August 2000

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY FOR PRIVATE BRANCH EXCHANGE SYSTEMS

By Richard Kuhn, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Hacker attacks on computer networks are well known, but Private Branch Exchange (PBX) systems are also vulnerable. In one case, a hacker penetrated the Private Branch Exchange (PBX) system operated by a hospital in Escondido, California. For nearly two years, on various occasions, he blocked calls to and from the hospital, connected hospital operators to spurious numbers (including the county jail), and placed bogus emergency calls that appeared to be coming from inside the hospital.

Unfortunately, the hospital's experience is not unique. Failure to secure a PBX system can result in exposing an organization to toll fraud, theft of proprietary, personal, and confidential information, loss of revenue, or legal entanglements. Depending on how the organization's network is configured and administered, information leading to intrusions of data networks may be compromised as well. 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. This bulletin introduces some of the vulnerabilities of PBX switches and describes some countermeasures that can be used to increase the security of your PBX. For a more detailed treatment of these issues, see NIST Special Publication (SP) 800-24, *PBX Vulnerability Analysis* (see http://csrc.nist.gov).

Introduction

Digital PBXs are widespread throughout government and industry, having replaced their analog predecessors. 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 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 and 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; time-dependent operations 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.

PBX Characteristics

PBXs are sophisticated computer systems, and many of the threats and vul-

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since February 1999

- *Enhancements to Data Encryption and Digital Signature Federal Standards*, February 1999
- *Measurement and Standards for Computational Science and Engineering*, March 1999
- *Guide for Developing Security Plans for Information Technology Systems*, April 1999
- *Computer Attacks: What They Are and How to Defend Against Them*, May 1999
- *The Advanced Encryption Standard: A Status Report*, August 1999
- *Securing Web Servers*, September 1999
- *Acquiring and Deploying Intrusion Detection Systems*, November 1999
- *Operating System Security: Adding to the Arsenal of Security Techniques*, December 1999
- *Guideline for Implementing Cryptography in the Federal Government*, February 2000
- *Security Implications of Active Content*, March 2000
- *Mitigating Emerging Hacker Threats*, June 2000
- *Identifying Critical Patches with ICAT*, July 2000

nerabilities associated with operating systems are shared by PBXs. There are two important ways, however, 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, provides the possibility of unexpected attacks. An attacker may use a feature in a manner that was not intended by its designers. Features may also interact in unpredictable ways, even when implemented correctly, leading to system compromise even if each component of the system conforms to its security requirements and the system is operated and administrated correctly.

Maintenance

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

Special Manufacturer's Features

There may be features that the manufacturer will rely on 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 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 primary reason for adding such special features. A switch manufacturer would not want the special features to be well known because of their potential for misuse. These types of features may be accessible via login IDs and passwords held privately by the manufacturer. Some possible special 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 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.

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 many dial-back modems are well known.

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.

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, some

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our Web site is http://www.itl.nist.gov/.

form of password protection usually restricts it. 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.

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 maintenance personnel use only one, the others may remain at their published factory settings. Anyone who knew the factory default settings could then gain access to the switch.

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 access to the PBX, an adversary could exploit practically any conceivable vulnerability.

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 rather than socketed, making removal and replacement difficult. Likewise, an internal hard disk is probably mounted internally and bolted to 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 readily available, an adversary may find it 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 have 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 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.

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.
- *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.

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. An adversary could intercept a software update sent to a PBX administrator. 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.

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.

■ Many software packages use error detection codes to protect against transmission or disk copying errors. Conven-

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

tional 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.

■ 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 sensitive memos or financial information.

■ To ensure the security of printouts, they must be shredded when discarded.

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 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 than 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, but there are potential vulnerabilities of the Attendant Console with respect to maintenance and administration. 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. An adversary with access to an Attendant Console could use this 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.
- *Attendant Forwarding*
  A common feature granted to the Attendant is the ability to control 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.
- *Attendant Conferencing*
  Attendants may also have the ability to initiate a conference or join into an existing conference. If this feature is available, the potential exists for an adversary logged in as an attendant to eavesdrop on a conversation or add an additional party to a conference without the knowledge of the other parties.

Automatic Call Distribution (ACD)

ACD allows a PBX to be configured so that incoming calls are distributed to the next available agent (e.g., reservation clerk) 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. Because of this feature, ACD systems are a potential vulnerability to the users of PBX. If an adversary could gain access to the configuration tools or the system database, they could become an ACD supervisor and set up an ACD group. The supervisor could then monitor the calls of any of the users in the group.

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 also to 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.

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 instru-

ment 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 (perhaps a subordinate) 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.

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.

Feature Interactions

With the advent of the digital PBX and its wealth of features, the interaction between features presents a significant possibility for vulnerabilities. For example, in some systems the return-call and camp-on features can be manipulated to defeat caller-ID blocking. With the large number of features available in modern PBXs, it becomes difficult for the manufacturer to consider all of the ways in which different features may interact. Because of this, vulnerabilities may exist that were undetected by the manufacturer 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. NIST SP 800-24 includes detailed examples of some feature interactions.

Countermeasures

■ Vulnerabilities can be minimized if the Attendant Console connects to the PBX with a different physical 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.

■ When implementing a Class of Service, 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.

■ Because the vulnerabilities described in this section are inherent in feature implementation, they are difficult to defend against. 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 a 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, and

■ 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.

Recommendations

Not all of the security measures described in this bulletin will be applicable to every organization. The first step in improving PBX security is to assess the organization's current telephony applications. This bulletin describes important areas to consider. Following this assessment, NIST SP 800-24 can be used in conducting a detailed evaluation. SP 800-24 also includes a set of baseline security considerations for PBXs and a more complete set of countermeasures for common vulnerabilities.

References

NIST SP 800-24, *PBX Vulnerability Analysis*, National Institute of Standards and Technology, 2000.

Online resources:

■ NIST Computer Security Resource Clearinghouse: http://csrc.nist.gov

■ DISA Information Assurance: http://www.disa.mil/infosec/iaweb/default.html

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8901
Gaithersburg, MD 20899-8901