Avaya™ Interactive Voice Response Security

Abstract

This paper provides information on the security strategy for Avaya Interactive Voice Response (formerly known as CONVERSANT® IVR). It also provides suggestions that companies can use to improve the security of their Avaya IVR systems and applications.

Contents

This page intentionally left blank.

1. Introduction

Avaya™ Interactive Voice Response (formerly known as CONVERSANT® IVR) is a self-service software platform for voice and speech applications. Avaya IVR empowers enterprises to automate common customer interaction and fulfillment tasks via touchtone, fax, or natural language speech.

This paper provides information on the security strategy for the following Avaya IVR products: CONVERSANT System Version 8.0 and Avaya Interactive Voice Response Release 9.0. It also provides suggestions that companies can use to improve the security of their IVR systems and applications.

In this paper, the term "IVR" will be used to refer to either the CONVERSANT V8.0 platform or the Avaya IVR R9.0 platform. Also, "companies" will be used to refer to the organizations that purchase the IVR systems and/or implement the IVR applications. "Customer" will be used to refer to an end-user of the IVR application.

Note: Avaya Inc. is providing the information contained in this document as a helpful tool. Avaya makes no representations or warranties that implementing the suggestions recommended in this document will eliminate all security threats to the IVR system and its applications. Avaya disclaims any responsibility for or liability associated with the information herein.

2. IVR Security Strategy

Avaya IVR is a sophisticated software platform for the development of advanced customer self-service solutions. Because the product is a platform, the security strategy for the product revolves around controlling access to the platform.

IVR security protection falls mainly into two areas. The first area deals with the security of the operating system and the associated platform software. The IVR system supports standard Unix security interfaces (e.g., user authentication, shoulder surfing protection, and encrypted password storage). In addition, companies may perform further system hardening as described in subsequent sections of this document. The IVR system also provides role-based authorization capabilities for controlling access to its menu-driven administration utilities.

Secondly, all dial-in lines are protected by an Avaya-developed solution called Access Security Gateway (ASG). For more information on ASG, refer to section 8.

Companies, their application developers, and independent software vendors use IVR features and capabilities to create applications that meet the end customer's self-service needs. The design of the self-service solution should include any security considerations that are appropriate for the

company's environment. For example, companies should ensure that sensitive customer data is not logged in plain text files and that the data is protected from unauthorized access and modification. IVR applications and scripts must also be written and audited to ensure that customer data is not inadvertently exposed in the application and that holes do not exist in the application that might allow attackers access back to the PBX to perform unauthorized calling. For more application development guidelines, see section 10.

Companies may use the capabilities of the operating system or other custom-developed solutions to implement the required application-level security. However, Avaya strongly discourages incorporating additional software (such as third-party auditing tools) or using the installed software for purposes not intended by Avaya. Although Avaya appreciates the benefits of installing software that conforms to a company's security policy, we strongly recommend that no additional software be loaded onto the IVR server that could potentially disrupt the performance or operation of the server.

3. Securing Access to the System

One of the most important steps in ensuring the security of a system is to limit ways by which individuals can access the system.

3.1. Physical system security

The IVR system should be placed in a physically secure environment that can only be reached by a limited number of trusted individuals. Putting the system in a location that allows free access by any employee creates the risk that someone could disrupt the operation of the IVR system, whether unintentionally or maliciously. The IVR system should be isolated from everyone except those people who are specifically authorized to access it.

3.2. Isolated LANs

Any server that is connected to the Internet is potentially subject to unauthorized use and malicious attacks. IVR systems can be protected by configuring them on a LAN that has no physical connection to the Internet or to an internal network that is considered hostile in nature. Sometimes referred to as an "island LAN," this type of network environment has its own LAN switch and contains only those network elements with which the IVR system needs to interface, such as speech servers, database servers, and a backup server. Because this LAN has no physical connection to the Internet, there is no risk of unauthorized access from external sources. As such, there is no need to use a firewall to protect the system from unauthorized use.

Physically isolating the LAN provides strong protection against fraudulent access. However, isolating the LAN may restrict a company's ability to remotely administer and/or maintain their IVR system. Companies should consider the requirements of their operating environment before deciding whether to place the IVR system on an island LAN.

3.3. Firewalls

If the LAN cannot be isolated, Avaya strongly recommends using a firewall product to protect the internal LAN, including any IVR servers, from unauthorized access. Firewalls sit between a LAN and the Internet and control access to designated ports.

Firewalls are commonly used to prevent denial of service attacks to application servers, snooping of sensitive data, and "hijacking" access sessions to appear as an authorized user. Most firewalls can be configured to allow specified remote IP addresses to connect to designated ports using only specified protocols.

4. Platform Security Hardening

Avaya IVR is based on the UnixWare 7.1.1 operating system. UnixWare offers C2-level security capabilities. Companies may use the operating system capabilities to further harden the security of the platform.

The hardening recommended in this paper should be performed by a system administrator who is familiar with the UnixWare operating system or by a qualified technical consultant. The Avaya Enterprise Security Practice, part of Avaya Network Consulting Services, can help perform this hardening while providing a total security solution that is tailored for a company's specific needs. In addition to providing hardening services on the IVR system, they can also provide wide-range security services on a variety of Avaya telecommunications equipment such as Call Management Servers and PBX systems.

For more information or to contact the Avaya Enterprise Security Practice, call them at 1-866-832-0925 or refer to http://www1.avaya.com/services/portfolio/security/index.html.

4.1. Disable Unneeded Network Services

The IVR platform is shipped with all network services enabled by default. This is the most flexible configuration; it allows companies to use any services that are needed by their IVR application and operating environment. However, many network services are subject to security vulnerabilities that may allow unauthorized individuals to access the system.

The IVR platform requires the use of relatively few network services. Therefore, Avaya recommends that companies disable any network services that are not required for the IVR system and which are not needed for the companies' business purposes. Doing this can mitigate known (and future) security vulnerabilities.

The following sections provide information on services that may be needed by the IVR system as well as services that companies may be able to disable.

NOTE: The information in the following sections may be used to harden the security of the IVR platform without affecting basic IVR functionality. However, companies may require the use of the services discussed in these sections based on the platform features that are used, how the IVR application is implemented, or other site requirements. In addition, some of these services may be needed if companies use features or functionality provided by third-party vendors.

It is strongly recommended that companies create a full backup of the system before implementing any of the steps recommended in the following sections. Companies must also fully test their system after implementing these steps to ensure that performing this hardening does not have any unintentional side effects on their application and/or operating environment.

4.1.1. telnet

The telnet service provides a mechanism for connecting to a host machine from a remote system.

The telnet service is not needed for IVR operation. It can be disabled if desired. However, companies should not disable the telnet service unless they have another means of accessing the system, such as using the system console or Secure Shell (see section 5).

If the telnet service is needed, companies should implement the telnet security hardening described in section 4.3.

Service	Port	Protocols	Purpose
telnet	23	tcp	Allows connections from remote systems

4.1.2. FTP

The File Transfer Protocol (FTP) service provides a mechanism for transferring files to and from remote systems.

Avaya IVR Designer (formerly known as Voice@Work™), the PC-based service creation tool for IVR applications, uses FTP to transfer applications to the IVR system. Therefore, the FTP service must remain enabled if companies plan to develop and install applications using IVR Designer.

Companies may disable FTP once the IVR Designer application development is complete and the final application has been installed on the IVR system. If necessary, they can temporarily re-enable FTP if they need to update the application later.

Many companies also use FTP for their normal operating procedures. For example, companies sometimes use FTP to retrieve reports from the IVR system. In these situations, it is preferable

for the IVR system to initiate the file transfers. Doing this allows the IVR system to act as the FTP client instead of the FTP server. As such, the FTP service does not have to be enabled on the IVR system.

If FTP is not required for IVR Designer application transfers or for other business practices, the FTP service can be disabled. If it is required, companies should implement the additional hardening practices described in section 4.4.

Service	Port	Protocols	Purpose
ftp	21	tcp	File Transfer Protocol service

4.1.3. exec

The exec service allows a remote system to invoke a process on a host machine.

Avaya IVR Designer uses the exec service for performing various functions such as installing applications on an IVR system or assigning the applications to channels on the IVR system. Therefore, the exec service must remain enabled if companies plan to develop and install applications using IVR Designer.

If IVR Designer is not used, the exec service may be disabled. Companies that use IVR Designer may also choose to disable the exec service once the IVR Designer application development is complete and the final application has been installed on the IVR system. If necessary, they can temporarily re-enable the exec service if they need to update the application later.

Service	Port	Protocols	Purpose
exec	512	tcp	Invokes a process on a host machine

4.1.4. ORACLE Services

The ORACLE database server provides database services to ORACLE clients. It must be enabled if ORACLE is installed and used on the IVR system. The port used by the database server can vary on each system and change after each system boot. Usually, however, the port number is greater than 32000.

The ORACLE listener service allows the IVR system to communicate with ORACLE databases on remote systems. The ORACLE listener service is required if the system needs to communicate with remote ORACLE databases. If this is not required, it can be disabled.

The ORACLE listener process is not enabled by default after system installation. It is normally enabled only if it is needed.

Service	Port	Protocols	Purpose
oracle	*dynamic*	tcp/udp	ORACLE database server
listener	1521	tcp	ORACLE listener service

4.1.5. inetd Internal Services

The inetd internal services are primarily intended as debugging and measurement tools. The IVR system does not require these services. Companies may disable them as a security hardening measure.

The internal services are as follows:

Service	Port	Protocols	Purpose
echo	7	tcp/udp	Echo service – sends data back to its originating source
discard	9	tcp/udp	Discard service – throws away any data received
daytime	13	tcp/udp	Daytime service – sends the current date and time as a character string without regard to the input
chargen	19	tcp/udp	Character generator service – sends a stream of data and throws away any data received
time	37	tcp/udp	Time service – sends the time (in seconds since midnight on January 1, 1900) back to the originating source. This service is used for clock synchronization.

4.1.6. RPC Services

The Remote Procedure Call (RPC) protocol provides a high-level mechanism for programs on networked platforms to communicate with programs on remote systems.

The IVR system does not require RPC services. Companies may disable these services if they are not required for an IVR application or its operating environment.

The RPC services are discussed in more detail in the following sections.

4.1.6.1 rpcbind

There is no fixed relationship between the addresses that a given RPC program will have on different machines. Thus, the port numbers used by the RPC services (with the exception of the rpcbind program) will generally vary on each machine.

The rpcbind program converts RPC program and version numbers to universal addresses. This makes dynamic binding of remote programs possible.

Rpcbind is run at a well-known universal address, and other RPC programs register their dynamically allocated addresses with it. Since the other RPC services do not have a fixed address, clients must send messages to the rpcbind program on the machines they wish to reach. The rpcbind program will then forward the message to the appropriate program on the system.

Rpcbind must be running to make RPC calls. Since the IVR system does not require the use of any RPC programs, the rpcbind service may be disabled. However, it should **not** be disabled if any of the RPC services are needed for a company's IVR application or its operating environment.

Service	Port	Protocols	Purpose
sunrpc	111	tcp/udp	rpcbind service

4.1.6.2 NFS Services

The Network File System (NFS) services are used for mounting remote resources. These services build on the basic RPC mechanism.

The IVR system does not require NFS functionality. The following services may be disabled as a security hardening measure:

Service	Port	Protocols	Purpose
nfsd	2049	tcp/udp	Starts the daemons that handle client filesystem requests
biod	*dynamic*	tcp/udp	Starts the asynchronous block I/O daemons
mountd	*dynamic*	tcp/udp	Server that answers file system mount requests
lockd	*dynamic*	tcp/udp	Server that processes lock requests
statd	*dynamic*	tcp/udp	Network status monitor daemon
bootparamd	*dynamic*	tcp/udp	Server process that provides information necessary for booting to diskless clients
pcnfsd	*dynamic*	tcp/udp	NFS daemon for PC-NFS user authentication and remote printing
status	*dynamic*	tcp/udp	Status monitor – used for file locking
llockmgr	*dynamic*	tcp/udp	Local lock manager – used for file locking
nlockmgr	*dynamic*	tcp/udp	Network lock manager – used for file locking

4.1.6.3 Other RPC Services

The IVR system does not require any of the remaining RPC services. The following services may be disabled as a security hardening measure:

Service	Port	Protocols	Purpose
rwalld	*dynamic*	tcp/udp	Server that handles requests for sending broadcast messages to all users on the system
rusersd	*dynamic*	tcp/udp	Server that returns a list of users on the host
sprayd	*dynamic*	tcp/udp	Server that records the packets sent by the "spray" command. The "spray" command sends a one-way stream of packets to the system using RPC.
cmsd	*dynamic*	tcp/udp	Calendar manager service daemon
ttdbserverd	*dynamic*	tcp/udp	ToolTalk database server

4.1.7. sendmail

The sendmail service is an electronic mail transport agent.

The IVR system does not require the sendmail service. Companies may disable this service as a security hardening measure. However, some companies use the sendmail service as part of their normal operating procedures. Avaya does not recommend this practice since the sendmail service has been subject to many security vulnerabilities in the past. If a company must use sendmail, Avaya recommends that it only be used to send outgoing mail; it should not be used as an incoming mail server.

If sendmail is not needed, both the sendmail startup script and the smtp port used by sendmail should be disabled.

Service	Port	Protocols	Purpose
smtp	25	tcp	sendmail service

4.1.8. Other Miscellaneous Network Services

The IVR system does not require any of the following miscellaneous network services. They may all be disabled to further harden the security of the system.

Service	Port	Protocols	Purpose
systat	11	tcp/udp	Provides information about processes running on the system
netstat	15	tcp/udp	Provides network status information
finger	79	tcp	Provides information about users on the system
http	80	tcp	Hypertext Transfer Protocol server daemon
pop-3	110	tcp	Post Office Protocol version 3 server daemon
nb-ns	137	tcp/udp	Netbios name service
nb-dgm	138	tcp/dup	Netbios datagram service
nb-ssn	139	tcp	Netbios session service
imap-4	143	tcp	Internet Message Access Protocol version 4 server daemon
i2odialog	360	tcp	HTTP front-end daemon for controlling the i2o subsystem
login	513	tcp	Remote login (rlogin) service
shell	514	tcp	Runs a command from a remote system using the Unix shell
printer	515	tcp	Line printer spooler service
swat	901	tcp	Samba web administration tool
listen	2766	tcp	Network listener port monitor service
nts	5017	tcp	Anypath number translation service
dtspc	6112	tcp	TED subprocess control daemon

4.2. Restrict Root Access

The root login has the highest level of authority on the IVR system. It can be used to modify any of the capabilities, features, or administration on the system. Therefore, it is very important to control access to the root login.

Companies should only provide root login access information to a limited number of trusted individuals. Furthermore, Avaya recommends that the IVR system be administered so that direct root logins are restricted to the system console only. Restricting root access to the console requires users to have physical access to the system. Remote users must log in as another user, then use the su command to log in as root. This provides an extra measure of security, since remote users must authenticate themselves twice (once using their normal user login, then a second time for root access) to use the root access; in addition, all use of the su command is logged for accountability.

4.3. Hide the Telnet Banner

By default, operating system and version number information is displayed when a user attempts to access the system via telnet. This information is displayed before a user performs any login authentication procedures. Individuals who are attempting to access the IVR system fraudulently can use the OS and version number information to attack the system using known security vulnerabilities.

Avaya recommends that the telnet daemon be modified so that the operating system and version number information is not displayed before user authentication is complete.

4.4. Restrict Users Allowed to Use Inbound FTP

If inbound file transfers from remote systems are needed, the FTP daemon on the IVR system should be administered to restrict which users are allowed to use inbound FTP. This can be accomplished in three ways:

- FTP access can be denied for specific users (especially privileged users). Doing this prevents certain users and services from delivering files to the IVR system via FTP.
- FTP access can be allowed or denied for specified accounts from specific hosts. This is a particularly useful security hardening measure if inbound FTP is required, since it allows the system to be administered so that only users from known hosts can perform file transfers.
- Anonymous FTP access can be disabled.

4.5. Restrict Users Allowed to Use the cron Command

The cron command starts a process to execute commands at specified times and dates. The cron daemon should be administered to restrict which users are allowed to submit jobs. Otherwise, unauthorized users could be allowed to submit jobs.

4.6. Restrict Users Allowed to Use the at Command

The *at* command is similar to the cron command except that it only executes a command one time. As with cron, the *at* daemon should be administered to restrict which users are allowed to submit jobs. Otherwise, unauthorized users could be allowed to submit jobs.

4.7. Disable Anonymous/Guest Logins

Anonymous and guest logins allow users to perform system activities while disguising their identity.

The IVR system is not provisioned with any anonymous or guest logins enabled. Companies should make sure that these types of logins are not added to the system to avoid potential security risks.

4.8. Change the Default oracle Password

When Oracle is loaded on an Avaya IVR system, a Unix login is created with a username of *oracle*. This login is administered with a password that is known to be weak.

Companies should change the oracle login password to meet their password requirements. If the password is not changed, unauthorized users could potentially break into the system by guessing the oracle login password.

5. SSH

SSH (Secure Shell) is a program that includes capabilities for logging into another computer over a network, executing commands on a remote machine, and moving files from one machine to another. It provides strong authentication and secure communications over untrusted networks.

SSH provides a more secure means of accessing remote systems than protocols such as telnet and FTP. Unlike telnet and FTP, SSH allows users to connect to remote hosts over an encrypted link. This protects against interception of clear text logins and passwords.

SSH is not provided with IVR systems. However, companies can install and use SSH if it is required by their business procedures.

6. Account and Password Administration

Companies should implement good user account management practices to help secure access to the IVR system. Using good account management procedures can ensure that the risk of unauthorized access is minimized. They can also ensure that login activities can be tracked and audited.

6.1. Account Management

Companies should follow the same practices for IVR administrative accounts as they would for any other mission-critical or proprietary enterprise system. These practices must be implemented as part of the company's operational procedures and should include the following:

- Minimize the number of accounts (especially privileged accounts).
- Strictly limit privileged accounts, such as root, to those people who have a business need for access.
- Do not set up user accounts with a user ID of 0. User ID 0 designates the root login account.
- Use unique user IDs for each user account.
- Deactivate logins if they are not used for a specified number of days.
- Deactivate or remove logins if the user leaves the company.
- Review account information (e.g., permissions, ownership, and unexpected changes) on a regular basis.
- Review activities performed by privileged users on a regular basis.
- Review logs for the following activities on a regular basis: login failures, unexpected user logins or unexpected login times, and system processes that should not be running.

6.2. Password Administration

The IVR system requires all user login passwords to meet the following password requirements which are enforced by the UNIX *passwd* command default verifier setting:

- Each password must have at least 3 characters.
- Each password must contain at least two alphabetic characters and at least one non-alphabetic character.
- Each password must differ from the user's login name and any reverse or circular shift of that login name.
- A new password must differ from the old one by at least three characters.

Companies may use the operating system capabilities to implement additional password requirements. For example, the following security improvements are recommended:

- Modify the minimum password length to require passwords to be at least 8 characters long.
- Enable password aging. This will force users to change their password after a configurable number of days.
- Set up passwords for new users to force them to change the password at the first login.

6.3. Role-based Authorization Capabilities for System Administration

The IVR system provides role-based authorization capabilities for controlling access to its menu-driven administration utility (cvis_menu). Companies should use these capabilities to control which users are allowed to modify the IVR system and applications.

The role-based authentication capabilities are controlled on a per-login basis. The administration utility requires the use of a login that has been assigned either "administration" or "operations"

permissions. Administration users can perform any administration task. Operations users have access to configuration management, reports administration, and system monitor capabilities, but do not have control of the voice system.

Root access is required to assign permissions.

7. Log Files and Audit Trails

Log files are often useful for detecting suspicious system activity. Companies should implement a process to review log files on a regular basis.

7.1. Operating System Logging

The UnixWare operating system generates several logs that can be checked for evidence of possible security breaches. These logs include:

- /var/adm/sulog – the su log
- /var/cron/log – the cron log

Other system logs may be available if the system has been administered to generate them. These logs include:

- /var/adm/loginlog – the log for failed login attempts
- /var/adm/xferlog – the FTP transfer log
- *syslog* (system control log) – the logs for system messages, FTP command log, etc. The *syslog* log file locations are configurable.

7.2. IVR Logging

The IVR platform contains a general-purpose message logging mechanism. This mechanism allows different code modules to generate distinct log events. Each event has an associated ID number and may be sent to multiple destinations. In addition to the events generated by system software processes, log messages are generated for the following events by default:

- All commands executed using the administration utility (cvis_menu)
- All commands executed from the system command line

Because all command invocations are logged, companies can use the IVR logging to determine if any access to or modifications to security objects, restricted resources, or configuration setup have occurred. Similarly, this logging can be used to track addition or deletion of user IDs, password resets, and modifications of event logs. The IVR system provides the date, time, user ID, and type of event for each logged event.

All log events are sent to the default log file known as the master log. Log events related to alarming are also sent to the alarm log file. Each log event can also be assigned a priority. The priority determines if the log event is an alarm and also determines the severity of the alarm. An alerter process monitors the master log, implements thresholds, maintains active and retired alarms, and provides dial out alarm capability. The IVR system includes message administration tools that can be used to add or remove a destination to/from the current list of destinations for

the message, modify the priority of the message, and change the threshold period for the message.

Multiple generations of each log file are maintained to control growth. A configuration file controls the maximum size of each type of log file, as well as the maximum number of each type of log file to be generated. Once the maximum number is exceeded, the oldest log file of that type is deleted to keep the number of files within the limit specified.

As mentioned above, the IVR message administration tools can be used to indicate whether particular log events should be treated as alarms. The dial out alarming capability is provided by the Remote Maintenance Board (RMB) on the IVR system. It supports up to two dial out locations and can be used to automatically notify system administrators when alarm events occur. The RMB can also be used to manage alarms and events. In addition, the IVR platform includes tools for viewing the events in the master log file. The review of events is a procedural issue that can and should be defined according to a company's needs.

8. Modem Access and ASG

Dial-in lines on the IVR system can be protected by an Avaya-developed solution called Access Security Gateway (ASG). The ASG package is included with the IVR system. This feature provides secure authentication and auditing for all remote access into the maintenance ports.

ASG authentication is based on a challenge/response algorithm using a token-based authentication scheme. Secure auditing is also provided. Logs are available that include information such as successful logins and failed logins, errors and exceptions.

Even though IVR dial-in lines are protected by ASG, some companies are concerned about the potential security risks of having a modem connected to their IVR system at all times. If this is an issue, it is possible to secure the modem by turning it off and only turning it on when service is required. However, this approach has two disadvantages: it disables the IVR dial-out alarming capability, and it makes it more difficult for Avaya technicians to respond to trouble escalations and service requests.

9. Disaster Recovery

As with any other application running on a server, it is important to be prepared to do a partial or complete IVR system restoration in the event of a disaster.

IVR systems should be backed up regularly. Companies should maintain two complete system backups. The backups should be identified by type, content, and date. Backups should be stored *away* from the IVR system; if possible, they should be stored at an off-site location.

Companies should also document the components and settings for their IVR system to facilitate the efforts required to restore their system. These system records should include:

- IVR system information, including the Customer Identification Number (CIN), Installation Location (IL), IP address of the Network Interface Card (NIC), dial-up number of the modem, telephone numbers for test calls, and sample account numbers for testing.
- Server names and IP addresses of any IVR system servers, including speech servers, database servers, and/or application servers.
- A current list of all software, including versions, installed on the system. The software itself should be stored in a safe and easily accessible location.
- Disk partitioning information, so that applications can be restored to the correct location.
- Information about what needs to be done to restore each application package. All values and parameters that must be entered should be recorded.
- Changes to system defaults.
- A printed copy of the information from the **Display Equipment** screen.
- Copies of host configuration files that contain the information required on the IVR system to be able to connect to a specific Host Mainframe System.
- Contact information for Avaya as well as for any application vendors, speech vendors, and/or database vendors that may have provided components used on or with the IVR system.

The Avaya Business Continuity Service can help design and implement disaster recovery plans to support rapid recovery from outages caused by unforeseen circumstances such as natural disasters or other emergency situations. It can help reduce expenses by proactively identifying potentially costly issues related to topology, hardware, software, security, network performance and business resiliency.

For more information or to contact the Avaya Business Continuity Service, refer to http://www1.avaya.com/services/portfolio/buscontinuity/index.html.

10. Application Development Guidelines

This section provides guidelines that self-service application developers can use when considering security in their application design. The information in this section is not necessarily an exhaustive list of application security considerations but is intended as a starting point.

There are basically two aspects to consider regarding self-service application security:

- Preventing unauthorized calls
- Securing the information exchange between the self-service application and the caller

The IVR platform can be used to build and execute voice response applications that involve network connections. Poor application design could allow unauthorized calls to be placed through the IVR system. Also, self-service applications can be used to transmit customer data between the call and the IVR system. Self-service application developers should ensure that any sensitive customer data is encrypted and protected from unauthorized access and/or modification. Also, the self-service application should be protected from unauthorized modification.

The security of the self-service application is the responsibility of the company that purchases and implements the IVR. However, the Avaya Enterprise Security Practice can provide application, PBX, and network assessment, auditing, and hardening services to help protect against unanticipated threats and security hazards.

For more information or to contact the Avaya Enterprise Security Practice, call them at 1-866-832-0925 or refer to http://www1.avaya.com/services/portfolio/security/index.html.

10.1. Preventing Unauthorized Use

The following two methods may be used to prevent unauthorized use of the IVR system:

- Block outbound access to the network at the switch (PBX or central office) that provides service to the IVR system. Blocking outbound access includes blocking call origination, bridging, and transfer capabilities. This method does not rely on a secure IVR or robust self-service application design, and can be done by blocking all outgoing calls or transfer access using one-way trunks for T1 or PRI, or by limiting the codes that can be dialed.
- Monitor the current IVR environment to determine if the application is at risk. This method should be used when blocking outbound access is inappropriate (for example, if the application requires outbound features, or if access to IVR administration is not well-controlled or only provides partial protection).

Another way to prevent unauthorized use of the IVR system is to design applications with toll fraud in mind. Toll fraud is possible when the application allows the incoming caller to make a network connection with another person. To avoid toll fraud, protect bridging to an outbound call, call transfer, and 3-way-conferencing in the following ways:

- Require callers to use passwords.
- Use appropriate switch translation restrictions.
- Make sure the application verifies that long distance numbers are not being requested, or that only permitted numbers are requested. The Transfer Call and Call Bridge capabilities of Script Builder, the 'tic' instruction at the transaction state machine (TSM) script level, and the VoiceXML transfer tag provide network access. If the ASAI package is loaded, additional TSM instructions and libraries provide access using the ASAI facility. In addition, a poorly designed prompt and collection action for transfer could let the caller enter any number for an outside access number.
- Build phone numbers into the application or have the application control them to minimize the possibility of toll fraud. If numbers are contained in a database where anyone with database access can change them, or if the caller enters them, fraud is possible.
- Only load the IVR Feature Test package (feature_tst) and assign it to channels when testing is required. The feature_tst package contains application programs that can be assigned to channels to test system components that allow any 4-digit number to be dialed, such as transfer and call bridging.

- Make sure that only trusted individuals can access application code. Anyone with access to application code can hide logic in it that provides network access and is triggered under specific circumstances.
- Collect numbers in a local database using Automatic Number Identification (ANI) capabilities through PRI and ASAI (or normal call data tools). If a significant number of repeat inbound calls are identified, an administrator can be notified using the Netview package or ARU, or an application can be spawned to alert the administrator about the calls.

10.2. Protecting Customer Data and Securing the Application

The following suggestions should be followed to further protect the application and its data:

- Restrict login access to trusted individuals with a need to maintain or administer the system.
- Restrict remote login access.
- Use the administrative interface and its security classes for logins. Certain capabilities are restricted for particular classes. For example, the Operations class cannot modify applications.
- Make sure that modems are administered properly to prevent access by outside users. Make sure that the phone line is disconnected from the modem when the modem is not in use.
- Use standard tools to monitor login statistics.
- Ensure that customer passwords, account numbers, etc. are not stored in plain text, not displayed in log files, etc.
- Ensure that access to customer data via the IVR application requires authentication from the customer.
- Make sure that sensitive customer data is encrypted as necessary using either the tools provided with the UnixWare operating system or another solution.

11. Operating System Patches

Security vulnerabilities in operating system software are commonly fixed with operating system patches.

Santa Cruz Operation (SCO), Inc., provides the UnixWare operating system. Avaya monitors the SCO web site for UnixWare 7.1.1 patches on a regular basis and posts certified patches on the support.avaya.com web site on a quarterly basis. Patches are posted in two ways:

- The patch is posted with installation instructions and can be downloadable from the support site.
- A statement is posted indicating that the patch has been certified and the Services organization needs to be contacted to obtain the patch.

If a company is aware of a UnixWare patch prior to seeing it posted on the support site, the company can open a ticket with Avaya and request that the patch be certified by Avaya. For these types of requests, the time frame for patch certification will vary.

12. System Access by Avaya Technicians

Companies may need to provide IVR system access to Avaya technicians under the following conditions:

- In response to a escalation
- In response to a service request. The service request could be for regular maintenance or a software upgrade.
- When an alarm is reported by the IVR system

All IVR activities, whether they are generated by a service call or an alarm report, are tracked by the Avaya support organizations. Items that are tracked are:

- The technician who accessed the customer's machine
- When the access was made
- What was done during the access based on the ownership of the support case and the case notes entered by the support associate

Additionally, log files are maintained on the system that capture all commands entered, whether they are entered locally through the system console or remotely.

IVR systems are pre-administered to include the “tsc” and “craft” logins. These logins are reserved for use by Avaya support personnel. The tsc login is an alias for root. It is primarily used by the Avaya Technical Support Center personnel. The craft login is a user login that has “operations” permissions. It is mainly used by the field support organization.

These accounts should not be changed, disabled, or have their passwords aged. Doing so will limit Avaya’s ability to support the platform.

13. Conclusion

No telecommunications system can be entirely free from the risk of unauthorized use. However, diligent attention to system management and to security can reduce that risk considerably. Often, a trade-off is required between reduced risk and ease of use and flexibility. Companies who use and administer their IVR systems make this trade-off decision. They know how to best tailor the system to meet their unique needs and, necessarily, are in the best position to protect the system from unauthorized use. Because the company has ultimate control over the configuration and use of Avaya services and products it purchases, the company properly bears responsibility for fraudulent uses of those services and products.