "overwhelming majority of respondents … did not even know that it was possible to hack into an organization's telephone system." The potential for attack is very real, and failure to secure a PBX and voice mail system can expose an organization to toll fraud, theft of proprietary information, loss of revenue, and loss of reputation. As with information security, threats to corporate telecommunications system can be deterred with a combination of awareness, user education, formal security policies/procedures, centralized administration, and increased vigilance.

Scope

The purpose of this practical is to create an awareness of the basic functionality and feature configuration of traditional Private Branch Exchange (PBX) and voice mail systems plus the existence of potential vulnerabilities. This practical is not a systematic "how-to" manual, but rather an introductory guide for new system administrators and security professionals.

What is a PBX?

PBX stands for **P**rivate **B**ranch e**X**change, which generally refers to the privately owned circuit switch that serves as a branch of the switching equipment found at the central exchange office. A PBX uses embedded, proprietary software that contains customer-specified data and translations for routing voice, data, and video transmissions. These transmissions can be routed:

- Between users within an organization
- From users within an organization to users outside of the organization
- From users outside an organization to users inside the organization

Historically, the first installation of a Private Branch Exchange system reportedly occurred in 1879 at Dayton, Ohio's Old Soldier's Home. These early systems were quite literally branches of the central office switches. They served to exchange connections between telephones on the private premises of an organization or business. This function addressed the fact that the majority of calls made by a business enterprise are internal,

and these systems could make the required connections without relying on the services of the central office. Just as a central office switch eliminated the need to wire each telephone to every other telephone, PBXs eliminated the need to wire each on-site telephone to every other on-site telephone. It also eliminated the requirement to wire each on-site telephone to the central office.

Circuit Switching

With the rapid development of digital technology, PBX systems have evolved from hardwired, mechanical devices to flexible, software-configurable systems. Modern PBXs are by nature circuit switches optimized for voice traffic. According to Cisco Press' Internetworking Technologies Handbook, 2nd Edition, circuit switching is a "switching method in which a dedicated physical circuit is established, maintained, and terminated through a [shared switching matrix] for each session." At the request of an individual terminal device (telephone, fax, or analog modem), the circuit switch (PBX) will establish and maintain a connection to other such devices. These connections are established on a temporary, continuous, and exclusive basis for as long as they are needed. Since these circuits and the required bandwidths are not shared, an incoming or outgoing facility must be available at the time of each request.

Common System Components

While PBX manufacturers vary with respects to terminology and software functionality, the following system components are found in most PBX systems.

Terminal Devices: (Commonly called "stations") Voices telephone sets including fax machines, modems, and specified data terminals.

Station Lines: These lines serve as the transmission path between the individual terminal device and the switching matrix.

Line Ports: The actual interface between the PBX and the terminal device. These ports are found on Line Cards.

Trunks: Pairs of copper wire or optical fiber that connect the PBX to an outside system. Trunks are classified based on what type of system they connect to or the service that they provide.

- **CO trunks:** Trunks that connect the PBX to the Central Office. CO trunks may be restricted to outgoing only calls, incoming only calls, or both. Normally, CO trunks are used for incoming calls to a main number routed to the attendant.
- **DID trunks:** (Direct Inward Dial) CO trunks that carry incoming calls, and give remote callers direct dial access to specific extensions on the PBX.
- **FEX trunks:** (Foreign Exchange) Trunks that connect the PBX to PSTN telephone switches outside of the local area. FEX (or FX) trunks carry both incoming and outgoing calls.
- **Music trunks:** Trunks that carry the recorded music for Music on Hold.

Paging trunks: Trunks that connect the PBX to equipment used for paging.

RAN trunks: (Recorded Announcement) Trunks that carry the recorded announcements used by the PBX.

TIE trunks: Trunks that connect the PBX to a second PBX within a company's private network. TIE trunks carry both incoming and outgoing calls.

WATS trunks: (Wide Area Telephone Service) Trunks that provide long distance service via an Interexchange Carrier (IC).

Trunk Ports: The actual interface between the PBX and all trunk facilities. These ports are found on Trunk Cards.

Routes: (Also, called a Trunk Group) A defined set of trunks connected to the same end-system that processes the same types of calls.

Common Control: The common control mechanism controls all aspects of the PBX. This mechanism includes the Central Processing Unit (CPU); Memory; Disks; Input/Output Disk Unit; and Input/Output ports.

Switching Matrix: Controlled by the CPU, the switching matrix interconnects lines and trunks through either Pulse Code Modulation (PCM) or time division multiplexing (TDM).

Common PBX Features

A review of the product literature for the major PBX manufacturers shows that there are literally hundreds of features available with any PBX system. These features range from the basic to the highly sophisticated, but as with common system components there are several essential features found in the basic configuration of most PBXs. The system administrator implements these features to improve employee effectiveness, ensure customer satisfaction, and improve network effectiveness. The following are a few of these features.

Automatic Route Selection: (Also called Least Cost Routing) This feature allows a system administrator to program a sequential list of outgoing routes usually configured based on the cost incurred by the organization. These routes are groups of trunks assigned to specific end-systems or services that requires a user to meet a minimum restriction level for access. Once configured, the process provides users access to specific routes based on their restriction level and availability of other least costly routes.

Time of Day Routing (TOD): This feature allows a system administrator to apply time of day restrictions to the route selection process. Each entry or route in a route list can be assigned to TOD schedule that defines when a route can be accessed.

Access Restrictions: This feature allows a system administrator to limit a terminal devices' access to the public network, private network, and certain services and features. Basic access restrictions are generally broken into two forms: access restrictions for trunk groups or route, which specifies what trunk

groups a terminal device can use; and class of service, which specifies the degree of access for a device. Together they control which trunk groups a specific terminal device, DISA extension, TIE trunk, and authorization code can access; and determine whether users can make local, TIE, or long distance calls over those trunk groups. These restrictions can be overridden by the use of other system features.

Authorization Codes: (Also called "authcodes") These codes are used to identify and control users. Without individualized authcodes, call privilege restrictions are associated with the specific terminal device not a user. Hence, authcodes allow restrictions to follow the user, and improve the effectiveness of the Call Detail Recording application.

Automatic Call Distribution (ACD): A feature used when a large number of incoming calls are queued and answered by a group of telephones (referred to as agents). The longest waiting call is sent to the agent that has been idle for the longest time. ACD also includes "Supervisor" features for controlling call distribution, monitoring agent activity, and listening to active calls.

Call Forward: This feature allows a user to manually forward incoming calls to an internal extension or a valid external number. Incoming calls can be forwarded based on a given situation including Busy, No Answer, Call Type, and All Calls.

Hunting: This feature allows incoming calls that encounter a "busy" or "no answer" extension to route automatically to another extension in a predefined path, known as the hunt chain.

Call Transfer: This features allows an internal user (Caller A) on a two-way call to put the existing party (Caller B) on hold and place a call to any valid internal extension or external number (Caller C). Once the Caller C answers the call, the internal user (Caller A) can transfer the existing party, Caller B, to Caller C.

Call Detail Recording (CDR): This feature captures call information based on a defined criteria for accounting purposes. For each selected call type, CDR identifies the calling parties and called parties and notes the time and duration of the call. Reports can be configured to capture data based on call type, trunk groups, extensions, and authorization codes just to name a few.

Direct Inward System Access (DISA): This feature allows selected offsite users (callers) access to the system from the public or private network by dialing a special extension assigned by the system administrator. Once the PBX has answered the DISA call, the offsite caller can use the system as an internal user. Administrators can control DISA extensions with access restrictions, security codes, and authorization codes.

Attendant Console: This feature allows a console operator or attendant to assist in placing and extending calls into and out of the PBX. Consoles are provided with many call-processing features that can include the ability to control trunk groups.

Remote Access: This feature allows an offsite administrator or support technician to dial in and assume administrative control of the system software and hardware. Terminals, PCs running terminal-emulation software, or specially programmed maintenance telephones can be used for this function. In addition, some newer systems support Point-to-Point (PPP) protocol.

Voice Mail

Voice Mail is an optional software application and call-processing system that uses predefined voice services to answer calls routed from the PBX to the voice mail system. In most systems, virtual ACD agents are used to create voice channels or paths between the PBX and the voice mail system. Once these channels are created, the Call Forwarding and Hunt features are used to route incoming calls to the voice mail system for processing. The system administrator can specify how and when calls flow to and from the voice mail system by controlling both the station and ACD agents. Once routed, the system can process calls with one of the following services or features.

Automated Attendant: The most basic version of this service allows incoming callers to use a thru-dial service. Once the call in answered by the PBX and routed to the voice mail system, the caller receives a message prompting them to dial by extension number or dial by name. If the caller does not respond, the call is routed to a live attendant.

Voice Messaging: This service is the most commonly used service in voice mail systems. The incoming call is routed to the appropriate mailbox, and the caller is played a recorded greeting and prompted to store a private message. Usually, the system administrator will create a mailbox for each assigned extension.

Voice Announcements: An announcement is recorded message played automatically to callers. Announcements are the simplest form of voice service, yet they can be very effective in providing specific information to callers. Announcements do not accept input from the caller - they simply provide information.

Voice Menus: This service offers a caller a series of options. A simple voice menu consists of a greeting followed by a list of options and the corresponding key that the caller must press to make a given selection (one layer). The system administrator can pre-assign actions for each listed option or allow thru-dialing. More complex menu or applications involve creating several layers of voice menus and linking them together to create multilevel menus.

Thru-Dialing: This feature is normally associated with voice menus for the purposes of handling calls. Thru-dial services allow call accessing a voice menu to dial out of the voice mail system to internal or external numbers. The system administrator can apply dialing restrictions by using a restriction and permission table found in the voice mail system. In addition, most voice mail systems include some form of thru-dial monitoring to track calls to and from the service.

Outcalling/Remote Notification: Outcalling is an optional feature that provides for external messaging. Remote Notification is the most common type of outcalling. When a message is received, it informs the user of the new message by contacting a remote device such as pager, paging service, or another telephone. In most situations, users define what of remote device and input the number for the device. However, the system administrator can apply dialing restrictions for the outcalling/remote notification in the voice mail system's restriction and permission table.

Telecommunications Fraud

Telecom fraud has existed since the 1970s when "telephone hackers", or phreakers, called their families and friends using stolen credit calling codes, "blue boxes", or cereal box toys, and the problem continues today. From the late 1970s to the mid-1980s, the advent of PCs, modems, password crackers, and autodialers allowed hackers to hone their skills and attack systems remotely with efficiency and easy. However, telephone operating companies are no longer the primary target for telecom fraud because these companies have decreased their vulnerability by aggressively using software controls and prosecuting phreakers. For this reason, phreakers have migrated to new, less risky targets - customer premise targets (like PBXs and voice mail systems). In 1998, studies showed that telecom fraud resulted in an estimated revenue loss of $13 billion worldwide and that figure will reach an expected $28 billion by 2003. So the existence of real threats and vulnerabilities can easily be documented and the financial losses to an organization can be huge.

Common Threats To PBXs and Voice Mail Systems

In the Department of Commerce publication, PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, NIST compiled the following list of potential threats based of the perceived goals of phreakers.

- **Theft of Service -** The common motive for attackers, Toll Fraud.
- **Disclosure of information -** The disclosure of confidential and/or proprietary information, including conversations and system configuration data.
- **Data modification -** The illegal modification of system configuration data or records.
- **Unprivileged access -** Access by unauthorized users to gain control of system resources or privileges.
- **Denial of service -** Attacks that lead to the deterioration of service or suspension of functionality.
- **Traffic analysis -** A passive attack that allows phreakers to view calling patterns and make conclusions based on the source and destination of calls.

Common Vulnerabilities

PBXs and voice mail systems can provide a vast array of useful features for an organization and its employees, but a phreaker or staff member can abuse even of the most well intentioned feature or service. The level of vulnerability presented by these features and services are unique for each system because each scenario is a combination of the physical environment, system configuration, functions, and features supported by that system. Therefore, a comprehensive list of vulnerabilities is beyond the scope of this practical. However, a review of PBX/voice mail security and phreaking web sites turned up five common vulnerabilities: physical security; remote access; DISA; call forwarding, and thru-dialing. At the very minimum, system administrators and security professionals can use these vulnerabilities as a starting point in a complete security analysis.

Physical Security: The most basic method for securing any system is restricting access to the actual hardware and system documentation. Without physical

security, a most securely designed system is still at risk. When reviewing physical access, consider the following:

Switchroom Security: When switchroom is not secure, an attacker has access to the software, system administrative database, system documentation, and often the "demarc" location for all incoming copper and/or fiber trunks. Activities can be as simple as turning off printers or as malicious as removing cards or equipment and rendering the system inoperable.

Suggested countermeasures:

- Physically lock the main switchroom and all other distribution closets.
- Maintain a log (preferably electronic) for all personnel accessing the switchroom.
- Require positive identification for all service technicians and vendor personnel.

System Printouts/Documentation: The access to and destruction of all system printout and out-of-date system documentation is a critical issue. System output can include: configuration records, call detail records; access codes/authcodes for trunks and special calling privileges; and remote access numbers. Phreakers, known as "dumpster divers", search dumpsters and trash bins looking for such data.

Suggested Countermeasures:

- Treat all system printouts and documentation as proprietary information.
- Keep required printouts and system documentation under lock and key.
- Shred or securely destroy all out-of-date material.

Remote Access: Unless deactivated, most PBX and voice mail systems allow system administrators and/or switch vendors to remotely access system resources for administrative and maintenance functions. These ports enable an outside caller to dial directly into the system in order to gain administrative control of the system hardware and software. In addition, many manufacturers incorporate "secret" diagnostic passwords to gain access code-level system functions. The importance of these issues speaks for itself, and it is imperative that security measures are taken.

Suggested Countermeasures:

- If possible, deactivate the remote access service.
- Do not use default passwords for any administrative account.
- Implement strict procedures for maintaining and deleting administrative accounts and passwords (including unnecessary accounts used during installation).
- Implement password timeout features after a specified number of incorrect password attempts.
- Do not publish or display passwords or modem numbers.

- Configure an A/B switch box between the administrative terminal and the access modem that requires a staff member to grant access to the system via the modem.
- Configure and print system history files to capture maintenance and service change activities.

Direct Inward System Access (DISA): Perhaps, the most commonly abused system feature. DISA offers a convenient means for offsite employees to place calls to internal extensions, private network locations, and external numbers by accessing the PBX. Often, phreakers use PC-based programs to find valid DISA extensions; crack the security and authorization codes; and store the valid extensions and codes. The information can be "personal use" or sold in a "Call Selling" scheme.

Suggested Countermeasures:

- Consider deactivating the feature and issuing corporate calling cards.
- Do not publish or display DISA extensions, security codes, or authorization codes.
- Implement strict procedures for maintaining and changing security and authorization codes.
- Configure CDR to capture data on all calls to and from DISA extensions.
- Explore toll fraud monitoring services by long distance and local service providers.
- Restrict access by DISA extensions to long distance and international trunks by restricting the trunk group access and class of service for those extensions.
- Use time-of-day controls for all trunks associated with DISA extensions in order to curb after-hours abuse.

Call Forwarding: Call forwarding is a convenient feature that allows users who are going away from their desk to forward their calls to another set or location. Station users, or anyone with physical access to the station, can abuse this feature by forwarding the station to either a long-distance telephone number or a direct trunk access code. Direct trunk access is an administrative and maintenance function used to gain control of trunks that bypassing all access and routing restrictions. Unrestricted, direct trunk access grants unparalleled call privileges to a knowledgeable caller. This action can be for personal use or sold in a "Call Selling" scheme.

Suggested Countermeasures:

- Restrict call forwarding to internal extension only.
- Block all forwarding to direct trunk access codes.
- If forwarding to a long distance is required, use time-of-day controls for trunks associated with these extensions in order to curb after-hours abuse.

- Configure CDR to capture outgoing calls from extensions allowed to call forward to external numbers.

Thru-dialing: A thru-dialing service performs basic call handling by allowing a caller to direct their own calls and reduce the need for a live attendant. In addition, this service can be used in voice menus serving offsite employees in a function similar to DISA. Because thru-dial allows a caller to call directly from the voice mail system, callers can dial both internal extensions and external numbers. Unrestricted, these external calls can be made to local, national, and international numbers similar to that of unrestricted DISA extensions.

Suggested Countermeasures:

- Block external dialing via voice menus by using restriction and permission tables found in the voice mail system.
- Where external dialing is necessary, system administrators can restrict usage by implementing and requiring access codes.
- Do not publish or display thru-dial access numbers or access codes.
- If installed, the system administrator can configure the thru-dial monitoring function to capture both outgoing calls and unsuccessful attempts to access the service.

Conclusion

PBX and voice mail systems have become integral parts of businesses, institutions, and government agencies throughout the world. The flexible nature and vast array of features offered by these systems allow administrators countless possibilities for addressing the needs of their end users and customers. However, the flexibility and feature configuration can make them vulnerable to abuses by employees as well as outside sources. System safeguards must be implemented to control access to these features and services. In addition to system safeguards, administrators should exercise control when handling and disposing of information that can compromise system security. Inadequate control calling privileges, like DISA, call forwarding, and thru-dialing, and unrestricted physical access to the switching system are the main reasons organizations incur unnecessary financial losses through use of their telecommunications facilities. Organizations must realize that vulnerabilities can and do exist, and unfortunately there are people who are motivated to do bad things. For this reason, it is worth taking PBX and voice mail security seriously.

References

Boccadoro, Diane. "PBX Protection." 1 July 1999. URL: http://www.teleconnect.com/article/TCM20000509S0022 (11 April 2001).

CommWeb.com. "PBXs." 3 October 2000. URL: http://www.coomweb.com/article/COM20001003S003/3 (15 April 2001).

Dodd, Annabel Z. The Essential Guide to Telecommunications, Second Edition. Upper Saddle River. Prentice Hall PTR, 2000.

Downes, Kevin, et. al. Internetworking Technologies Handbook, Second Edition. Indianapolis: Cisco Press (Macmillan Technical Publishing), 1998.

Hybrid. "Meridian I Hacking." URL: http://hybrid.dtmf.org/files/hybrid-files/mer-hack.txt (7 April 2001).

Hybrid. "Hacking Meridian Mail - An Overview." URL: http://hybrid.dtmf.org/files/hybrid-files/mer-ninj.txt (7 April 2001).

Laino, Jane. "Your Telecom Equipment Room: The Grand Tour. 6 November 2000. URL: http://www.teleconnect.com/article/TCM200001031S0003 (11 April 2001).

Nortel Networks. Meridian 1 Options 21 through 81c: System Programming Guide. Standard 5.00. Canada. Nortel Networks Corporation, June 1999.

Nortel Networks. Meridian 1: X11 System Security Management. Standard 5.00. Canada. Nortel Networks Corporation, June 1999.

Siemens Communication Unlimited. A Management Guide to the Prevention of Telephone Fraud in the UK. 1998. URL: http://www.siemenscooms.co.uk/useful_information/collateral_archive/fraud.pdf (13 April 2001).

"The Private Branch Exchange (PBX)." URL: http://www.tollfree.com/basic/pbx/pbx.htm (2 April 2001).

United States Department of Commerce - National Institute of Standards and Technology. "PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does." Special Publication 800-24. August 2000. URL: http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf (6 April 2001).

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event