Security and Avaya™ Communication Manager Media Servers

Issue 3.0
Summer 2005
# Table of Contents:

- Introduction 3
- Elements of Security 3
- Vigilance 4
- Updates 5
- Security by Design 5
- Linux 5
- Avaya Media Servers 6
- Link Protection 12
- Virus Protection 12
- Testing 13
- Environment 13
Introduction

This paper discusses security as it relates to the Linux based media servers used in Avaya communication systems. Its purpose is to highlight for owners and prospective owners of Avaya Media Servers, the approach Avaya has taken to secure these systems and to provide information to assist owners in operating them in a secure manner. The information is necessarily generic and incomplete; incomplete because this information is valuable both to those who would like to protect the system and also to those who have more sinister motives; and generic because, as has been said many times, security is a journey, not a destination. By the time you read this paper, it will somewhat obsolete. The journey never ends. The advancement of technology never stops. Avaya never stops. There are new attacks every day. New countermeasures are developed and deployed to meet them.

Papers such as this that were written a few years ago would have focused mostly on toll fraud issues. Earlier systems did not interface with the data network and were neither susceptible to the types of attacks prevalent on those networks nor provided a gateway into such networks from which an attack might be launched. With the convergence of voice and data and the advent of IP Telephony, this is no longer true. Toll fraud is still an important issue, but one that is covered in other Avaya documentation. This paper focuses primarily on security issues that arise due to the connection to the enterprise data network.

Elements of Security

A chain is only as strong as its weakest link, a house only as secure as its weakest door, window, or wall. If a burglar alarm is installed in a house but turned off, there are two consequences. One, the house is not secure and two, a lot of time, money, and effort are wasted installing the alarm system in the first place. All doors, all windows, all walls, all systems (whether figurative or literal) must be secured.

Securing a system does not begin with the system itself, but with the people and organization that operate or use it. One of the most important tools for securing a system is to have a written, published, security policy and to make sure it is enforced. RFC2196 will help you to create a security policy and defines these steps:

1. Identify what you are trying to protect.
2. Determine what you are trying to protect it from.
3. Determine how likely the threats are.
4. Implement measures which will protect your assets in a cost-effective manner.
5. Review the process continuously and make improvements each time a weakness is found.

In examining whom to protect against, do not forget to look internally. A significant number of attacks come from within.

Part of the "measures" should include rules about behavior, the consequences of bad behavior, a path of escalation, and whom to notify of security issues. It does little good to enforce long randomized passwords if people are allowed to write the password on a sticky note on their computer monitors.

Often the weakest links are the most obvious and most easily overlooked and often involve human behavior. e.g., locking the doors to the equipment room and wiring closets. Denial of service is easier to
accomplish with a hammer or wire cutters than with the root password.

Security is very often a trade-off; the more security, the more pain and the more cost. The more pain the more likely the human users will subvert the security measures. Make passwords too complex such that they are difficult to remember and people will write them down. Users prefer easy access without security; having to log on is inconvenient; not being able to cross mount file systems is inconvenient. However, everyone must endure some level of inconvenience if the system is going to be secure against those who would do harm. The security policy needs to define this level of pain and ensure that it is not circumvented by anyone.


Vigilance

A new security policy is in place. The journey has now begun.

New products come on the market. New versions of software become available. New vulnerabilities are discovered. New attacks are launched. Security patches are published. New people are hired. Some people leave.

Now is not the time to rest. Now is the time to be ever watchful, to monitor what is happening in the environment and to respond quickly. A number of organizations are dedicated or have dedicated departments to help in monitoring. Two prominent examples are the Computer Emergency Response Team (CERT®) at Carnegie Mellon University and the SysAdmin, Audit, Network, Security Institute (SANS™). These and other groups search for product vulnerabilities and/or monitor for the appearance of malicious software such as viruses or trojans and generate alerts when something important is found. Avaya’s Security Rapid Response Team (SRRT) monitors alerts from CERT, SANS, Red Hat and others who monitor events pertinent to Avaya’s products. Avaya’s SRRT evaluates each of these alerts against Avaya’s products, classifying the alerts as high, medium, low or not applicable. For alerts that receive a high classification, a response is produced within 24 hours. This response includes remediation actions that can be taken (if any), and a software update (if immediately available) or a timeline for availability of an update if additional time is needed. A list of such alerts is available at http://support.avaya.com/security

Any Avaya customer can subscribe to automatically receive alerts as they occur. Access http://support.avaya.com and click on register now under Self-Service Support, or click on My E-Notifications if already registered. Anyone can also send Avaya information about suspected vulnerabilities or other security concerns relevant to Avaya’s products by sending mail to securityalerts@avaya.com.

---

**Updates**

Customers should monitor for alerts from all the relevant organizations such as CERT or SANS or Red Hat as well as from vendors such as Avaya to obtain information for all the products which they own. Whenever a security alert is announced, it is important that updates to affected products are installed as soon as possible to minimize the exposure.

This, however, is not as straightforward as it might appear. Re-read item number 4 in *Elements of Security* above. It says, "Implement measures which will protect your assets in a cost-effective manner". Or in the vernacular, "Don't be dumb!". If an update is installed on a live production system, and the update itself has a problem, the cure may be worse than the original disease. Perhaps this is a new type of denial of service -- denial of service by fright (DOSBF). Be vigilant, but don't be frightened into moving too quickly.

Security conscious customers continually query Avaya as to why they should not monitor, for example, the Red Hat advisories, obtain the update directly from Red Hat, and install it immediately. The answer is simple. The reason to obtain the update from Avaya is to avoid being a victim of DOSBF. Before Avaya releases a security update, Avaya thoroughly tests the update on a non-production system, along with all the other software that is normally loaded (and not loaded) on an Avaya server. Sometimes the update must be modified before it will work correctly. For example, a Red Hat update might depend on a module that Avaya does not load on the server. This is not to say that Red Hat (or any vendor) produces bad updates. Rather, it is a reflection of the complexities of modern software. What works in one environment may fail totally in another and there are too many environments for anyone to test all of them.

**Security by Design**

Security is something that should be designed into the product and processes from the beginning. Security is much more difficult to add in later and often less effective. Being able to design securely means understanding all aspects of security, from business continuity planning, to access security, to secure management and servicing, to development methodologies. It means being able to anticipate areas of difficulty in order to formulate a multi-layered framework to guide development. It means using industry best practices and being ever vigilant for improvements. Further information on secure by design can be found on the Avaya web at http://www.avaya.com. Search for the phrase, "Avaya Trusted Communications Framework".

**Linux**

The move from Oryx-Pecos to open operating systems such as Linux is often looked upon as a move to a less secure environment. To some extent this is true, but it is very important to understand why. Oryx-Pecos is used in systems which either did not support data connectivity at all or supported such connectivity in interface cards isolated from the rest of the system. Without data connectivity or with very restricted connectivity, the types of security attacks are much reduced. Unfortunately, so is the functionality. Oryx-Pecos is more secure because it does not support the types of connectivity that the convergence of voice and data demand.

So why not enhance Oryx-Pecos? Aside from the economic reasons, there is a security paradox: *To make an operating system secure, reveal its inner most secrets*. When the operating system software is publicly available and used in varying environments and for a wide range of applications, there are many many

---

5 Oryx-Pecos is the proprietary operating system used by Avaya’s DEFINITY® systems.
more eyes, both friend and foe, looking for security holes. The expertise of the entire technical community is brought to bear on the problem. The weakness created by exposing the flaws is outweighed by the probability that they will be fixed and the speed of getting it done.

Of the major operating systems (Unix, Linux, Windows), one is not inherently more secure than another. All are completely not secure out of the box. All can be made secure through the application of a good security policy which includes proper administration and configuration, and diligent application of vendor updates when security problems are discovered. Linux has a slight advantage in that problems can be identified both by testing (hacking) and by review of the source code itself.

**Avaya Media Servers**

**Linux**

The Avaya Communication Manager Media Servers run under the Linux operating system. Linux has two features which are important for security. First, there is built in protection against certain types of Denial of Service (DOS) attacks such as SYN floods, ping floods, malformed packets, oversized packets, sequence number spoofing, ping/finger of death, etc. Attacks are recognized at the lower levels of the software and their effect blunted. (It is not possible for a target system to always provide service during a DOS attack; the protection is to automatically resume service as soon as the attack is removed.) Second, the Linux kernel is compiled with a set of options to precisely tailor its operation to maximize security consistent with required operation of the system. These include a number of built-in firewall and filtering options.

All file and directory permissions are set to minimize access as much as possible consistent with proper system operation. Multiple partitions exist on an Avaya Media Server disk drive. Each partition is restricted according to the type of data that it may contain. Some partitions contain only software executables; these partitions are mounted to allow program execution. Other partitions contain only data; execution of software from these partitions is disabled.

The Avaya media servers use a hardened Linux operating system customized for real time applications and based on the Red Hat Linux distribution. The entire Red Hat Linux distribution is not loaded. The operating system is specifically configured for these servers. This means that only those components that are needed are loaded and modules that are not used are not loaded. Additionally, components that are used only in certain configurations are disabled when not used. Examples of modules affected by these policies include NFS, SMB, X-windows, rcp, rsh, rlogin, and rexec.

All IP ports that are not used are closed and firewalled.

**Secure Access**

Typical mechanisms of server access include telnet, WEB Browser (HTTP), and FTP for file transfer. Each of these mechanisms can support login authentication, but suffer a common weakness. During the login sequence, the password being supplied by the user is sent in clear text. This allows a person with a network monitor/sniffer to capture the password and gain access. In addition, these mechanisms transmit all the session information in clear text. Some of this information might contain data such as account codes, authorization codes or other data useful to an attacker. To overcome these problems, Avaya Media Servers also support Secure Shell Access (SSH), Secure Copy (SCP/SFTP), and secure WEB access using the Secure Sockets Layer (SSL) with HTTPS.

SSH and SCP/SFTP provide an access mechanism for terminal access and file copy that encrypt the entire
session including the login sequence as well as subsequent data transfer.

SSL/HTTPS provide a similar mechanism for WEB access. HTTP administrative access is automatically redirected to HTTPS.

In addition, the Avaya Media Servers support one-time-passwords for logins through these mechanisms even though the exchange is already encrypted.

On an Avaya Media Server, the FTP service is disabled by default. Each time a file is to be transferred to the server, an administrator must log in and enable the FTP server. The file is then transferred using anonymous FTP, and the FTP server can then be disabled. (The FTP server will automatically disable itself after a period of inactivity.) Using anonymous FTP in this manner avoids the problem of sending passwords in clear text. However, SCP is the preferred method of transferring files.

**One-Time-Passwords**

The Avaya Media Server software provides an option to use one-time-passwords for all logins. A regular password account uses a fixed user name (ID) and a password which can be used multiple times to log into the system. A person who can monitor (network sniffer) the login messages can capture this password and use it to gain access. A one-time-password uses a fixed user name, but not a fixed password. Instead, every time a user attempts to log in, they must supply a password which is unique to that session and which will be incorrect if used again. Even if the password is compromised, it cannot be re-used immediately or at a later time, even by the same person from the same terminal. One-time-passwords can be enabled for each login on an Avaya media server.

**Shell Access**

Access to a “shell” from which arbitrary commands may be executed is not granted by default to a login on an Avaya Media Server. When a login is created, the system administrator can specify whether or not the account is permitted to have shell access. Accounts which are denied shell access receive either an Avaya Communication Manager software administration screen or a WEB page upon successful login. In both cases, the operations that may be performed are restricted. In general, shell access is needed only by individuals that perform hardware or software maintenance of the server.

**Root Access**

On a Linux system the highest level of administrative access is known as “root”. Direct login to a root level account is not permitted on an Avaya Media Server. Administrative access which requires root level permissions is handled via “proxy” programs which grant limited access to specific accounts and create auditable logs. The ability to obtain full root level access is granted only in very special circumstances, and then only to a user who is already authenticated with a lower privileged account.

**Remote Access**

Avaya media servers can be accessed remotely in one of two ways, either via a modem connection or via a network connection. Either method, and remote access in general, are not helpful to security. Security professionals generally frown on (and some corporate security policies forbid) modems, because modems form a point of entry that bypasses the corporate firewall. Remote network access is also problematic in that such access has to be carefully firewalled and constrained to specific devices. Support for any sort of remote access is part of the trade-off in providing cost effective security.

Remote access is used by Avaya services for delivery of maintenance alarms to Avaya and for access by
maintenance technicians. Both a modem based remote access and a Virtual Private Network (VPN) based access are supported.

Understanding the issues with modem access, Avaya has configured this feature with maximum flexibility for the system user. The server logins which are used to establish a remote modem connection are separate from those that allow administrative functions. One account is used to establish a connection; once the link is established, a second login is required using a separate account.

Use of the dial in line can be restricted for incoming calls by choosing one of the following:

- disallow all incoming calls
- allow one incoming call only
- allow all incoming calls

When the interface is set to "allow one incoming call only", the line is enabled to answer a single call. As soon as a call arrives, the line is disabled and must be re-enabled via administration before another call will be accepted. This feature does not inhibit outgoing alarm calls which are needed for maintenance. The feature is intended to be used as follows. Normally, the line is disabled for all calls. When a maintenance activity is needed, the maintenance technician must contact the server administrator via telephone, e-mail, etc. and request the line be activated. The server administrator must then log in to the server and enable the line for one call only. The maintenance technician then calls the server, performs necessary maintenance and disconnects. At this point the line is automatically disabled again.

Enabling the data line for one call only is a good example of a feature that illustrates the trade-off required between security and convenience. Having the data line disabled provides better security. But during diagnostic activity when multiple calls must be made, the server administrator must be called to manually re-enable the line for each call. This can be a nuisance and slow down the maintenance work. In addition, Avaya employs expert systems technology to contact systems automatically for monitoring and diagnostics. Disabling the data line disables this technology, resulting in higher maintenance costs and possibly longer down times when a failure does occur.

As an alternative to modems, Avaya also offers a Virtual Private Network (VPN) based solution, known as Avaya Global Services Secure Access and Control (SAC). Full information can be obtained at http://support.avaya.com/sac/. In this solution, a VPN/firewall is placed on the customer’s network. The unit is controlled and administered by the customer to restrict access by Avaya technicians to only those products that are appropriate. Similarly, alarms are delivered to Avaya via this secure link.

**Monitoring and Alarming**

Avaya Media Servers support a variety of security monitoring features. Accounts are automatically locked out for a period of time as a consequence of consecutive failed login attempts. Files and directories are monitored and audited by tripwire. All login sessions, whether successful or not, are logged. All interactive shell command activity is logged. Security events are alarmable events which can be reported as an SNMP trap to one or more destinations.

**Data Protection**

Attacks against a system are not limited to attempts to find holes in the access structure. There are also techniques known as data mining, dumpster diving, or "phishing" that can be used even more effectively

---

6 See also http://www.avaya.com and perform an advanced search for “Secure Access and Control” to locate the white paper, Secure Access and Control 3.0 for Services Delivery in a Converged Communications Environment.
if the system owner is not careful.

Avaya Media Servers have the ability to store (backup) copies of critical configuration information including authentication and account information on external systems. If this information is stored in clear text, and the file server on which it is stored is compromised, the Avaya Media Server could be compromised. To make this more difficult, Avaya media servers have the ability to encrypt all backup data. This option should always be used when using the backup feature. It is the user’s responsibility to remember the key, because Avaya will not be able to assist if the key is forgotten.

From time to time, new software features are created which require that the software or firmware be updated. This process involves the transfer of executable files to the Avaya media servers or other system components from a variety of sources. It is important that these files arrive exactly as they were created at Avaya. To prevent malicious modification in transit, all distributions are cryptographically signed so that modifications can be detected and installation prevented.

In the protection of data, social engineering must not be overlooked. In particular, users must be made conscious of "phishing" attacks in which attempts are made to get users to send sensitive information ostensibly for verification. Avaya never sends e-mails requesting login credentials or other sensitive information. If such attacks are received they should be forwarded to securityalerts@avaya.com and otherwise deleted and ignored.

**LAN Isolation**

Avaya provides communication systems in a wide variety of configurations to support customer needs. One way to classify these systems is whether the main media servers are simplex or duplex. Duplex server systems provide higher availability (up to 99.999% availability) whereas simplex server systems are lower cost.

Figure 1 is an example of a configuration with duplicated main processors. Each media server can employ 5 or more separate Ethernet interfaces (NICs) and media gateways can contain additional Ethernet interfaces. Multiple NICs allow LAN traffic to be isolated for either traffic or security reasons. The figure shows the following types of LANs:

- Enterprise LAN
- Control LAN (Duplicated)
- Duplication LAN
- Local Access LAN
- Adjunct LANs

The enterprise LAN is used for administration and time synchronization; telephony traffic does not use this LAN. Two control LANs are used to connect between the servers and the gateways. These two LANs can be private LANs carrying no other traffic and can be encrypted. The duplication LAN is a point-to-point LAN that is only used to send information between the two duplicated servers. The local access LAN is a point to point LAN that is used only for local administration and maintenance and carries no other type of traffic. Adjunct LANs can be used to isolate traffic for services such as call detail recording or voice mail.
The enterprise LAN, control LANs, and adjunct LANs can all be connected together to form one network, or they can be kept physically separate for either traffic or security reasons. Separation can be physical or accomplished through VLANs.

In order to provide the most secure environment possible for the system, network access should be divided into separate zones of control (sometimes referred to as DMZs). Figure 2 illustrates one example. In this example, LANs are configured to isolate traffic and access according to function. One VLAN could be administered for administrative traffic, one for call signaling, another for voice bearer traffic, etc. Layer 3 boundary devices (routers, layer 3 switches, and firewalls) should be administered to enforce the corporate security policy on traffic destined for the Avaya Media Servers, Media Gateways, or adjuncts. Packet filters could be put in place to permit administrative access only from an administrator’s PC and to deny access from the Avaya Media Servers or their gateways to the corporate LAN, while allowing appropriate access for call signaling and bearer traffic from all IP telephones.

The Avaya Media Server software can itself be configured to allow only certain types of access to specific LAN interfaces on its gateways. So, for example, in figure 2, even if one were to connect an administration terminal to one of the other (non-administrative) LANs, administration access would be denied.
**Disaster Recovery**

Security isn’t just about hackers and software attacks. Security involves protecting the entire enterprise from all events that might disrupt its normal functioning. These events include normal LAN disruptions as well as large scale acts of nature, vandalism, or even terrorism. Avaya’s communication systems can be configured for maximum survivability should the network become fragmented or parts of the system become inoperable, including the main servers. Figure 3 illustrates the addition of two types of survivable servers, Enterprise Survivable Servers (ESS) and Local Survivable Processors (LSP). (Some details removed from the figure for simplicity.) These spare servers can be located in multiple physical locations and take over control of portions of the system or the entire system depending on the type of disruption. Hundreds of these servers can be added to the system as needed.
**Link Protection**

The modern communications system employs many physical and logical links to exchange data between system components as well as from user to user. These links include media gateway control links, registration, admission, and status (RAS) links, call signaling links, media (voice or data) links, and administration access links. Each of these links must be protected, both from information loss to persons who shouldn’t have it and from interference/disruption or theft of services. Protection is achieved by encrypting the entire link, by encrypting critical data and/or by secure challenge/response mechanisms. Voice streams can be protected (administratively selectable) by encryption with the Advanced Encryption Standard (AES) algorithm or by an algorithm known as the Avaya Encryption Algorithm (AEA). Server/gateway signaling links are protected with AES by default. Administration links can use SSH or TLS/HTTPS.

**Malware Protection**

The viruses and worms that have made the headlines have mostly targeted Microsoft Windows operating systems or more specifically some of the Microsoft application software such as IIS, Exchange, Outlook,
or Word. Because the Avaya Media Server is Linux-based and does not employ any of this software, it has some level of natural immunity. In addition, viruses and worms are most commonly delivered via e-mail, by visiting infected WEB sites, or by sharing of disk drives. The Avaya Media Server does not support incoming e-mail, does not support forwarding of e-mail (since there is no incoming e-mail in the first place), does not support user WEB browsing, and does not support NFS or SMB (i.e. does not share drives).

The Linux operating system used by the Avaya Media Servers is not the standard distribution of Linux. Many modules are not loaded on the Avaya server. This means that malware which depends on specific capabilities being available (like a compiler) is thwarted.

All software releases and updates transferred to the Avaya Media Server are cryptographically signed to prevent introduction of unwanted software.

In addition to this natural immunity, the Avaya Media Server incorporates additional anti-tampering features. The disk drive is divided into multiple partitions. Executable code is stored in separate partitions from data; data are likewise stored in separate partitions which do not have execute permissions. Direct root level access is not normally permitted, and when it is granted, the login is protected by one-time-passwords. This is important because one of the first goals of an attacker is to obtain root level access as this provides the opportunity for the most destruction. Login accounts on the Avaya system do not necessarily receive any type of shell access. This is also important because shell access allows the user to enter commands at will, whereas the more controlled access limits the user to the functionality presented on menus or screens. The files and file system is monitored by tripwire. This software product maintains a cryptographically encoded signature of the files on the system and generates alarms in the event any unexpected changes occur.

The Avaya Media Server development team considered adding some form of virus scanning software to its repertoire. However, virus scanner software for Linux is not common, generally because the market and threat is not sufficiently large to entice scanner vendors. In addition, those vendors that do offer Linux scanners primarily scan e-mail to prevent the spread of a virus to Windows based machines on the same network; they do nothing for the Linux box itself. As already stated, Avaya Media Server has no incoming e-mail and so there is nothing for these products to scan.

**Testing**

During the development of the Avaya Media Server based system or in production of upgrades to its software, Avaya subjects the system to a variety of common “attack tools” as additional validation steps aimed at reducing the likelihood of known vulnerabilities being re-introduced. The exact set of tools which are used varies to keep up with the technology. Common tools include nmap and nessus. Security problems found by these efforts are corrected prior to the product or update being released.

**Environment**

Avaya has taken steps to make the Avaya Media Servers as secure as is reasonable, consistent with the operational needs of the product and business it serves. Security, however, does not end with the servers and host security is only one aspect of a layered security approach. These servers will be connected to one or more networks, which are in turn connected to other equipment in the enterprise. As a minimum, these servers should be located behind a firewall. Where this firewall is located with respect to other LAN components must be designed on a case-by-case basis. Avaya professional services can assist owners in configuring their networks for both security and optimal Voice over IP (VoIP) operation. In addition other
vendors specialize in this type of consulting. Owners are advised to seek assistance if internal staff is not trained in these areas. Security holes which arise from negligence, ignorance, or oversight or the pressures of schedule or budget are all equally usable by those who would do harm.

Malicious activity is a moving target. What is safe today may not be safe tomorrow. Avaya is committed to providing appropriate secure solutions for its products and continuously monitors the nature of these threats. As this paper is written, the Avaya Media Servers are appropriately secure against the known threats. Avaya will respond quickly should new threats appear. Your Avaya account team and Avaya’s support web site (http://www.avaya.com/support) should be consulted for the latest information in this area.

© 2005 Avaya Inc. All Rights Reserved. Avaya and the Avaya Logo are trademarks of Avaya Inc. or Avaya ECS Ltd., a wholly owned subsidiary of Avaya Inc. and may be registered in the US and other jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of their owners.