



Avaya™ Interactive Response Security

Abstract

This paper has been updated to provide information about the security strategy for Avaya Interactive Response (IR) R2.0. It also provides suggestions that companies can use to improve the security of their Avaya IR systems and applications.

Copyright © 2005, Avaya Inc. All rights reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc.

Solaris is a trademark of Sun Microsystems, Inc.

All other trademarks are the property of their respective owners.

The information provided in this document is subject to change without notice. The configurations, technical data, and recommendations provided in this document are believed to be accurate and dependable at the time of publication, but are presented without express or implied warranty. Users are responsible for their application of any products specified in this document.

For the latest version of this document, visit the Avaya customer support website at support.avaya.com.

Issue	Description	Date
1.0	Initial version for Release 1.2.1 and later	April 30, 2004
1.1	Updated version for Release 2.0	March, 2006

Contents

1. Introduction	5
2. IR Security Strategy	5
3. Securing Access to the System	6
3.1. Physical system security	6
3.2. Isolated LANs	7
3.3. Firewalls.....	7
4. Platform Security Hardening	7
4.1. Disable Unneeded Network Services and Ports.....	8
4.1.1. telnet.....	8
4.1.2. FTP.....	9
4.1.3. SFTP	9
4.1.4. exec	10
4.1.5. SNMP.....	10
4.1.6. RPC Services	11
4.1.7. sendmail	13
4.1.8. Solaris Common Desktop Environment (CDE).....	13
4.1.9. inetd Internal Services.....	14
4.1.10. Other inetd Network Services	14
4.1.11. Network Service Startup Scripts.....	15
4.1.12. Other Well-Known Ports	15
4.1.13. Ports Used by Avaya IR Processes	16
4.2. Restrict Root Access	23
4.3. Hide the Telnet Banner	23
4.4. Hide the FTP Banner	24
4.5. Restrict Users Allowed to Use Inbound FTP.....	24
4.6. Modify the Default SNMP Community Strings	24
4.7. Restrict Users Allowed to Use the cron Command	24
4.8. Restrict Users Allowed to Use the at Command	25
4.9. Disable Anonymous/Guest Logins	25
4.10. Use Stronger TCP Sequence Numbers	25
4.11. Make the System Stack Non-executable.....	25
5. SSH	25
6. SSL	26
7. Account and Password Administration	26
7.1. Account Management	26
7.2. Password Administration.....	27
7.3. Role-based Authorization Capabilities for System Administration.....	27
7.4. Logins Provided with IR Systems.....	28
8. Log Files and Audit Trails	28
8.1. Operating System Logging	28
8.2. IR Logging.....	29
9. Modem Access and ASG	30
10. Disaster Recovery	30

11. Application Development Guidelines	31
11.1. Preventing Unauthorized Use	32
11.2. Protecting Customer Data and Securing the Application	33
12. Operating System Patches	33
13. System Access by Avaya Technicians	33
14. Known Security Issues in Avaya IR	34
14.1. JDBC.....	34
14.2. IVR Designer Service Creation Tool.....	35
14.3. Web Administration Utility	35
14.4. VoiceXML Feature	35
15. Conclusion	36
Appendix A.	
Services Disabled by the <i>disableServices</i> Command	37

1. Introduction

Avaya™ Interactive Response (IR) is a self-service software platform for voice and speech applications. Avaya IR empowers enterprises to automate common customer interaction and fulfillment tasks using touchtone, fax, or natural language speech.

This paper provides information on the security strategy for Avaya IR Release 2.0. It also provides suggestions that companies can use to improve the security of their IR systems and applications.

In this paper, the term “companies” will be used to refer to the organizations that purchase the IR systems and/or implement the IR applications. “Customer” will be used to refer to an end-user of the IR 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 IR system and its applications. Avaya disclaims any responsibility for or liability associated with the information herein.

Note also that this document is current as of the time of its issue. To obtain the latest version of this document, visit the customer support website at support.avaya.com.

2. IR Security Strategy

Avaya IR 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.

IR security protection falls mainly into two areas. The first area deals with the security of the operating system and the associated platform software. The IR system supports standard Sun Solaris security interfaces (for example, 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 IR system also provides role-based authorization capabilities for controlling access to its web-based administration utilities.

Secondly, all dial-in lines are protected by an Avaya-developed solution called Access Security Gateway (ASG). For more information on ASG, see section 9.

Companies, their application developers, and independent software vendors use IR 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. IR applications and scripts must also be written and audited to ensure that customer data is not inadvertently exposed in the application and that holes that might allow attackers access back to the PBX to perform unauthorized calling do not exist in the application. For more application development guidelines, see section 11.

Companies may use the capabilities of the operating system or other custom-developed solutions to implement the required application-level security. Avaya realizes that many companies employ the use of third-party software to enhance the security of their systems. Avaya appreciates the benefits of installing software that conforms to a company's security policy. However, any additional software that is installed on the system must be installed under a policy of permissive use. Avaya cannot ensure that such software will not affect the operation or performance capabilities of the IR system.

If a company chooses to install additional software, they must accept the responsibility of ensuring that it does not degrade system performance to an unacceptable level. Companies may choose to trade some system performance for the use of third party applications, but Avaya does not warrant that additional software can be added and full system capacity be maintained. Furthermore, Avaya will not verify or ascertain the validity of any other vendor's software or its impact on the IR system unless prior business arrangements have been made through Avaya product management. If a company installs additional software that causes problems on the system, Avaya may charge for any assistance required in troubleshooting the problem or may require that the software be removed before Avaya begins the troubleshooting process.

The Avaya Enterprise Security Practice, part of Avaya Network Consulting Services, 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 1-866-832-0925 or see <http://www1.avaya.com/services/portfolio/security/index.html>.

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 IR 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 the operation of the IR system could be disrupted, whether unintentionally or maliciously. The IR 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. IR systems can be protected by configuring them on a LAN that has no physical connection to the Internet or to any internal networks that are not secure. 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 IR system needs to interface, such as speech servers, database servers, a MultiVantage switch (for VoIP connectivity), 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 the IR system. A company should consider the requirements of their operating environment before deciding whether to place the IR 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 IR servers, from unauthorized access. Firewalls sit between the Internet and a network device or LAN and control network traffic to/from particular devices, including access of designated ports using particular protocols or applications.

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

Even if the internal LAN is protected by a firewall, the IR system may still be accessible to anyone who has access to the internal network. Therefore, it is still important to restrict access to the IR system in this environment to lessen the risk of fraudulent use by an insider. See section 7.

4. Platform Security Hardening

Avaya IR is based on the Solaris operating system. Solaris offers C2-level security capabilities as defined by the Department of Defense Trusted Computer System Evaluation Criteria. 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 Solaris operating system or by a qualified technical consultant. The Avaya Enterprise Security Practice 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 IR system, they can also provide a wide range of 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 1-866-832-0925 or see <http://www1.avaya.com/services/portfolio/security/index.html>.

4.1. Disable Unneeded Network Services and Ports

Many network services are subject to security vulnerabilities that may allow unauthorized individuals to access the system. The IR system requires the use of relatively few network services. Therefore, Avaya recommends that companies disable any network services not required for the IR system and not needed for the companies' business purposes. Doing this can mitigate known (and future) security vulnerabilities.

Starting with IR Release 1.2, many unneeded services and ports are disabled by default as part of the IR software installation process. These services are disabled for all IR 1.2 systems — both total solution systems (in which Avaya provides both the hardware and software) and software-only solutions (where the company is responsible for providing its own IR hardware).

In IR Release 1.2.1, even more of the unneeded services are disabled. These services are disabled using the `/vs/bin/utl/disableServices` command. This command turns off those services that are not needed for IR and stores a list of the services that were disabled in the `/voice1/disabledServices.log` file. However, these services are only disabled by default on total solution systems. The services are *not* disabled by default on software-only solutions. Companies who purchase the software-only solution and who wish to disable these services may do so by executing the `/vs/bin/utl/disableServices` command manually. For a list of the services disabled by this command, see Appendix A.

The following sections provide information on services and ports that may be needed by the IR 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 IR platform without affecting basic IR functionality. However, companies may require the use of the services discussed in these sections based on the platform features that are used, how the IR 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 IR 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 5.2 (formerly known as Voice@Work™), the PC-based service creation tool for IVR applications, used only FTP to transfer applications to the IR system. Therefore, the FTP service had to remain enabled if companies planned to develop and install applications using IVR Designer. However, in Avaya IVR Designer 5.3, the option of choosing between FTP and SFTP (Secure File Transfer Protocol) has been provided.

Companies may disable FTP once the IVR Designer application development is complete and the final application has been installed on the IR system. If necessary, they can temporarily re-enable FTP 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 IR system. In these situations, it is preferable for the IR system to initiate the file transfers. Doing this allows the IR 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 IR 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 sections 4.4 and 4.5.

Service	Port	Protocols	Purpose
ftp	21	tcp	File Transfer Protocol service

4.1.3. SFTP

The Secure File Transfer Protocol (SFTP) service is similar to FTP, but performs all operations over an encrypted Secure Shell (SSH) transport link, thus gaining the features of public key encryption and compression.

Avaya IVR Designer 5.3 offers the option of using either FTP or SFTP. A common misconception about SFTP is that SFTP is simply FTP run over SSH. However, SFTP is the service, which works above the SSH protocol. SFTP expects the underlying SSH protocol to secure authentication and security. Therefore, SFTP is most often associated with SSH.

SFTP, in the context of Avaya IVR Designer 5.3 implements the client part of the SSH protocol. On IR systems using Solaris 10 as the operating system, SSH is provided by default. On IR systems using Solaris 8 as the operating system, SSH can be installed using the openSSH package (<http://www.sunfreeware.com>).

Compared to the earlier Secure Copy protocol (SCP), the SFTP protocol allows for many more operations on remote files, and functions like a remote file system protocol. It attempts to be more platform-independent. With SCP, the expansion of wildcards specified by the client was up to the server, whereas the design of SFTP avoids this problem. SFTP also provides a more secure connection, as against using FTP or telnet because passwords are never transferred in clear text, preventing the possibility of capture of sensitive data, while eavesdropping on the connection. Data is also encrypted during the transfer, making it difficult to spy or modify the connection.

Service	Port	Protocol	Purpose
sftp	22	ssh	Secure File Transfer Protocol service

4.1.4. 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 IR system or assigning the applications to channels on the IR 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 IR system. If necessary, they can temporarily re-enable the exec service to update the application later.

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

4.1.5. SNMP

The Simple Network Management Protocol (SNMP) provides a mechanism for managing complex networks.

The Avaya IR SNMP Agent® enables network management stations to proactively monitor, administer, and receive alerts from IR systems. It operates with the native master SNMP agent, the Sun Solstice Enterprise Master Agent. Therefore, the SNMP services must remain enabled if the Avaya IR SNMP Agent is used.

If SNMP is used, companies should implement the additional hardening practices described in section 4.6.

Service	Port	Protocols	Purpose
snmpdx	161	udp	SNMP daemon requests
	162	udp	SNMP trap events
snmpdx	dynamic (internal to IR)	udp	SNMP trap notifications
snmpXdmid	dynamic (internal to IR)	tcp/udp	SNMP-DMI mapper subagent
dmispd	dynamic (internal to IR)	tcp/udp	DMI Service Provider

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.

Avaya IR uses Network File System (NFS) services for performing backup and restore activities. These services build on the basic RPC mechanism.

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 Avaya IR requires the use of RPC programs, the rpcbind service should **not** be disabled.

Service	Port	Protocols	Purpose
sunrpc	111	tcp/udp	rpcbind service

4.1.6.2 NFS Services

IR systems use Network File System (NFS) services for mounting remote resources. Backup files are stored on a remote system. The remote system must have NFS service available, and the backup directory must be an NFS mount point.

The NFS client services must be enabled on the IR system so that the IR server can mount its remote backup directory. These client services are as follows:

Service	Port	Protocols	Purpose
lockd	4045	tcp/udp	Server that processes lock requests
statd	dynamic	tcp/udp	Network status monitor daemon

IR does **not** require the use of NFS server services. The NFS server services can be disabled.

Service	Port	Protocols	Purpose
nfsd	2049	tcp/udp	Starts the daemons that handle client filesystem requests
mountd	dynamic	tcp/udp	Server that answers file system mount requests

Tape backup has been introduced in IR R2.0. Tape backup does not require NFS mounted services.

4.1.6.3 Other RPC Services

The IR system does **not** require any of the remaining RPC services, so they can be disabled.

Service	Port	Protocols	Purpose
sadmind	dynamic	udp	Distributed system administration daemon
rquotad	dynamic	datagram_v	Daemon that manages quotas for local file systems mounted on remote systems
rusersd	dynamic	datagram_v/ circuit_v	Server that returns a list of users on the host
sprayd	dynamic	datagram_v	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.
walld	dynamic	datagram_v	Server that handles requests for sending broadcast messages to all users on the system
rstatd	dynamic	datagram_v	Kernel statistics server
rexed	dynamic	tcp	Remote execution daemon
ttdbserverd	dynamic	tcp	Sun ToolTalk database server

Service	Port	Protocols	Purpose
ufsd	<i>dynamic</i>	*	UFS-aware service daemon
kcms_server	<i>dynamic</i>	tcp	Kodak Color Management System server
cachefs	<i>dynamic</i>	ticotsord	Cache filesystem daemon
kttkt_warnd	<i>dynamic</i>	ticotsord	Kerberos warning daemon
gssd	<i>dynamic</i>	ticotsord	Generic Security Service daemon
amiserv	<i>dynamic</i>	ticotsord	AMI (smart card) daemon
ocfserv	<i>dynamic</i>	ticotsord	OCF (smart card) daemon
cmsd	<i>dynamic</i>	udp	Calendar manager service daemon
sunvts	<i>dynamic</i>	udp	Sun Validation Test Suite

4.1.7. sendmail

The sendmail service is an electronic mail transport agent.

The IR 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 because 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 as well as the *smtp* and *submission* ports used by sendmail should be disabled.

Service	Port	Protocols	Purpose
smtp	25	tcp	sendmail service
submission	587	tcp/udp	Mail message submission

4.1.8. Solaris Common Desktop Environment (CDE)

The Solaris CDE provides a graphical user interface (GUI) for Solaris systems.

The IR system does not require the use of the CDE. It is not disabled during the IR installation process in case companies wish to use it in their operating environments. However, since it is not required for IR, companies may disable it as a security hardening measure.

If the CDE is not needed, both the CDE login service (dtlogin) startup script and the CDE Subprocess Control Service should be disabled.

If the CDE is needed, Avaya recommends that the XDMCP service should be disabled. The XDMCP service is only needed if a system is being used to manage other X servers. Since the IR system has no reason to manage other display connections, and since XDMCP has some known security vulnerabilities, it should not be enabled on IR systems.

Service	Port	Protocols	Purpose
dtlogin	<i>dynamic</i>	tcp	CDE login service
dtspc	6112	tcp	CDE subprocess control

4.1.9. inetd Internal Services

The inetd internal services are primarily intended as debugging and measurement tools. The IR 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.

4.1.10. Other inetd Network Services

The IR system does not require any of the following inetd network services. They can all be disabled to further harden the security of the system.

Service	Port	Protocols	Purpose
systat	11	tcp	Provides information about processes running on the system
netstat	15	tcp	Provides network status information
name	42	udp	Name server protocol (obsolete)
tftp	69	udp	Trivial File Transfer Protocol service
finger	79	tcp	Provides information about users on the system
comsat	512	udp	Server process which listens for reports of incoming mail
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
talk	517	udp	Two-way, screen-oriented communications program
uucp	540	tcp	UNIX-to-UNIX system copy service
fs	7100	tcp	Sun Font Server

4.1.11. Network Service Startup Scripts

Network service startup scripts are used to automatically start system services when the system run level changes. Several of the services are not needed by the IR system, so their corresponding startup scripts can be disabled. The unneeded startup scripts are as follows:

Script Name	Location	Purpose
S70uucp	/etc/rc2.d	UNIX-to-UNIX system copy utilities
S71ldap.client	/etc/rc2.d	Lightweight Directory Access Protocol client configuration management
S72slpd	/etc/rc2.d	Service Location Protocol common server functionality
S73cachefs.daemon	/etc/rc2.d	Cache file system services
S74autofs	/etc/rc2.d	File system Automounter services
S74xntpd	/etc/rc2.d	Network Time Protocol clock synchronization services
S80lp	/etc/rc2.d	Line printer scheduler
S80spc	/etc/rc2.d	Printer services
S88sendmail	/etc/rc2.d	Sendmail service
S93cacheos.finish	/etc/rc2.d	Cache file system configuration
S94ncalogd	/etc/rc2.d	Solaris Network Cache and Accelerator services
S95ncad	/etc/rc2.d	Solaris Network Cache and Accelerator services
S15nfs.server	/etc/rc3.d	Network File System server services
S34dhcp	/etc/rc3.d	Dynamic Host Configuration Protocol services

4.1.12. Other Well-Known Ports

The IR system does not require any of the following well-known ports on the system.

Service	Port	Protocols
tcpmux	1	tcp
whois	43	tcp
domain	53	tcp/udp
bootps	67	udp
bootpc	68	udp
hostnames	101	tcp
pop2	109	tcp
pop3	110	tcp
imap	143	tcp
ldap	389	tcp/udp
ldaps	636	tcp/udp
rje	77	tcp
link	87	tcp
supdup	95	tcp
iso-tsap	102	tcp

Service	Port	Protocols
x400	103	tcp
x400-snd	104	tcp
csnet-ns	105	tcp
uucp-path	117	tcp
pop-2	109	tcp
nntp	119	tcp
ntp	123	tcp/udp
netbios-ns	137	tcp/udp
netbios-dgm	138	tcp/udp
netbios-ssn	139	tcp/udp
news	144	tcp
slp	427	tcp/udp
mobile-ip	434	udp
cvc_hostd	442	tcp
courier	530	tcp
who	513	udp
syslog	514	udp
route	520	udp
ripng	521	udp
klogin	543	tcp
kshell	544	tcp
new-rwho	550	udp
rmonitor	560	udp
monitor	561	udp
pcserver	600	tcp
sun-dr	665	tcp
kerberos-adm	749	tcp/udp
kerberos	750	tcp/udp
krb5_prop	754	tcp
cvc	1495	tcp
ingreslock	1524	tcp
www-ldap-gw	1760	tcp/udp
listen	2766	tcp
eklogin	2105	tcp

4.1.13. Ports Used by Avaya IR Processes

The IR system enables several ports for use by its features and processes. These ports are activated during the IR process initialization. They **must** remain enabled if the associated features are used or IR functionality will be affected.

4.1.13.1 WholeWord Speech Recognition

Whole-speech recognition on IR systems can be performed using an Automatic Speech Recognition (ASR) server. In this configuration, a multi-channel front-end recognition engine is used to handle communications between the IR and the speech server process. (Note, however, that the IR system always acts as the hosting speech server.)

The WholeWord recognition engine enables one port for each channel that uses ASR services. These ports listen for recognition jobs associated with each channel. The WholeWord recognition engine supports 60 channels by default.

The initial default port number that the WholeWord recognition engine uses is 2345. This number can be changed if necessary. The other port numbers increase sequentially from the initial number.

Process	Default Ports	Protocols	Purpose
aasrProxy	2345 to 2404	tcp	WholeWord speech recognition connections to speech server process

4.1.13.2 Dial Pulse Recognition (DPR) (*IR Release 1.2.1 and later*)

Dial Pulse Recognition on IR systems can be performed using a DPR server. In this configuration, a multi-channel proxy front-end DPR engine is used to handle communications between the IR and the DPR server process. (Note, however, that the IR system always acts as the hosting DPR server.)

The DPR proxy engine enables 10 ports by default. These ports listen for recognition jobs associated with each channel. The number of ports can be changed if necessary.

The initial default port number that the DPR proxy uses is 7500. This number can be changed if necessary. The other port numbers increase sequentially from the initial number.

The DPR feature is only available in IR Release 1.2.1 and later.

Process	Default Ports	Protocols	Purpose
dprProxy	7500 to 7500+ (n-1)	tcp	DPR Proxy connections to DPR Server, where “n” is the number of ports

4.1.13.3 Natural Language Speech Recognition (NLSR)

Natural Language Speech Recognition is performed using speech servers separate from the IR system. The IR system uses a speech proxy process to handle communications between the IR and the NLSR speech servers.

Unlike the ASR proxy, the speech proxy process does not enable a port for each NLSR channel. However, the speech recognition client libraries provided by the Open Speech Recognition vendors and used by the speech proxy process on the IR may open ports for communicating with the NLSR server. Whether or not a port is enabled depends on which vendor's speech recognition software is used.

Process	Ports	Protocols	Purpose
srproxy	dynamic	tcp	Connections from Speech Proxy client libraries to NLSR speech server

4.1.13.4 Telecommunications Device for the Deaf (TDD) Recognition

TDD recognition on IR systems can be performed using a TDD server. In this configuration, a multi-channel proxy front-end TDD engine is used to handle communications between the IR and the TDD server process. (Note, however, that the IR system always acts as the hosting TDD server.)

The TDD proxy engine enables 10 ports by default. These ports listen for recognition jobs associated with each channel. The number of ports can be changed if necessary.

The initial default port number that the TDD proxy uses is 5111. This number can be changed if necessary. The other port numbers increase sequentially from the initial number.

Process	Default Ports	Protocols	Purpose
tdd	5111 to 5111 + (n-1)	tcp	TDD Proxy connections to TDD Server, where "n" is the number of ports

4.1.13.5 Digital Call Processing

Digital call processing features on IR systems use Natural Microsystems (NMS) digital cards and associated software. The main NMS software process, *ctdaemon*, enables one port for communications with its software libraries.

Note that this port is only used for communications within the IR system. It is not used for communications to an external component.

Process	Port	Protocols	Purpose
---------	------	-----------	---------

ctdaemon	2244	tcp	NMS digital call processing
----------	------	-----	-----------------------------

4.1.13.6 Voice over IP (VoIP) Call Processing

The VoIP feature enables the Avaya IR system to serve as an IVR adjunct that connects to a MultiVantage switch over a packet-based network.

The VoIP feature enables one port for each channel that uses VoIP call processing. These ports are used for communications between the IR and the MultiVantage switch. They listen for call processing messages associated with each channel.

The VoIP ports are dynamically allocated during VoIP feature initialization. The actual port numbers may vary on different machines.

Process	Ports	Protocols	Purpose		
VoIPCard	<i>dynamic</i>	tcp	VoIP call processing – one port per VoIP channel		

Source	Ports	Destination	Ports	Protocols	Purpose
IR	1024+	CLAN (CM)	1719	udp	H.323 RAS
IR	1024+	CLAN (CM)	1720	tcp	H.323 Signalling
IR	2048-65534	MedPro (CM)	2048-65534	udp rtp	VoIP bearer traffic
MedPro (CM)	2048-65534	IR	2048-65534	udp rtp	VoIP bearer traffic

The RTP port ranges are configurable via CM administration.

4.1.13.7 Web and Java-based Features

Several IR features require the use of Java features for their implementation and functionality. For example, the Web Administration utility provides a web browser interface for administering the IR system. The web interface requires the use of a web server. The administration utility also uses a Java Virtual Machine for executing its code as well as Java servlets for some specialized tasks. The JDBC, CDH, and CTI features also use the Java interpreter and Java servlets. These features are described in more detail in later sections.

4.1.13.7.1 Web and Java-based Features on IR 1.2 and earlier

Release 1.2 and earlier of IR use the Apache HTTP web server. The *httpd* server process listens on one port for incoming HTTP requests. These releases of IR also use the Apache Tomcat Java servlet engine. Tomcat uses two ports: one for its HTTP connection handler, and one for control messages.

The IR system uses the following port numbers for the Apache web server and for the Tomcat servlet engine. However, these port numbers can be changed if necessary.

Process	Default Ports	Protocols	Purpose
httpd	80	tcp	Apache HTTP web server
java	8007	tcp	Tomcat control messages
java	8081	tcp	Tomcat HTTP connection handler

4.1.13.7.2 Web and Java-based features on IR 1.2.1 and later

Starting with Release 1.2.1, IR no longer uses the Apache HTTP web server. Instead, it uses Tomcat as both the web server and the servlet engine. IR Release 1.2.1 also provides Secure Sockets Layer (SSL) support for both the Web Administration utility and the VoiceXML feature (see section 6).

In IR 1.2.1 and later, Tomcat uses three ports: one for its HTTP connection handler, one for its HTTPS connection handler, and one for control messages.

Process	Default Ports	Protocols	Purpose
java	80	tcp	Tomcat HTTP connection handler (web server)
java	8005	tcp	Tomcat control messages; used only within the IR server itself, so no external exposure is needed
java	8443	tcp	Tomcat HTTPS connection handler (web server) for SSL requests

The Tomcat web container produces standard error pages for conditions such as “HTTP Error 404 – Not Found”. To change the default pages, add appropriate <error-page> and <error-code> tags to the file /webadmin/jakarta*/webapps/ROOT/WEB-INF/web.xml. See <http://www.connecties.com/cymulacrum/tomcat4/c507.html> for more examples.

4.1.13.8 Java Database Connectivity (JDBC)

The JDBC feature provides database connectivity and activity on the Avaya IR server and to remote database servers. The JDBC feature supports connections to up to five different databases. Each database is accessed using a Data Interface Process (DIP) that has been configured with the appropriate administration information for that database.

Each of the five database DIPs (DBDIPs) enable two ports. One port is used for communications between the *jdbcdip* process, which provides JDBC functionality for TAS applications, and the main JDBC server process. The other port is used for communications between the JDBC servlet interface, which provides JDBC functionality for VXML applications, and the main JDBC server process. These ports are only enabled if the DBDIP has been configured and is running. The default port numbers can be changed if needed.

Note that since the JDBC feature uses a servlet interface, it also requires the use of the servlet ports described in section 4.1.13.7.

Process	Default Ports	Protocols	Purpose
jdbcdip	6500	tcp	JDBC support for TAS applications using DBDIP1
jdbcdip	6505	tcp	JDBC support for TAS applications using DBDIP2
jdbcdip	6510	tcp	JDBC support for TAS applications using DBDIP3
jdbcdip	6515	tcp	JDBC support for TAS applications using DBDIP4
jdbcdip	6520	tcp	JDBC support for TAS applications using DBDIP5
java	7001	tcp	JDBC support for VXML applications using DBDIP1
java	7002	tcp	JDBC support for VXML applications using DBDIP2
java	7003	tcp	JDBC support for VXML applications using DBDIP3
java	7004	tcp	JDBC support for VXML applications using DBDIP4
java	7005	tcp	JDBC support for VXML applications using DBDIP5

4.1.13.9 Call Data Handling (CDH)

The CDH feature accumulates generic call statistics and application events for call data reports. The CDH feature is based on the JDBC feature.

Call data can be stored in flat files on the IR system. Alternatively, the CDH feature can be administered to store the data in a database. The CDH feature supports a connection to a single database. The database is accessed using a CDH DIP that has been configured with the appropriate administration information for that database.

The CDH DIP enables one port that is used for communications between the *cdhdip* process and the main JDBC server process. This port is only enabled if the CDH feature has been administered to use database CDH, the CDH DIP has been configured, and the CDH DIP is running. The default port number can be changed if needed. If the CDH feature has been administered to store the call data in flat files, no ports are used.

Note that since the JDBC feature uses a servlet interface, it also requires the use of the servlet ports described in section 4.1.13.7.

Process	Default Port	Protocols	Purpose
cdhdip	6525	tcp	Internal communications for Call Data Handling feature

4.1.13.10 Computer-Telephony Integration (CTI)

The CTI DIP feature allows applications to communicate with an Avaya Computer Telephony (CT) server that controls ports on a MultiVantage switch.

The CTI DIP enables one port that is used for communications between the *ctidip* process and a Java Telephony API (JTAPI) client process on the IR system. The JTAPI client process communicates with the Avaya CT server over a LAN.

Note that since the CTI feature uses a servlet interface, it also requires the use of the servlet ports described in section 4.1.13.7.

Process	Ports	Protocols	Purpose
ctidip	6800	tcp	Internal communications for CTI DIP feature

4.1.13.11 Interaction Center (IC) Integration

The IC Integration feature supports the integration of the IR system with computer telephony services provided by Avaya Interaction Center.

The *vesp_dip* process on the IR system provides the means to access Avaya Computer Telephony services such as data retrieval and telephone call transfers. It enables the IR system to interact transparently with Avaya Computer Telephony for IC across the network.

The *vesp_dip* process enables one port for communications between the IR and IC systems.

Process	Ports	Protocols	Purpose
vesp_dip	3000	tcp	IR to IC communications

4.1.13.12 Predictive Dialing System (PDS) Integration

The PDS Integration feature integrates the functionality of the IR system and the Avaya Predictive Dialing System. It provides a subset of PDS commands for the IR system, which allows the IR to act as agents attached to the PDS.

The *dialer_conn* process on the IR system enables one port for communications with the PDS. This port is used for sending configuration and control information back and forth between the IR and the PDS.

Process	Ports	Protocols	Purpose
dialer_conn	22800	tcp	IR to PDS communications

4.1.13.13 Vonetix

Vonetix is software provided by Gold Systems that provides an infrastructure for integrating applications on the IR system with a company's existing communication interfaces. For more information, see the Vonetix web site, www.vonetix.com.

Vonetix uses plug-ins to provide connectivity between the IR system and corporate data systems. These plug-ins enable ports for communications with the data systems. The default port numbers can be changed if needed.

Default Ports	Protocols	Purpose
28080	tcp	Vonetix Web Administration
28005	tcp	Tomcat control messages for Vonetix
443	tcp	Vonetix Document Plug-in - Secure web server
1521	tcp	Vonetix JDBC Plug-in - Communication with local/remote Oracle Server
5000	tcp	Vonetix JDBC Plug-in - Communication with remote DB2 Server
6764	tcp	Vonetix JDBC Plug-in - Communication with remote Sybase Server
23	tcp	TN Series Plug-in
20171, 20172	tcp	MQ Series Plug-in

4.2. Restrict Root Access

The root login has the highest level of authority on the IR 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 IR system be administered so that direct root logins are restricted to the system console only. This is the default configuration on all IR systems.

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

Operating system and version number information is normally 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 a 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. This is the default configuration on all IR systems.

4.4. Hide the FTP Banner

Operating system and version number information is normally displayed when a user attempts to access the system via FTP. This information is displayed before a user performs any authentication procedures. Individuals who are attempting to access a system fraudulently can use the OS and version number information to attack the system using known security vulnerabilities.

Avaya recommends that the FTP daemon be modified so that the operating system and version number information is not displayed before user authentication is complete. This is the default configuration on all IR systems.

4.5. Restrict Users Allowed to Use Inbound FTP

If inbound file transfers from remote systems are needed, the FTP daemon on the IR 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 IR system using 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.

4.6. Modify the Default SNMP Community Strings

The SNMP service normally uses default values for the SNMP community strings. Because these values are commonly known, individuals can use these default values to attempt to access the system fraudulently.

If SNMP is used, the community strings should be modified to avoid the use of well-known strings.

4.7. 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.

Note that the IR system uses *cron* jobs to perform periodic maintenance tasks. These jobs are executed by the root login. Therefore, the root login should not be denied *cron* access, as doing so may affect system operations.

4.8. 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.

4.9. Disable Anonymous/Guest Logins

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

The IR 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. Companies should also provide each individual IR system user with a unique login ID so that activities can be associated with a specific user.

4.10. Use Stronger TCP Sequence Numbers

By default, the IR system uses the “improved” TCP sequence number generation scheme, which uses a random variant in the sequence number increment. This is the default setting for the Solaris operating system. However, this sequence number generation scheme may be subject to TCP sequence prediction (IP spoofing) attacks.

The TCP sequence number generation parameter should be modified to use the RFC 1948 sequence number generation scheme.

4.11. Make the System Stack Non-executable

Some security exploits attempt to overwrite parts of the program stack in an attempt to get the system to execute arbitrary code. Some of these exploits can be avoided by making the system stack non-executable. The system stack is executable by default.

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 communication over untrusted networks.

SSH is the underlying protocol over which the SFTP service is provided. SSH provides the authentication and security functions for SFTP. Therefore, SFTP is most often associated with [SSH](#).

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.

On IR systems using Solaris 10 as the operating system, SSH is provided by default. On IR systems using Solaris 8 as the operating system, SSH can be installed using the openSSH package. (<http://www.sunfreeware.com>).

Service	Ports	Protocols
sftp	22/tcp	ssh
sftp	22udp	ssh

6. SSL

SSL (Secure Sockets Layer) is a protocol that provides a mechanism for securely transmitting documents over the Internet. The protocol allows client/server applications to use encrypted transmissions as well as perform client/server authentication. This helps prevent eavesdropping, tampering with transmissions, and message forgery.

Avaya IR Release 1.2.1 and later provides SSL support for both the Web Administration utility and the VoiceXML feature. All Web Administration traffic for IR 1.2.1 and later runs over an SSL/HTTPS connection. This ensures that no Web Administration data is transmitted in clear text. This includes logins and passwords, configuration changes, and views of the system configuration.

Application developers can specify whether VoiceXML application data should be transmitted in an encrypted format using SSL, or as clear text. Secure transmission is accomplished by using a URL that starts with *https*: when an SSL connection is needed. If encrypted transmission is not required, the URL can start with *http*:.

SSL is **not** supported for Web Administration or the VoiceXML feature on IR Release 1.2 and earlier.

7. Account and Password Administration

Companies should implement good user account management practices to help secure access to the IR 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.

7.1. Account Management

Companies should follow the same practices for IR 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, such as 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.

7.2. Password Administration

The IR 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 6 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 forces users to change their passwords after a configurable number of days.
- Set up passwords for new users to force them to change the password at the first login.

7.3. Role-based Authorization Capabilities for System Administration

The IR system provides role-based authorization capabilities for controlling access to its web-based administration utility. Companies should use these capabilities to control which users are allowed to modify the IR 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 switch interfaces or backup and restore activities. The tasks associated with these two web administration roles are not configurable.

Root access is required to assign permissions.

7.4. Logins Provided with IR Systems

IR systems are pre-administered to include several user logins. These logins are as follows:

- root - This login has the highest level of authority on an IR system. Companies are responsible for controlling access to the root login on their systems. See section 4.2.
- tsc, craft, and ivrppp – These logins are reserved for use by Avaya support personnel. See section 13.
- cron - This account is used for establishing the cron jobs needed by the IR system. The cron account is a locked (inaccessible) account. It cannot be used for logging in to an Avaya IR system.

IR systems are also administered with several other accounts that are installed by default in the Solaris operating system. These accounts are for standard daemons, which are processes usually started at boot time to perform some system-wide task such as printing, network administration, or port monitoring. These accounts are:

- daemon
- bin
- sys
- adm
- lp
- uucp
- nuucp
- listen
- nobody
- noaccess
- nobody4

The *listen* account is administered as a locked account. All the others are administered as NP (no password) accounts, which means they have passwords which are impossible to use. Because of this, these accounts cannot be used for logging into an IR system.

For more information on these accounts, see "Managing User Accounts and Groups (Overview)" in the *Solaris System Administration Guide, Volume 1*.

8. 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.

8.1. Operating System Logging

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

- /var/adm/sulog – Log of all attempts to assume another user ID using the su command
- /var/adm/vold.log – Log from the Volume Management daemon

- `/var/adm/wtmpx` – User access log (logins and logouts — should be viewed using the “last” command)
- `/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 commands, etc. The `syslog` log file locations are configurable.

8.2. IR Logging

The IR system 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 web-based administration utility
- All commands executed from the system command line

Because all command invocations are logged, companies can use the IR logging to determine if any access 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 IR 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 IR 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. However, Avaya recommends that only Avaya service personnel administer alarms and messages.

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.

IR log files are stored in the directory `/var/spool/log/data`.

As mentioned above, the IR message administration tools can be used to indicate whether particular log events should be treated as alarms. The dial-out alarming capability supports up to

three dial-out locations and can be used to automatically notify system administrators when alarm events occur. The IR system also 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.

9. Modem Access and ASG

Dial-in lines on the IR system can be protected by an Avaya-developed solution called Access Security Gateway (ASG). The ASG package is integrated into the IR 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 private key-pair cryptographic authentication scheme. Secure auditing is also provided. Logs are available that include information such as successful logins, failed logins, errors, and exceptions.

Even though IR dial-in lines are protected by ASG, some companies are concerned about the potential security risks of having a modem connected to their IR 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 IR dial-out alarming capability, and it makes it more difficult for Avaya technicians to respond to trouble escalations and service requests. Another alternative would be to use a dial-out-only telephone line connected to the modem. While this alternative would still restrict the Avaya technicians' ability to access the system, it would allow the dial-out alarming capability to remain functional.

If a company wants to turn off the modem or connect it to a dial-out-only telephone, it should contact Avaya so that the appropriate information can be put in special handling notes in the Avaya support organization's tracking database. The company must also ensure that a local support contact is available who can activate remote access if an Avaya technician needs to troubleshoot or service the IR system.

10. Disaster Recovery

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

IR systems should be backed up regularly. Companies should maintain two complete system backups. For Avaya IR R2.0, optional tape backup mechanism has been introduced, in addition to NFS (Network File Service) backup present in the older versions of Avaya IR. The backups should be identified by type, content, and date. Backups should be stored *away* from the IR system; if possible, they should be stored at an off-site location.

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

- IR 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 IR 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 locations.
- 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 IR 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 IR 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, contact them at <http://www1.avaya.com/services/portfolio/buscontinuity/index.html>.

11. 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 IR system 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 IR system. Also, self-service applications can be used to transmit customer data between the caller and the IR 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 IR system. 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 1-866-832-0925 or see <http://www1.avaya.com/services/portfolio/security/index.html>.

11.1. Preventing Unauthorized Use

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

- Block outbound access to the network at the switch (PBX or central office) that provides service to the IR system. Blocking outbound access includes blocking call origination, bridging, and transfer capabilities. This method does not rely on a secure IR system 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 IR 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 IR administration is not well-controlled or only provides partial protection).

Another way to prevent unauthorized use of the IR 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 digit 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 IR Feature Test package (AVfst) and assign it to channels when testing is required. The Feature Test 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 application can be spawned to alert the administrator about the calls.

11.2. 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 switch interfaces or perform backup and restore activities.
- Make sure that modems are administered properly to prevent access by outside users. If feasible, the phone line should be disconnected from the modem when the modem is not in use. See section 9.
- 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 IR application requires authentication from the customer.
- Make sure that sensitive customer data is encrypted as necessary using either the tools provided with the Solaris operating system or another solution.

12. Operating System Patches

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

Sun Microsystems provides the Solaris operating system. Avaya monitors the Sun web site for Solaris patches on a regular basis and posts a list of certified patches on the support.avaya.com web site on a quarterly basis.

If a company is aware of a Solaris 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.

13. System Access by Avaya Technicians

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

- In response to an 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 IR system.

All IR 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.

IR systems are pre-administered to include the “tsc”, “craft”, and “ivrppp” 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. The ivrppp login is used only for starting a Point-to-Point Protocol (PPP) connection to an IR system. The PPP connection is used if the support personnel need to run the Web Administration utility over a dial-up connection.

The tsc, craft, and ivrppp accounts should not be changed, disabled, or have their passwords aged. Doing so will impair Avaya’s ability to support the platform. The initial passwords for these accounts are administered when the system is provisioned. The passwords are then maintained by the Avaya support organization.

14. Known Security Issues in Avaya IR

The following items address known security issues with IR features, as well as actions companies can take to help mitigate them.

14.1. JDBC

Some JDBC drivers transmit clear text data between the JDBC client and the database server by default. Because of this, database connectivity between the IR system and the remote database servers may not be secure.

Several third party vendors offer packages that provide secure JDBC connections. Avaya has tested the Avaya IR R2.0 system on an IDS 4.1 server with an Oracle 10g database. The IDS Server 4.1 is an Internet database access server that enables both Java and .NET applications to connect to the database. Avaya has validated that the IDS server provides a secure connection

between the Avaya IR system and the Oracle 10g database. The IDS server supports all the databases which IR 2.0 system supports.

Companies should ensure that the IR system and the database servers, as well as any routers or other equipment that transmit data between the two, are located in a protected environment (that is, behind a firewall or on a physically isolated LAN, as well as in a physically secure location) to reduce the risk of eavesdropping. If this is not feasible, companies should avoid using the JDBC feature for sensitive applications or data.

14.2. IVR Designer Service Creation Tool

As mentioned in earlier sections, the IVR Designer 5.3 service creation tool requires either the use of exec service with FTP or the use of SFTP with SSH to transmit and install applications on the IR system. However, FTP and the exec service both have inherent security risks, as they both allow clear text transmission of data. Because of this, a person snooping on the network between the IVR Designer PC and the IR system could potentially obtain sensitive data such as login and password information.

To reduce this risk, companies should ensure that the IVR Designer PC and the IR system are located in a protected environment. In addition, companies may disable the FTP and exec services, once their application development is complete and the final application has been installed on the IR system. Companies may choose to use the combination of SFTP and SSH, to provide a more secure transmission environment. This environment eliminates the inherent risk present in the use of the exec and FTP service.

14.3. Web Administration Utility

Avaya IR Release 1.2 and earlier systems do not support SSL for Web Administration. Therefore, Web Administration data for these releases, including login and password information, is transmitted in clear text over an unencrypted link. This implies that an unauthorized individual could potentially obtain sensitive information by using a network sniffer or similar tool.

SSL is supported on Avaya IR Release 1.2.1 and later. If companies are concerned about the potential for unauthorized access to their Web Administration data, they should consider upgrading to IR 1.2.1 or later.

14.4. VoiceXML Feature

Avaya IR Release 1.2 and earlier systems do not support SSL for the VoiceXML feature. Therefore, VoiceXML application data for these releases is transmitted in clear text over an unencrypted link. This implies that an unauthorized individual could potentially obtain sensitive information by using a network sniffer or similar tool.

SSL is supported on Avaya IR Release 1.2.1 and later. If companies are concerned about the potential for unauthorized access to sensitive VoiceXML application data, they should consider upgrading to IR 1.2.1 or later.

15. 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 IR systems make this trade-off decision. They know how best to 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.

Appendix A. Services Disabled by the *disableServices* Command

A.1 Services in the */etc/services* File

The */usr/bin/util/disableServices* command disables the following services in the IR system's */etc/services* file:

Service	Port/Protocol
tcpmux	1/tcp
echo	7/tcp
echo	7/udp
discard	9/tcp
discard	9/udp
systat	11/tcp
daytime	13/tcp
daytime	13/udp
netstat	15/tcp
chargen	19/tcp
chargen	19/udp
smtp	25/tcp
time	37/tcp
time	37/udp
name	42/udp
whois	43/tcp
domain	53/udp
domain	53/tcp
bootps	67/udp
bootpc	68/udp
hostnames	101/tcp
pop2	109/tcp
pop3	110/tcp
imap	143/tcp
ldap	389/tcp
ldap	389/udp
ldaps	636/tcp
ldaps	636/udp
submission	587/tcp
submission	587/udp
tftp	69/udp
rje	77/tcp
finger	79/tcp
link	87/tcp

Service	Port/Protocol
supdup	95/tcp
iso-tsap	102/tcp
x400	103/tcp
x400-snd	104/tcp
csnet-ns	105/tcp
pop-2	109/tcp
uucp-path	117/tcp
nntp	119/tcp
ntp	123/tcp
ntp	123/udp
netbios-ns	137/tcp
netbios-ns	137/udp
netbios-dgm	138/tcp
netbios-dgm	138/udp
netbios-ssn	139/tcp
netbios-ssn	139/udp
NeWS	144/tcp
slp	427/tcp
slp	427/udp
mobile-ip	434/udp
cvc_hostd	442/tcp
login	513/tcp
shell	514/tcp
printer	515/tcp
courier	530/tcp
uucp	540/tcp
biff	512/udp
who	513/udp
syslog	514/udp
talk	517/udp
route	520/udp
ripng	521/udp
klogin	543/tcp
kshell	544/tcp
new-rwho	550/udp
rmonitor	560/udp
monitor	561/udp
pcserver	600/tcp
sun-dr	665/tcp
kerberos-adm	749/tcp
kerberos-adm	749/udp
kerberos	750/udp
kerberos	750/tcp
krb5_prop	754/tcp

Service	Port/Protocol
ufsd	1008/tcp
ufsd	1008/udp
cvc	1495/tcp
ingreslock	1524/tcp
www-ldap-gw	1760/tcp
www-ldap-gw	1760/udp
listen	2766/tcp
nfsd	2049/udp
nfsd	2049/tcp
eklogin	2105/tcp
fs	7100/tcp

A.2 Services in the */etc/inetd.conf* file

The */vs/bin/util/disableServices* command disables the following services in the IR system's */etc/inetd.conf* file:

Service Name or RPC Program	Protocol	Process Name
name	udp	udp
shell	tcp	in.rshd
shell	tcp6	in.rshd
login	tcp6	in.rlogind
comsat	udp	in.comsat
talk	udp	in.talkd
uucp	tcp	in.uucpd
tftp	udp6	in.tftpd
finger	tcp6	in.fingerd
systat	tcp	ps
netstat	tcp	netstat
time	tcp6	<i>internal</i>
time	udp6	<i>internal</i>
echo	tcp6	<i>internal</i>
echo	udp6	<i>internal</i>
discard	tcp6	<i>internal</i>
discard	udp6	<i>internal</i>
daytime	tcp6	<i>internal</i>
daytime	udp6	<i>internal</i>
chargen	tcp6	<i>internal</i>
chargen	udp6	<i>internal</i>
100232	rpc/udp	sadmin
rquotad	rpc/datagram_v	rquotad

Service Name or RPC Program	Protocol	Process Name
rusersd	rpc/datagram_v,circuit_v	rpc.rusersd
sprayd	rpc/datagram_v	rpc.sprayd
walld	rpc/datagram_v	rpc.rwalld
rstatd	rpc/datagram	rpc.rstatd
rex	rpc/datagram_v	rpc.rexd
100083	rpc/tcp	rpc.ttdbserverd
ufsd	rpc/*	ufsd
100221	rpc/tcp	kcms_server
fs	tcp	fs
100235	rpc/ticotsord	cachefs
100134	rpc/ticotsord	ktkt_warnd
printer	tcp6	in.lpd
100234	rpc/ticotsord	gssd
100146	rpc/ticotsord	amiserv
100147	rpc/ticotsord	amiserv
100150	rpc/ticotsord	ocfserv
100068	rpc/udp	rpc.cmsd

A.3 Services in the */etc/rc2.d* Directory

The */usr/bin/util/disableServices* command disables the following network service startup scripts in the IR system's */etc/rc2.d* directory:

<u>Script Name</u>
S70uucp
S71ldap.client
S72slpd
S73cachefs.daemon
S74autofs
S74xntpd
S80lp
S80spc
S88sendmail
S93cacheos.finish
S94ncalogd
S95ncad

A.4 Services in the */etc/rc3.d* Directory

The */usr/bin/util/disableServices* command disables the following network service startup scripts in the IR system's */etc/rc3.d* directory:

<u>Script Name</u>
S15nfs.server
S34dhcp