



Hardening Practices of the Linux Operating System within Avaya Communication Manager

Abstract

Although Avaya uses Linux in its product line of Avaya Communication Manager media servers, Avaya take specific steps to customize the installation for reasons of management, performance, and security. This document outlines the steps Avaya is taking to harden the Linux operating system for use in its media servers.

1. Introduction

The Linux Operating System has grown in popularity over the last decade with promises of an “open-source” alternative other operating systems. Since it is open-source, users hope to ride the wave of technological features and contribute to their improvement without the limitations or expenses of proprietary operating systems.

However, as the popularity of Linux has grown, so has its varied capabilities and features – most of which will not be used by any particular end-user.

Avaya’s Communication Manager™ and Converged Communication Server™ utilize the Linux operating system. However, these products implement Linux in a manner that is customized to meet the demands of IP Telephony. The follow sections describe the specific areas where Avaya has customized Linux to allow it to align with the demands of IP telephony including making it more manageable, more secure, and more stable.

2. Linux Hardening Efforts

2.1. RPM Removal

General distribution of Linux includes RPMs for most, if not all, possible Linux configurations. These distributions include a complete development suite, complete graphics support for X- Windows, numerous development debugging tools, a variety of network administrative tools, etc. However, for IP Telephony only a small portion (15-20%) of the distributed RPMs is actually needed. As the distributions of Linux include more RPMs (Red Hat Package Management) modules, the relative percentage of RPMs needed by Avaya applications become a smaller percentage.

Because Avaya’s products do not need most of the packages provided in the general distribution, these unused RPMs are removed from the Avaya products prior to release.

Aside from making the software product file images smaller and more manageable, it actually makes it more secure. With such a large number of RPMs actually removed, they cannot be compromised because they are not present on either Communication Manager or Converged Communication Server.

2.2. Closure of Ingress Ports

Many modules of Linux are applications which open Ingress network services. Examples would be SSH or Apache over SSL/TLS (HTTPS). In an effort to minimize exposure of the operating system to network-based attacks, Avaya reduces the number Ingress network services to only those which are needed. Additionally, there are some legacy network services which are still supported (e.g. FTP). For those services, Avaya provides the ability to disable the service when it is not needed.

2.3. Firewall Protection

To provide an additional layer of protection, the Linux Operating System of Communication Manager and Converged Communication Server are running the IPTables firewall (CM2.1 and higher). This firewall utility provides protection against various kinds of networking attacks and is also used to provide protection against Ingress services which are enabled via the XINETD mechanism (which listens for connection requests or messages for certain ports and starts server programs to perform the services associated with those ports).

Avaya provides a web-based, user-interface for management of the IPTables firewall where the administrator can specifically open and close ports based on the needs of their implementation.

2.4. Logging

Extensive logging of operating system and application-level activity is performed. To prevent unauthorized modification of log files, administrators may use web-based tools to only read the log files instead of risking inadvertent modification of the files. Additionally, log files may be backed-up and stored off-premise.

2.5. Secure Protocols

Secure protocols, such as SSH and HTTPS (HTTP or TLS/SSL), are implemented to provide the utmost in privacy and authentication at the protocol-level. The protocols implemented are intended to be compliant with industry standards of security.

Although a number of legacy protocols are still available on the platform, Avaya is always striving to provide secure, interoperable alternatives to meet customer needs.

For recommended implementation practices of Communication Manager, please see:

- **Avaya IP Telephony Implementation Guide**
<http://www1.avaya.com/enterprise/applicationnotes/av-iptel-imp-gd-acm-0503.pdf>
- **IP Telephony Deployment Guide**
http://support.avaya.com/elmodocs2/comm_mgr/r2_0/245801_1_1/245600_2/245600_2.pdf

2.6. Drive Partitioning

Linux provides the ability to partition of the hard drive of the server in a number of ways. One of the valuable features of this capability is its ability to mount partitions with a NOEXEC flag which prevents binaries located on those partitions from being directly executed. Avaya uses the NOEXEC capability when partitioning the hard drive of its linux-based servers for Communication Manager or Converged Communication Server and a precautionary measure against malware.

2.7. Vulnerability Tracking

Avaya has an active organization which tracks security advisories and susceptibility of Avaya products to vulnerabilities described in those advisories. This organization coordinates Avaya advisories which generated in response to those advisories issued by vendors who supply operating systems or software components to Avaya. To sign up for advisory notification, please go to <http://support.avaya.com> and Select “My e-Notifications.”

For more detail on Avaya tracking policies and practices, please see:

- **Avaya's Product Security Vulnerability Response Policy**
http://support.avaya.com/elmodocs2/security/security_vulnerability_response.pdf
- **Avaya Security Vulnerability Classification Policy**
http://support.avaya.com/elmodocs2/security/security_vulnerability_classification.pdf

2.8. Privilege Escalation

Communication Manager and Converged Communication Server adopt the concept of “privilege escalation.” To implement this concept, only accounts with a lower privilege can log into the server. If higher privileges are required by the technician, they must log in using their normal accounts first and then escalate their privileges to perform more restrictive tasks (such as software replacement). Each time a technician escalates their privileges, logs are created containing the time that the escalation occurs. Since an escalation requires a password or ASG response to be entered, this significantly restricts the ability for a would-be intruder to obtain root-level privileges.

2.9. Prevention of direct UID 0 Login

As indicated in the previous section, the concept of privilege escalation requires that only lower-privilege accounts are allow to directly login to the system. The means that the high-level (a.k.a. root-level or UID-0 level) account cannot login directly to the system.

2.10. ASG Protection

Once a system is installed, all support accounts are protected by the Access Security Guard (ASG). ASG is a challenge-response mechanism which replaces the use of passwords for administrative or technical support accounts with a mechanism that challenges the user differently for each login. In particular, when a person attempts to login to the server using an ASG-enabled account, instead of a request for a password, the person is given a randomly-generated number and they must perform a calculation using that number to determine the correct response. Only if the correct response is entered, is the user allowed to log in. For more on ASG, please see:

- **Protecting Passwords Using the Avaya ASG**
<http://www1.avaya.com/enterprise/whitepapers/protectingpasswordsusingmv.pdf>

2.11. Ongoing Improvements

The aforementioned hardening steps are just the beginning.

Linux is an ever-changing operating system with numerous contributors. Avaya works diligently to monitor the enhancements and improvements created by the Linux community and adopt those changes into Avaya products. However, many changes available to the Linux community require careful review before incorporation into Avaya products to ensure interoperability, understand performance impact, and understand implications on security and support.

Similarly, Avaya strives to make changes to its foundational architecture to continue to provide high-availability products which do not require frequent patching or updates. Through a constant process of improvement, Avaya works to find new ways to meet the needs of our customers through further OS hardening, improvements in monitoring, logging, and reporting; greater protection against denial-of-service attacks, and secure transport and storage of information.

Furthermore, certification of Avaya products is important. Avaya is actively pursuing certification of its products against Federal standards. Achievement of these certifications means that Avaya has designed and implemented features to a level of security that allows the Federal Government to approve it for its own use.

3. Kernel Hardening

The Linux kernel provides great flexibility for hardening. Avaya does not use the “off-the-shelf” Linux kernel. Avaya’s kernel is based on the Linux-community offering but has been “tuned” for the demands of real-time telephony processing including handling unique conditions about our servers or to give finer grained time increments. In many cases, when kernel advisories have been issued by the Linux community, Avaya is already inherently immune because of the changes we have made in an effort to make the kernel better suited for the demands of our applications.

4. Conclusion

Avaya has been the industry leader in providing a foundation for its Communication Manager and Converged Communication Server products. This foundation is an Avaya-hardened Linux Operating system with numerous features and capabilities which not only meet the needs of real-time communications processing, but also meet the needs of our customers.

©2004 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. All other trademarks are the property of their respective owners. The information provided in this White Paper is subject to change without notice. The technical data provided in this White Paper are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in this White Paper.