Compliments of Avaya
Leader in IP technology

AVAYA

VoIP Security FOR DUMMIES®

Avaya Limited Edition

Realize VoIP benefits and stay secure!

A Reference for the Rest of Us!®

Peter H. Gregory, CISA, CISSP
Security speaker and columnist, author of Blocking Spam & Spyware For Dummies

What is the truth about VoIP security? Finding the right partner that delivers secure IP telephony — while leveraging existing security investments — is the key.

There is no single "right way" to do VoIP security — it may require "ground-up" design, or it may require only an upgrade here or there. It makes good business sense to apply security holistically across the enterprise for both voice and data. The challenge is finding the right way to make an environment as secure as possible for the least possible cost and effort.

Avaya products utilize best-of-breed security design and implementation that integrate with existing security services in small and large businesses. Avaya Global Services provides expert advice for small business and world-wide enterprises, and brings Avaya's depth of expertise to bear on any company's VoIP security needs.

Explore the possibilities at
www.avaya.com.

AVAYA

VoIP Security FOR DUMMIES®

AVAYA LIMITED EDITION

by Peter H. Gregory

Wiley Publishing, Inc.

VoIP Security For Dummies®, Avaya Limited Edition
Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774
www.wiley.com

Published simultaneously in Canada

ISBN-13: 978-0-470-00987-1

ISBN-10: 0-470-00987-X

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1O/ST/QT/QW/IN

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at www.dummies.com/register/. For details on how to create a *For Dummies* book for your company or organization, please contact dummiesrights&licenses@wiley.com.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Christine Berman

Acquisitions Editor: Melody Layne

Business Development Representative: Jackie Smith

Editorial Manager: Jodi Jensen

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Janet Seib, Michael Sullivan

Proofreaders: Jessica Kramer, Dwight Ramsey

Additional proofreading help: Tom Porter, Jim Mannion, Andy Zmolek, Kevin Johnson, Doug D'Angelo, Horst Kuchelmeister, Juniper Networks, Extreme Networks, Patricia Moran, Lisa Kluberspies

---

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Acquisitions Director

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Joyce Pepple, Acquisitions Director

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Table of Contents

Introduction

Traditional enterprise telecommunications networks used to be viewed as relatively secure because you practically needed to be within physical reach to gain access to them. Sure, things like toll fraud and war dialing were problematic, but those were easily remedied by longer or more complicated passwords and other access controls. The age of converged networks has changed that — with voice now traveling over IP networks (VoIP). These converged networks inherit all the security weaknesses of the IP protocol (spoofing, sniffing, denial of service, integrity attacks, and so on). In addition, voice quality and confidentiality are potentially affected by common data network problems such as worms and viruses. Converged networks also offer an array of new vectors for traditional exploits and malware, as each IP endpoint becomes a potential point of network entry.

Not only is VoIP exposed to old attacks introduced by new methods and vectors, VoIP itself also exposes a few new vulnerabilities. Hacking is also converging as intrusion techniques are becoming more widely available via the Internet and other media. To be sure, VoIP demands a new way of thinking about security. And converged environments require converged security that protects all network information and extends to IP applications.

Data networks, including the Internet, are under constant, deliberate, and ever more harmful attack. People attack data networks for many reasons, from thrill to monetary gain; they attack data networks *because they can.* IP is an open protocol with characteristics that make network endpoints such as IP phones and home computers, as well as network devices such as routers, ripe for exploitation.

Attacks don't happen just because of weaknesses in the IP protocol itself. When IP protocols were first designed, cybercrime was nothing but science fiction and networking software vulnerabilities were widespread. If, by some miracle, IP

were fixed overnight and all its direct and indirect weaknesses were eliminated, hacking would continue because of weaknesses inherent in the endpoints.

If you're a telecom manager of IT, pay attention. If you're considering implementing VoIP, the Internet's security issues will become *your* concerns. No more whistling past the graveyard — it's time for you to become informed. But take heart. New security methods and mechanisms can make VoIP networks virtually as secure as trusted telephone networks, while letting you reap the benefits provided by converged voice and data networks.

Paradigm Shift

In the 1980s, the Internet's security paradigm was "connect everyone and trust everyone." The Internet was small — mostly accessed by military and educational users — and public access was extremely limited. The World Wide Web had not yet been developed, there were few sites of general interest, and moving around the Net was often cumbersome. The fear of malicious intent was minimal. Neighbors knew each other, and no one locked their doors at night.

But security incidents in the late 1980s and early 1990s, many with devastating consequences, precipitated a new paradigm: Trust internal users, authenticate external users, and protect the internal network with a firewall.

By the late 1990s, innovations in Web software, along with a dramatic increase in the number of organizations who were exposing internal information and applications to external users, led to today's paradigm: Trust no one, authenticate everyone (and everything), know (and control) where your data is at all times, and protect data whether it is at rest or in motion.

Many organizations think that firewalls and a bit of internal authentication are still sufficient to protect their information assets. This older mindset is vastly insufficient for converged networks. You must build your network with the latest security in mind to make communication reliable.

Securing networks is not a trivial task, and there is no instant solution. The following table describes what you need to do to secure your network and how it may be vulnerable.

What You Must Do	*What Hackers Can Do*
Protect every point of entry	Attack the weakest point of entry
Be constantly vigilant, 24/7/365	Attack at a time of their choosing
Close every vulnerability	Exploit all vulnerabilities
Close every known vulnerability	Search for new vulnerabilities

Converged networks are a win-win for everyone. Converged networks, and the IP applications running on them, offer tremendous advantages in terms of cost, flexibility, and new application capabilities. Your organization will enjoy greater flexibility, improved responsiveness, and increased productivity. To ensure that your organization realizes these benefits, security must be part of your company's VoIP recipe starting on day one — not day one of implementation or day one of operations, but day one of requirements, architecture, and design. By building in security from the start, your VoIP network will be as secure (if not *more* secure) than your old telecom network.

The Avaya Advantage

As you begin to understand the significance of converging your traditional telephony systems onto your data network to create an enterprise-level communications network, keep one thing in mind: You don't have to throw out the investments you've made in other telephone system hardware. You can do it the Avaya way, avoiding forklift upgrades and reaping the benefits of the new IP-based features and functionality available *right now* in the VoIP world.

You need reliability, security, and availability, and Avaya delivers all three. If you're considering a converged voice and data network, you're seeking a lower-cost, business-driven architecture that gives you an edge over your competitors. Avaya can help you accomplish that goal. Avaya is helping more than a million companies around the world today, including more than 90 percent of the Fortune 500 companies.

To protect your organization's communications, Avaya offers its Trusted Communication Framework. The Framework, built on open standards and architecture and based on best practices, is a multilayer approach for distributing security features and services throughout your communications environment. By using a distributed architecture, security is designed into each solution instead of being added after the fact. (See Part IV for more details about Avaya's Trusted Communications Framework.)

Avaya has forged strategic alliances with many top network companies, including Juniper Networks and Extreme Networks, to address all the layers of the Trusted Communication Framework. By leveraging Extreme's strength in LAN switching and Juniper's strength in secure routing, a complete standards-based solution can be deployed that delivers secure communications.

About This Book

Regardless of your role in your organization, VoIP security matters. Your role determines the part you play in incorporating security into your VoIP environment.

If you are a manager playing a role in the implementation or operation of your VoIP network, this book is an excellent place to begin. If you are a systems administrator, software engineer, network designer, auditor, or security expert, you'll find enough details to engage you and get you started thinking about issues in your own environment. If you are an end-user, this book will lift the veil and show you the future of converged voice and data communications and how they are protected. If you'll be using the new VoIP network, this book gives you an appreciation for the types of issues that converged network personnel face today.

You'll see three different perspectives on VoIP security in this book: the business perspective (why security is important), the technical perspective (what the threats are and how they're solved), and the products and services perspective (what Avaya offers organizations that want to leverage a secure VoIP network).

For a more thorough understanding of VoIP security, you might want to read this book cover to cover. But if you're in a hurry, jump to the part of the book that answers the questions you have right now.

How This Book Is Organized

Each part of this book considers a different aspect of securing a VoIP environment. The following sections explain what you'll find in each of the four parts.

Part I: Making the Business Case for VoIP Security

Part I explains why security is needed for VoIP. It starts by defining some basic security terms you need to know.

In case you aren't sure that your VoIP environment needs security, Part I describes some of the things that could happen if security features are *not* present in your communications network and applications and also discusses current security regulations. Part I continues by explaining security issues you should consider if you're planning to add VoIP to your existing network, or if you are designing an entirely new converged infrastructure to support all your voice and data needs.

Part I ends with a discussion of security planning best practices that you should consider, particularly if you are going it alone.

Part II: Recognizing and Managing Security Issues

Part II explains the security issues related to VoIP and converged networks, including technological and people-related security threats and vulnerabilities. Threats and vulnerabilities can be resolved, and Part II describes these solutions.

Part III: Designing and Building Security into Your VoIP Network

Whether you're in the planning stages of your network or are already operating a VoIP network, security needs to be an integral part of your environment.

Part III highlights Avaya's products and services to support VoIP security and continuity in the converged network environment. Avaya's products include media servers and gateways that can help enhance security for your environment, with functionality such as encryption techniques that protect critical data links and voice streams. In this part, you also find out how Avaya Global Services can provide you with VoIP security consulting and planning services, system security, secure remote maintenance, and ongoing network and application monitoring services.

Part IV: Ten Reasons to Look to Avaya for VoIP Security

There are lots more than ten good reasons to partner with Avaya. We can name fifteen reasons — just like that (insert sound of snapping fingers here). And fifteen is nowhere near the limit.

Part IV describes the best reasons to use Avaya security solutions. Do it right the first time and make Avaya's security solutions a part of your VoIP security strategy.

Icons Used in This Book

Icons are used throughout this book to call attention to material worth noting in a special way. Here is a list of the icons along with a description of each:

If you see a Tip icon, pay attention — you're about to find out how to save some aggravation and time.

This icon indicates technical information that is probably most interesting to IT professionals.

Some points bear repeating, and others bear remembering. When you see this icon, take special note of what you're about to read.

Where to Go from Here

If you already have a VoIP network, be sure to read Part II to understand the threats and potential weaknesses in your VoIP environment. And you may want to enlist assistance from Avaya Global Services to identify these and any additional threats and weaknesses and get your organization on a plan to reduce risks to an acceptable level.

If you're considering migrating to a VoIP network, read Part I to understand why security needs to be a part of your strategy from the very beginning — not something to be spray-painted on at the end.

If you're already beyond the conception stage and have begun the high-level work of designing or building your converged voice and data environment, read Part III to understand where and how Avaya's products and services can assure your success.

No matter where you are in your VoIP project, never lose sight of the big picture: Avaya is the voice and converged networks expert and has strategic vision and leadership in VoIP and VoIP security. Companies that go with Avaya to realize their own VoIP network reap all of the benefits of Avaya's knowledge, experience, and strategic partnerships with Juniper and Extreme Networks. Turn the page and discover for yourself why Avaya is the undisputed leader in converged voice and data environments.

Part I

Making the Business Case for VoIP Security

In This Part

- Understanding consequences of inadequate protection
- Considering security regulations
- Looking at how VoIP security affects infrastructure and application security
- Moving to centralized security services
- Building a VoIP security plan

Fear, uncertainty, and doubt, known as FUD in the information security industry, is a popular tactic used to scare customers into purchasing security mechanisms they may or may not need. You'll see no FUD in this book — just the facts.

Few people would argue with the idea that a data network needs to be secure. You need the same security for voice as you do for data in converged environments, and new security challenges arise in converged networks. The attacks aren't new, but the telecommunications environment is exposed to the same worms, viruses, and hackers as data networks. Converged networks also offer an array of new vectors for traditional exploits, and you must secure these as well.

In security-speak, you need to understand three key security concepts: vulnerabilities, threats, and incidents.

- *Vulnerabilities* are weaknesses present in a program, network, device, or system.
- *Threats* are the possible actions or attacks that may take place, particularly in a vulnerable system.

- *Incidents* are the events that can take place if someone or something successfully damages, disrupts, or steals information from an information system.

This part helps you understand the importance of a security plan and some of the incidents you may risk if you don't protect your VoIP network. To find out more about vulnerabilities and threats, and to see how you can mitigate these risks by choosing the right vendor, check out Part II.

The Consequences of Not Protecting a VoIP Network

The question isn't *if,* but *when*. Left unprotected, anything connected to the Internet eventually is open to attack. The more popular the device or system, the sooner the attack is likely to happen.

As VoIP becomes more widely deployed, hackers will devise attacks that directly target IP media servers, gateways, and even phones! Already, worms and other malicious code attack smart cellular phones and instant messaging (IM) programs.

Twenty minutes . . .

. . . is how long it takes for an unprotected PC to be compromised when connected to the Internet. That's down from forty minutes a year ago. Thousands (if not tens of thousands) of systems scan the Internet, seeking to identify devices of every type of system that can be exploited. These numbers come from a study conducted by the Internet Storm Center, a part of the SANS Institute. The SANS Institute is a highly respected organization dedicated to security education for IT and IS professionals.

Remnants of virulent worms such as Blaster, Sasser, Slammer, Nimda, Nachi, Code Red, and others continue to scan the Internet, seeking new victims. Like biological viruses, it is unlikely that many of these cyber-infections can be completely eradicated. As computing power increases, it becomes increasingly easier to execute attacks with far-reaching effects from a simple PC.

When any IP-connected product appears in sufficient numbers, the attacks are more likely to begin.

The Internet isn't the only means of attacking a system or network. Several ways exist to attack an *information system* — a generic term meaning just about any system or network device connected to a network.

Here are the types of incidents that may occur in a converged network that doesn't have adequate security measures in place:

- **Eavesdropping.** An improperly protected VoIP network may permit an intruder to listen in on VoIP conversations or access voice-mail messages.
- **Access to sensitive information.** An intruder may be able to access information on servers, gateways, phones, and other network devices such as switches, firewalls, or routers. Available information could range from device configuration information (which may permit a hacker to more easily attack other devices or systems) to business secrets. A VoIP network breech can also be used to gain access to the entire data network.
- **Vandalism.** An attacker may want to damage a company's network by erasing or altering information or by changing the way a device or system operates. The type of damage a vandal can inflict is limited only by his or her imagination. The type of damage may be immediately apparent or it may take days, months, or even years to discover the destruction.
- **Quality of service.** An attack may have more subtle effects upon a VoIP network that are manifested in reduced call quality: jitters, voice-quality, prematurely terminated calls, and so forth.

Aside from these types of incidents, keep in mind that you still must address traditional telephony attacks to a VoIP network, such as toll fraud and voice-mail breech.

Detecting security incidents can be difficult. And, as mentioned earlier, these incidents may be easily detected or may go undetected for a long period of time.

Designing and building with the principles of *least privilege* and *least need* go a long way toward protecting information systems. Least privilege is the concept of providing only the access required to fulfill any given function. Least need is the concept of including only the functions required for an application or system to function.

From a high-level point of view, all devices that participate in network communications should follow the principle of *least.* This is particularly important for critical infrastructure, including servers, routers, firewalls, and so on. You should disable anything not required or in use, turn off all unneeded services, and remove all unnecessary applications. Following the *least* philosophy reduces the number of possible attacks on the system.

Regulatory Compliance

As a VoIP user, what do you need to know about U.S. privacy regulations? Neither the Gramm-Leach-Bliley Act (GLBA) passed in 1999 to protect the personal financial information of consumers, nor the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protects consumer healthcare information, specifically addresses security within the communications infrastructure. However, these acts also do not specifically *exclude* communications — so you can't simply ignore them.

Under HIPAA, the test for what information is covered is whether "protected healthcare information" is stored electronically in a system. For a VoIP call, that test is met only if the call is recorded and stored. So voice-mail and call recording systems may need to document HIPAA conformance if healthcare information is likely to be discussed. Any call center systems that access healthcare records will similarly require documentation.

As with HIPAA, GLBA has a *safeguarding* component distinct from the privacy component you may be familiar with because of the disclosure statements you routinely receive in the mail. A couple of years ago, the Federal Financial Institutions Examination Council (FFIEC) finally came out with detailed guidance for bank regulators; but again, you won't

see VoIP systems specifically mentioned. But it's a good idea to treat VoIP systems just like any other application on the data network and periodically check FFIEC guidance in the event they add VoIP security standards. And it's prudent to ensure that VoIP conversations and related information are secured from the prying eyes of eavesdroppers and hackers — regardless of the status of regulation.

A great deal of regulatory uncertainty still surrounds the concept of *lawful call interception*. A recently released summary of the new FCC Communications Assistance Law Enforcement Act (CALEA) appears to suggest that "facilities-based broadband Internet access service providers" (which seems to cover any organization offering any type of cable modem, DSL, satellite, or wireless service) must be prepared to accommodate law enforcement wiretaps within the next 18 months or face fines.

Less clear still is the responsibility of an organization in providing E911 services. In July 2005, the FDA mandated that within 120 days VoIP providers must offer this enhanced 911 service, which delivers a caller's name, telephone number, and physical address directly to the console of the local Public Safety Answering Point (PSAP) in an emergency. It's clear that few organizations will be able to accomplish this; most are waiting for an extension to the deadline.

How VoIP Security Affects Data Security (and Vice Versa)

If you have an existing data network and you plan to add VoIP to it, you need to assess your current data network, paying particular attention to the security devices, features, and mechanisms already in place. Some mechanisms may need to be reconfigured, updated, or replaced to accommodate VoIP's needs. For example, as more remote users leverage VoIP, the Virtual Private Network (VPN) gateway may need to be upgraded to accommodate the significant increase in IP traffic due to the VoIP streams. You will also need a VPN product that doesn't add even a moderate amount of latency to the conversation, which may result in poor audio performance.

If you decide to start with a clean slate and design an all new converged network that supports both data and voice, you need to keep both voice and data security requirements and features in mind and design for the security of both.

You may need to move your current systems from your existing data-only network to a new converged network. In that case, you need to do migration planning. But rather than view the migration planning as a hindrance, consider it an opportunity to discover ways to streamline and protect your new converged network.

Either way, unless you have seasoned VoIP/converged network experts in-house, you should plan to engage Avaya Global Services to assist with architecture and planning so that your new converged network can support your voice and data needs. AGS can put the security features in place to ensure the integrity, availability, and confidentiality of your voice and data applications.

Moving to Centralized Security Services

Building a converged network is a great opportunity to introduce centralized security services into your environment. Here are a few examples of these security services:

- **Authentication.** Consider centralizing authentication using RADIUS- or LDAP-based services. RADIUS and LDAP are open standards embraced by virtually all systems and network vendors for central authentication and access control.
- **Event logging.** Think about building a central log server; design new applications and features to utilize it and migrate existing systems to it. Be sure to use intelligent software to correlate and analyze the log data.
- **Network management.** Consider acquiring a Network Management System (NMS). If you are adding a significant number of infrastructure devices to your network to support VoIP, you may be better off in the long run with

centralized network management that will assist with fault detection and mitigation, as well as performance monitoring and tuning.

- **VPN Technology.** VPNs enable remote workers at virtual office locations to receive the same functionality as if they were sitting at the central office location. Whether it is a VPN/firewall gateway at the virtual office or a VPN remote for an IP phone client, remote workers are increasingly using VoIP as a core means for communications at virtual office locations. For branch offices scattered throughout the world, consider deploying a VPN device at those locations that enables connectivity back to the central location.
- **Implement core network security.** You can do this via the vendor that provides the IP network infrastructure as well as additional security appliances.

Security can be an enabler instead of a hidden tax. For example, centralized authentication with LDAP, centralized log file and event correlation, and network management are security-related services that can save money and better protect information through economy of scale. Without these central services, these capabilities need to be built into each application, often at greater expense.

Building a VoIP Security Plan

Although there is no silver bullet for securing an enterprise communications environment, Avaya has established a list of best practices based on years of experience and documented research by various security experts. Avaya also teams with Juniper Networks and Extreme Networks for WAN and LAN security, providing you with a complete solution. But even if you have a Cisco network, Avaya has voice and data security competency that can help you. Avaya suggests the following best practices to its customers:

- Plan effectively for multilayered security (in-depth planning for defense, for example) to meet business and regulatory requirements.
- Implement, communicate, and enforce security policies.

- Deploy a robust security architecture and "best-of-breed" solution components.
- Harden operating systems and encrypt when and where possible.
- Secure implementation processes and maintain operational security practices.
- Manage security through proactive monitoring, event management, remediation, and follow-up actions.

The next part of the book, "Recognizing and Managing Security Issues," explains how to protect your VoIP network in even greater detail.

Part II

Recognizing and Managing Security Issues

In This Part

- Examining the threats to VoIP
- Understanding VoIP vulnerabilities
- Protecting your VoIP network

The Internet is under attack. Hackers can exploit everything that's connected to TCP/IP networks — and that's *everything* — and attacks are becoming increasingly more sophisticated. You can bet that as more organizations migrate to VoIP networks and become more widely deployed, they'll be popular targets as well.

If you outsource your VoIP network security, you still need to understand these security issues in some detail. Each issue has potential business impact by affecting costs, processes, or technical architecture (usually all three!).

Threats to VoIP

In this chapter, the words *threats* and *vulnerabilities* are tossed about pretty freely. People often use these terms interchangeably, but they're actually quite different. Here's what they mean:

- *Threats* include hackers, viruses, worms, Trojan horses, phishing scams, spam, spyware, malware, and more.

- *Vulnerabilities* are weaknesses (whether by design or by configuration) which, left unattended, increase the risk of a system attack or failure. Hackers often attack a VoIP network by exploiting vulnerability.

Just as a coach knows the strengths and weaknesses (vulnerabilities) of his team, you need to be aware of security threats and what you're doing about them. That's why you're reading this chapter — so buckle up and hang on!

This chapter discusses two kinds of threats: technology-based threats and human-based threats. Although classifying types of threats can be difficult, most security professionals think of threats in this way.

Although related, threats and vulnerabilities are different. A threat is the intention or indication of impending harm, whereas a vulnerability is a weakness. Threats usually *target* and *exploit* vulnerabilities.

Technology-based threats

What kinds of technology-based threats do you need to be concerned about in the context of VoIP networks? Here are the most important threats:

- Infrastructure-based attacks
- Application-based attacks
- Call interception
- Denial of Service attacks
- Session hijacking/impersonation
- Pharming
- Caller ID spoofing
- Toll fraud
- Protocol-specific threats (H.323, SIP, and MGCP)
- Worm storms
- Day Zero attacks

I talk about each of these threats in more detail in the following sections.

Infrastructure-based attacks

At the device level, VoIP networks are traditional data networks engineered to run voice applications. They contain routers, switches, servers, and gateways. These devices are mass-produced by well-known companies, and are often ubiquitous. Hackers know how to exploit vulnerabilities in these devices. Their attacks on networks can compromise system integrity, expose information, and disrupt service.

Viruses and worms are designed to exploit weaknesses in software. Viruses need user action to propagate, whereas worms do not. Some can replicate on their own, and others need a nudge from unknowing people to propagate through networks. Some of these worms and viruses are designed to merely disrupt normal services, whereas others are designed to inflict harm by changing configurations or retrieving sensitive data.

Application-based attacks

Relatively unheard of ten years ago, tools and methods for attacking applications are readily available. Many attack tools are highly automated and spend their time searching for newly implemented applications to exploit.

Call interception

Make no assumptions about privacy when you send information over a data network. E-mail, instant messaging, and (yes) VoIP traffic are all subject to eavesdropping. Think of information traversing in the same way as post cards traveling by mail — anyone along the way can read the contents of a message.

A conversation on a VoIP network passes from handset to handset through many devices and networks. Someone who is able to access any of the devices or networks through which VoIP traffic passes may be able to intercept VoIP data packets and intercept a conversation.

In a data network, intercepting data packets is trivial. Many sophisticated tools such as Ethereal are free and easy to use to collect packets associated with one or more VoIP conversations.

Denial of Service attacks

A Denial of Service (DoS) attack occurs when someone deliberately floods a particular network (or device on a network) with so much illegitimate network traffic that legitimate use is impossible.

You may be able to understand a DoS attack more easily through this real-world example: In 2000, French farmers, ambulance drivers, truckers, and taxi drivers protested the high price of gasoline by blocking freeways and fuel depots with their vehicles. In two days, the entire country had virtually shut down because fuel couldn't be distributed to gas stations. The French truckers had mounted a DoS attack on France's transportation system by blocking all its legitimate uses.

Internet DoS attacks are not unlike the truckers' protests in France. Flood the networks (or the freeways) with enough traffic and all legitimate uses are virtually unavailable.

DoS attacks are becoming more potent than before. Hacker gangs and organized crime organizations are creating *bot nets* and *bot armies* consisting of thousands of ordinary home (and work) computers that they can control remotely to launch attacks on companies and governments.

Stopping a Denial of Service attack is very difficult, although with proper architecture, critical assets can be spared from a direct attack. Hardware products are available that can absorb the blow from a DoS attack; another solution is to have more bandwidth than the attacker can muster.

Session hijacking/impersonation

Session hijacking is a type of attack in which an attacker is able to use special hacking tools to place his identity into an active data connection, with the intention of altering the *flow* of data or the data itself.

Data or voice communication sessions are more vulnerable to session hijacking if the data or voice is not encrypted. Hijacking encrypted sessions is nearly impossible because the attacker cannot decrypt the data to alter it.

Pharming

Pharming exploits vulnerabilities in the part of a network device that is responsible for translating e-mail and Web addresses, computer names, and network device names into IP addresses. Without their knowledge, VoIP users' calls can be redirected to IP addresses completely different from the ones the users dialed. In telephony language, this would be like hacking a telecom switch or PBX so that dialed phone numbers would route calls to a rogue location instead of to the intended destination.

Caller ID spoofing

In spoofing, a perpetrator hijacks the identity and phone number of a trusted party, such as a bank or a government office. The identity appears on the caller ID box of an unsuspecting victim, with the caller hoping to acquire sensitive and valuable information such as account numbers, or otherwise engage in malicious mischief. Caller ID spoofing is a particularly vicious ploy because it exploits a socially accepted form of authentication provided by caller ID.

Toll fraud

For years, hackers have perpetrated toll fraud by gaining access to PBX and telco switch maintenance ports to control their operation and permit toll fraud activity.

Without the proper controls, VoIP networks are also vulnerable to toll fraud because gateways and switches can be accessed over data networks. Configuration weaknesses and default administrative passwords would permit easy access by fraudsters.

Protocol-specific threats

Some hackers attempt to break into networks (or just disrupt their operation) by concentrating their attack on the details of the communications protocols that they use.

As VoIP becomes widely used, some hackers will study and look for weaknesses in the protocols that VoIP uses for communication and control. Here are some of the potential threats:

- **H.323-specific threats.** In 2004, The University of Oulu Secure Programming Group (OUSPG) tested the effects of sending modified call setup packets to a number of differing VoIP vendor implementations. They found that many VoIP systems that implement H.323 are vulnerable to one or more of these malformed packets. These failures result from insufficient validation of messages as they are parsed and processed by affected systems. Depending upon the affected system and implementation, these attacks result in system crash and reload, or in the case of systems that filter these data (such as Microsoft ISA server), execution of arbitrary computer software code.
- **SIP-specific threats.** When it comes to Session Initiative Protocol (SIP), more intelligence is moved from the guarded center to the edge of the network — and increased network points of access equal increased network complexity. In addition, SIP may become particularly attractive as a hacking target due to its HTTP-based underpinnings and the ease with which ASCII-encoded packets can be manipulated. Some specific threats against SIP include

  Registration hijacking. Occurs when an attacker impersonates a valid User Agent (UA) to a registrar and replaces the registration with his own address. This attack causes all incoming calls to be sent to the attacker.

  Proxy impersonation. Occurs when an attacker tricks a SIP UA or proxy into communicating with a rogue proxy. If an attacker successfully impersonates a proxy, she has access to all SIP messages and is in complete control of the call.

  Message tampering. Occurs when an attacker intercepts and modifies packets exchanged between SIP components. Message tampering can occur through registration hijacking, proxy impersonation, or an attack on any component trusted to process SIP messages, such as the proxy, media gateway, or firewall.

  Session tear down. Occurs when an attacker observes the signaling for a call and then sends spoofed SIP "bye" messages to the participating UAs. Unfortunately, most SIP UAs don't require strong authentication, which allows an attacker to send properly crafted "bye" messages to the two UAs, tearing down the call.

Denial of Service. Can occur through any of the means described above or through additional DoS-specific attacks. Because strong authentication is rarely used, SIP processing components must trust and process SIP messages from possible attackers.

- **MGCP-specific threats.** Like SIP, with MGCP intelligence is moved from the center to the edge of the network. Threats against MGCP include impersonation, session tear-down, and Denial of Service.

Worm storms

A worm storm can occur when an Internet worm is spreading so rapidly that legitimate Internet traffic is disrupted. Worm storms race around the globe and may last only a few hours, or several days, causing data connections that use the Internet to become congested and unreliable.

Day Zero attacks

A Day Zero attack is a worm or virus that immediately precedes or follows announcements of vulnerabilities in hardware or software products.

Human-based threats

Some threats are considered human-based as they involve acts of commission or omission. The human-based threats you need to be familiar with are

- Hackers
- Social engineering
- Insiders
- Former employees and contractors
- Errors, assumptions, and omissions

Hackers

The term *hacker* encompasses attacks in a range from those perpetrated by *script kiddies* (young adults who use prepackaged hacking software) all the way to extortionists and organized crime. Generally, these are people who use software and

hardware tools to deliberately attack an organization's network or information assets. Here are some of the reasons for hacker attacks:

- **Joyriding.** Some hackers hack just for the thrill of it, not unlike kids of earlier times who threw bricks through plate glass windows and stole automobiles for, well, joyriding. Hackers may perpetrate Denial of Service attacks or outright defacements, where a hacker has been able to exploit a weakness in a company's Web server and replace the contents of the company's Web site with contents of their own. This type of attack is so common that there are many Web sites whose sole purpose is to catalog defacements.
- **Status.** Hackers earn prestige by competing in the hacking community for the top spots — those who have hacked the most computers and the biggest companies.
- **Revenge**
- **Anger**
- **Information theft**
- **Extortion**
- **Industrial or political espionage**

A great way to better understand your vulnerability to hackers is to try to think like one.

Social engineering

Social engineering is the practice of acquiring confidential information by manipulating legitimate users. A social engineer commonly uses the telephone, face-to-face meetings, or the Internet to trick people into revealing sensitive information or get them to do something against typical policies.

Social engineers exploit people's natural tendencies to trust and help someone in need. A typical social engineer can make several phone calls to different people in an organization to obtain information. For example, a social engineer might call one person to get a VPN IP address, and another to get a userid, and still another to get a password reset.

Insiders

Technology workers in the organization have considerably more knowledge than outsiders. Insiders know the architecture, components, IP addresses, server locations, protocols, and have ready access to much of this from inside the office as well as from any other location through VPN remote access.

Employees with a poorly formed conscience or a less-than-stellar work ethic may exploit opportunities to improve job stability, make other employees look bad, or build private back doors for themselves if they find themselves out of a job.

Don't forget insiders — yes, the people you trust to operate and manage your information. Most security incidents are perpetrated by insiders, former insiders, and others with extra knowledge about a targeted company's systems and networks.

Former employees and contractors

Technology workers who have been fired, laid off, or who quit because they felt they were treated unfairly are serious threats to an organization because they possess not only detailed information about the architecture and operations but also access codes that may not have been deactivated. Technology workers often know where weaknesses are and how to exploit them.

Paranoid employees build back doors for themselves to access internal networks and systems in the event they lose their jobs or are transferred to another part of the organization. These back doors enable them to monitor the workplace, steal information, or disrupt operations.

Errors, assumptions, and omissions

Systems and network infrastructures are highly complex and ever changing environments. Even in a highly organized and mature organization with a formal Change Control environment that includes design and peer reviews, testing, and verification, mistakes are bound to occur. Many times these mistakes may create a vulnerability that can later be exploited.

Human-based threats include both malicious acts by insiders and outsiders, as well as innocent mistakes made by people who handle information.

The future of attacks

Bad behavior is part of the human condition: Build something for good and someone else will either attack it or use it to commit malevolent acts. Often, system designers don't anticipate how attacks can happen and resort to quick fixes or retrofits when security issues arise. Those efforts can lead to more complication and opportunities for vulnerabilities.

As with all earlier technologies that have been developed in the networking age, attacks will occur in this sequence:

1. **Operating Systems.** Hackers first exploit features in devices and servers to gain access or disrupt operations.
2. **Protocols.** Hackers exploit weaknesses in network protocols that will lead to malfunctions on devices and servers.
3. **Applications.** Hackers exploit application functionality in order to cause malfunctions at the application level. Hackers have a great imagination here.

Vulnerabilities in VoIP

As with threats, vulnerabilities can be either technology based or human based. Several examples of these two types of vulnerabilities are described in the sections that follow.

Technical vulnerabilities

If you were hoping to find specific vulnerabilities in VoIP cited here, you may find something even better than a complete list. This section describes the *categories* of vulnerabilities and shows you where to find current information. First, here are the types of technical vulnerabilities that you need to be familiar with:

- **Software bugs.** From BIOS to firmware to operating systems to applications, bugs happen. Many go undetected for years; some affect functionality and some create a security weakness that could be exploited to gain unauthorized access, make unauthorized changes (to data or configurations), or disrupt operations.
- **Incorrect configurations.** Configuring devices, operating systems, and applications can be complicated. Getting things to work often requires cooperation between disparate systems. Many configurations are security-related, having to do with authentication, access control, or audit logging, for example. Because of a lack of training, an incomplete understanding of related configurations or architectures, or distractions, employees can configure systems incorrectly. This may result in security weaknesses ready to be exploited.
- **Flawed architectures.** The architecture of a complete information system (a VoIP network, for example), because of flawed design or engineering, can sometimes lead to security vulnerabilities that can be exploited for a variety of reasons.

Human vulnerabilities

We remain imperfect creatures who make more mistakes than we can keep track of. Here are a few of our more obvious mistakes:

- **Lack of experience.** Many times in the high-tech industry, people are hired into positions that are a few sizes bigger than they are. This is typical in high-tech — people don't want a job they've done before, but something challenging that they have not done before. Employees with less experience than most of us would be comfortable with can end up designing, building, or operating information systems.
- **Lack of training.** Experienced workers frequently know what it is that they want a device or system to do, but they may not know *how* to do it. Often, employees are asked to build or deploy hardware- or software-based systems they haven't used. They may understand the concepts, but not the specific methods. Inexperience can lead to security weaknesses.

- **Distractions.** IT departments are squeezed to produce more with less. This is often the case with overworked programmers, network engineers, and system administrators. Coworkers can pull them in many directions at once to complete important projects on time, but still, they must fight the everyday fires.
- **Weak processes and procedures.** Organizations that lack good processes and procedures, especially Change Control, Configuration Management, and IT Architecture and Standards, are more likely to leave weaknesses in their environments that can be exploited by worms, viruses, or hacker attacks.

The key to reducing errors lies in attention to quality as well as formal processes such as change control and configuration management.

How to Protect Your VoIP Network

If you think a lot of system holes remain to be filled, you're right. As you read this section, you'll find that making environments secure isn't just about technology. It's also about business processes, procedures, and people. Without these, no amount of technology will adequately secure an environment.

Implementing protection

IP networks and applications are not naturally safe all on their own, and you need to take several measures to protect them. The following list is not strictly sequential, but it does represent the most important principles for securing VoIP networks:

- Develop and enforce security policies and processes
- Enforce physical security
- Lock down servers, systems, and networks
- Unify network management

- Confirm user identity and enforce security policies at a device level
- Maintain active security monitoring
- Ensure logical segregation
- Use encryption

I describe these protection measures in more detail in the sections that follow.

Develop and enforce security policies and processes

Policy formulation is an important step toward standardization of enterprise security activities. The organization's security policy is management's vehicle for emphasizing the commitment to IT security and making clear the expectations for workers' involvement and accountability.

Policy implementation is a journey. Policy can't merely be dictated by upper management in a one-time statement or directive with high expectations of its being readily accepted and acted upon. Rather, just as formulating and drafting policy involves a process, implementation similarly involves a process, which begins with the formal issuance of policy.

Security policy should address the following areas:

- **Empowerment and enforcement.** Which person or group is responsible for implementing and enforcing security policy.
- **Roles and responsibilities.** Which people or departments are responsible for various security functions.
- **Risk management.** How the organization assesses risk and makes risk decisions.
- **Asset management.** How assets are managed and tracked.
- **Classification and handling of information.** How information is classified according to sensitivity, and how classified information should be handled.
- **HR security.** Screening, terms and conditions of employment, security training, termination of employment and removal of access rights.

- **Physical and environment security.** Secure areas, physical access control, equipment security, environmental controls.
- **Communications and operations management.** Operational processes and procedures, third-party service delivery, system planning and acceptance, protection against malicious code, backup, security management, media handling, exchange of information, e-commerce, and monitoring.
- **Access control.** User access management, user responsibilities, network and operating system access control, application and information access control, and mobile computing.
- **Information systems acquisition, development, and maintenance.** Security requirements, integrity in information processing, cryptographic controls, security in the software/product development life cycle, and technical vulnerability management.
- **Security incident management.** Reporting incidents and weaknesses, management of incidents.
- **Business continuity and disaster recovery.** Information security, business continuity and disaster recovery planning.
- **Compliance.** Compliance with legal requirements, security policy, and applicable laws and regulations.

An effective security policy should be drafted by an experienced team or individual, vetted by several subject-matter experts, ratified by the organization's executive management, and implemented through proper deployment of technology.

A widely recognized source for IT best practices is the ISO17799:2005 standard, which you can find at `www.iso.org`.

Enforce physical security

Physical security is essential, and it forms the basis for many other security efforts. Physical security refers to the protection of building sites and equipment (and all other information and software contained within them) from theft,

vandalism, natural disaster, man-made catastrophes, and accidental damage (for example, electrical surges, extreme temperatures, and spilled coffee). It requires suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Lock down servers, systems, and networks

Every server, gateway, switch, network device, and server should be locked down — a concept that includes the following:

- Disabling or removing all unnecessary services and components in a system.
- Limiting accessibility to all necessary services and components in a system to only people who need it to function.
- Using the most recent versions of software/firmware on the system.
- Installing security patches in a timely manner.
- Authenticating administrative access and encrypting all remote management using SSH or IPsec.

  Avaya S8700 and S8300 servers support Secure Shell access (SSH) and Secure Copy (SCP), and Secure Web access using Secure Sockets Layer (SSL). All Web access to Avaya S8700 and S8300 servers is through a secure connection. Unencrypted Web access is not supported. Media Servers also support the use of one-time passwords for logins through these mechanisms, thus providing another layer of secure access.
- Refraining from using default passwords. Guest accounts should be turned off. All users should be required to use strong passwords and change their passwords periodically.
- Implementing VPN access for employees who require access to centrally-located network resources from off-premises locations. Consider a VPN that supports two-factor authentication such as smart-cards, hardware tokens, or biometrics.

Unify network management

Network management tools that are used on the data network should be used to monitor the entire converged infrastructure. This is one of the advantages of a converged network. Existing network management tools may need to be updated to reflect the enhanced requirements of a VoIP network. If possible, segregate management traffic to an out-of-band, dedicated management network.

Confirm user identity

Confirming user identity is a key part of implementing a secure environment. Some methods available include

- Using handsets that implement user authentication. Avaya handsets support this feature.
- Implementing device authentication with ARP (Address Resolution Protocol) and 802.1X.
- Centralizing user management. Consider using Microsoft Active Directory or LDAP for enterprise-wide authentication into applications, e-mail, VoIP, and other facilities.
- Employing DHCP authentication procedures. Why? Because DHCP is what assigns IP addresses to IP phones.
- Deploying Juniper Networks' Infranet Controller to ensure host checks and security policy conformance.

Maintain active security monitoring

Because you can't anticipate every type and manner of attack in advance, keeping a watchful eye on everything — network components, gateways, and servers — is important. Some of the ways to enhance monitoring include

- **Host-based intrusion detection systems (HIDS).** Software mechanisms on hosts, gateways, and servers watch for anomalous behavior that could be indicative of a security issue. HIDS typically log these events to a central logging server.
- **Network-based intrusion detection systems (NIDS).** Special devices on networks monitor and analyze network traffic in real-time and report anomalies to a central logging server.

- **Centralized logging, correlation, and analysis.** HIDS, NIDS, firewalls, switches, routers, and practically everything else in a network create event and audit logs that should be piped in to a central log server to make it easier to detect and understand complex events. This understanding is achieved through *correlation*, where intelligence in the log server software can detect the presence of significant events by considering what log entries are coming in from many devices. For example, the presence of relatively insignificant authentication attempts on large numbers of devices could signal an organized attack that may require attention.
- **Penetration testing.** The purpose of penetration testing is to detect any security vulnerabilities on network devices, so that they can be repaired. It is much better to find them first and fix vulnerabilities before hackers find them for you.

Ensure logical segregation

Logically segregating voice and data networks is recommended to prevent data network problems from affecting voice traffic, and vice versa. Segregating customer traffic (voice or data) from administrative traffic (network management, command and control, and so on), again is a good idea. Segregation keeps problems in one logical network from adversely affecting other networks.

- **VLANs.** VLANs, or Virtual LANS, can be thought of as logically segmented networks mapped onto physical hardware. Logically separating voice and data traffic via VLANs is a good way to segregate networks without adding physical infrastructure.
- **Traffic shaping.** When voice data is introduced into a network, it becomes most critical that priority is given to the voice packets to ensure the expected quality of voice calls. The mechanisms used to accomplish this are generally called *traffic shaping*. Traffic shaping is an attempt to organize network traffic to optimize or guarantee performance and/or bandwidth. Traffic shaping relies upon concepts such as classification, queue disciplines, scheduling, congestion management, quality of service (QoS), class of service (CoS), and fairness.

- **Firewalls.** Firewalls are points of traffic control between networks. Using a set of site-defined rules, firewalls either pass or block network traffic from entering (and leaving) a network based upon its traffic type, source, and destination. If you're designing a VoIP network, you'll need to consider upgrading your firewall to a make and model that is VoIP-aware because VoIP network services such as H.323 introduce additional complexities that older firewalls have a tough time dealing with. Application Layer Gateways designed to handle VoIP protocols such as H.323 and SIP can help in addressing security concerns.
- **NAT and private IP addressing.** NAT, or Network Address Translation, together with the use of private IP addressing, will provide another layer of control for your network.

Use encryption

All communication between network elements should be encrypted if possible. Complete handset-to-handset IP voice encryption is recommended to mitigate the threat of eavesdropping. Also, administrative access to critical server and network components should use encrypted protocols such as SSL, IPsec, or SSH. All access to remote administrative functions should be restricted to connections to the switch itself or to a designated management PC. Access to Avaya S8700 via the CLAN interfaces should also be disabled.

Encryption is the most effective means of mitigating the problems of eavesdropping or call interception. Until recently, Avaya's H.323-based VoIP products were unique in that they provided media encryption, thus ensuring that even if a call was intercepted, an attacker wouldn't be able to decrypt its contents.

Media or payload encryption is an important piece of the VoIP security puzzle; but in most cases, the ability of an attacker to access the signaling channel will yield information about a call that is almost as valuable as the data content. This is not new: Forty years ago, phreakers whistled, yelled, or red-boxed

(used devices to produce telco signaling sounds) into telephones and compromised the signaling channel in order to make free phone calls. Today, analyses of a signal channel, for example, could allow an attacker to gather information regarding the duration, endpoints, and other parameters of incoming and outgoing calls.

The term *phreaker* (coined from a combination of the words *phone* and *freak)* refers to an individual who attempts to exploit telephone systems by committing telephone fraud. Back in the '70s, the most famous phreaker, John Draper, used a whistle that came in a box of Captain Crunch cereal that caused AT&T long-distance trunks to reset and prepare to route new calls.

In multi-office deployments, using VPN-based encryption ensures that any traffic that goes over the public infrastructure is secure.

No amount of encryption can protect against a single bad password, naïve system administrators, or poor protocol implementations.

Issues to consider

Note that implementing some security measures such as firewalls can degrade VoIP quality. These complications range from interruption or prevention of call setup by firewalls to encryption-produced latency and delay variation (jitter). But, not implementing security measures can degrade VoIP quality by making it vulnerable to attack or failure.

As a market leader, Avaya Global Services has experience building secure, reliable VoIP networks. In addition, Avaya's security partners, Juniper Networks and Extreme Networks, offer hardware- and software-based products that provide superior security while ensuring no impact to VoIP quality or performance.

Avaya Global Services Security Assessments

When San Francisco International Airport standardized on an Avaya voice infrastructure several years ago, the airport also engaged Avaya Global Services to help with all aspects of network support.

SFO asked Avaya to conduct an assessment that would directly address the operational integrity of the airport's voice communications network.

The Avaya System Security Assessment zeroed in on SFO's central voice server and voice messaging system to help ensure that all possible measures had been taken to secure the voice network from external intrusion. They wanted to make sure that no one could get in and compromise the operation of the voice network, access proprietary system information, or commit toll fraud.

The security assessment was very methodical. Avaya looked at every possible point of entry into the voice network and assessed whether appropriate controls were in place. They truly left no stone unturned.

The System Security Report was extremely thorough and highly specific. The assessment had extremely high business value and completely met all of SFO's expectations. Avaya definitely had the right skills and experience for the job.

According to John Payne, Chief Information Officer of San Francisco International Airport, "The Avaya Business Continuity and System Security Assessments gave us exactly what we were looking for — a clear blueprint that would allow us to prioritize our investments while taking the airport's emergency preparedness and security to a whole new level."

The result? Security was improved when assessments were conducted that directly addressed the operational integrity and emergency readiness of the airport's voice communications network.

Part III

Designing and Building Security into Your VoIP Network

In This Part

- Looking at the security built into Avaya's server and gateway products
- Examining Avaya's product solutions
- Taking a look at Avaya Global Services
- Understanding how Avaya works with its strategic partners

Avaya offers a rich set of products and services that cover virtually every need a small or large customer may require. Avaya product solutions cover the full range of voice, data, and converged network offerings from one-person branch offices to enterprises with tens of thousands of stations. To complement this array of products, Avaya offers professional services, maintenance, and managed services for any size business or project.

Security is at the forefront of Avaya solutions. Not merely providing functionality, every product delivers its services securely, and every service engagement considers security non-negotiable. You demand it, and Avaya delivers it.

A simple litmus test determines whether a specific security solution is used:

- Does it provide the most effective protection?
- Is it transparent to end users?

- Does it require extensive management?
- Does it degrade network performance?
- Does it include security functionality compatible with today's and possibly tomorrow's standards?

Avaya doesn't simply drop the latest and greatest security mechanisms into its products because they're cool; instead, the company performs an extensive risk analysis.

Avaya Builds Security into Its Servers and Gateways

Security is not added on but is designed into Avaya products. The methods that Avaya uses to secure its products are described in the sections that follow.

Secure operating system

Avaya's newest servers and gateways are built on the open Linux operating system. Linux has an advantage over other operating systems because its source code can be (and is) reviewed by thousands of security experts and researchers throughout the world.

Avaya made the move to Linux because of a security paradox: To make an operating system secure, you must reveal its innermost secrets. When the operating system software is publicly available and used in varying environments and for a wide range of applications, there are many 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 surety that flaws can and will be fixed quickly outweighs the weakness created by exposing them.

Media and signaling encryption

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. You can achieve protection by encrypting the entire link, 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.

Hardened operating system

Avaya servers and gateways built on Linux have 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, and so on. Attacks are recognized at the lower levels of the software and their effect blunted.

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.

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. By closing unused ports, worms that attempt to exploit weaknesses associated with those ports are blocked.

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 encrypts the entire session, including the login sequence as well as subsequent data transfer. SSL/HTTPS provides 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. Using anonymous FTP like this avoids the problem of sending passwords in clear text. However, SCP is the preferred method of transferring files.

One-time passwords

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 that 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 the account is permitted to have shell access. Accounts that 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, only individuals that perform hardware or software maintenance of the server need shell access.

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 that 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

You can access Avaya Media Servers remotely in one of two ways, either via a modem connection or via a network connection. Either method, and remote access in general, can cause security problems. 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 can also present a challenge 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 modem-based remote access and Virtual Private Network (VPN) based access are supported. Avaya considers VPN a more secure remote-access mechanism; however, modem access is often a necessary alternative in the event of a network failure that prevents VPN access from functioning.

Understanding the issues with modem access, Avaya has configured this feature with maximum flexibility for the system user. The server logins that are used to establish a remote modem connection are separate from those that allow administrative functions. One account is used to establish a connection; after the link is established, a second login is required using a separate administrative account. Modem configuration could also be disabled or configured for one-time-only use where the modem will be disabled automatically after it is used. This assures that the administrator doesn't forget to turn it off.

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. Critical 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 that 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 if the system owner is not careful.

Avaya Media Servers have the capability 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.

From time to time, new software features are created that require the software or firmware to 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.

LAN isolation

The enterprise LAN, control LANs, and adjunct LANs can all be connected together to form one network, or they can be kept physically or logically separate for either bandwidth control or security reasons. Separation can be physical or accomplished logically through VLANs.

In order to provide the most secure environment possible for the system, network access can be divided into separate zones of control.

VLANs can be configured to isolate traffic and access according to function. One VLAN can be configured for administrative traffic, one for call signaling, another for voice bearer traffic, and so on. Layer 3 boundary devices (routers, layer 3 switches, and firewalls) can be administered to enforce the

corporate security policy on traffic destined for the Avaya Media Servers, Media Gateways, or adjuncts. Firewalls can 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, 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 communications systems can be configured for maximum survivability should the network become fragmented or parts of the system become inoperable, including the main servers.

There are two types of survivable servers: Enterprise Survivable Servers (ESS) and Local Survivable Processors (LSP). These servers can be located in multiple physical locations and can 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.

Protection against malware

The viruses and worms that have made the headlines have mostly targeted Microsoft Windows operating systems and 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 disk drives. The Avaya Media Server does not support incoming e-mail, forwarding of e-mail, user Web browsing, or NFS or SMB (that is, 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 features being available (such as 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 server incorporates additional anti-tampering features. The disk drive is divided into multiple partitions. Executable code is stored in separate partitions from data; data is 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 using a one-time password.

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. Critical files and the file system are monitored by Tripwire, a software product that maintains a cryptographically encoded signature of the files on the system and generates alarms in the event any unexpected changes occur.

Testing

During development, Avaya subjects systems to a variety of common "attack tools" as additional validation steps aimed at reducing the likelihood of known vulnerabilities being reintroduced. The exact set of tools that 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.

Avaya Product Solutions

Avaya has a wide range of product solutions that support VoIP and converged infrastructure networks: from Media Servers to Media Gateways to secure gateways to IP infrastructure devices, including switches and routers.

Media Servers and Gateways

A Media Gateway is a communications system that, when placed in a branch office, provides advanced voice and data communications features that are logically extended from other branch locations and from a headquarters facility.

Avaya Media Gateways protect your network by blocking unauthorized communications and by permitting only authorized personnel to access and administer them.

Switches and WAN access devices

Avaya network switches and access devices deliver advanced support for converged infrastructures. Devices in this family include Ethernet stackable switches, ATM switches, workgroup switches, gigabit switches, and routers. These devices protect your network by withstanding attacks and tampering, and can be tied in to enterprise-wide Avaya network management systems.

Avaya's PXXX line of switches provides Layer 2 functionality. Extreme Networks, one of Avaya's strategic partners, has Layer 3 switches that are vital to core network operations.

Intelligent system and network management

Avaya offers tool suites to manage VoIP and converged infrastructure networks. These fall into six product groups described here. These products help to improve enterprise security by providing the tools to maintain the security and integrity of the entire network, as well as individual devices in the network:

- **Basic Administration Tools.** These tools are used to administer and manage fault and performance for a network of voice systems. They enable enterprises to manage adds, changes, backups, and broadcasts of recorded announcements over the LAN to Avaya Media Servers systems with Avaya Voice Announcement Manager.
- **Communication Manager System Management.** The ideal complement to the capabilities of both the Basic Administration Tools and Enterprise Integrated Management Offers, this is designed for enterprises that are implementing IP telephony and require management of centralized media servers with distributed media gateways.
- **Converged Network Analyzer.** This amazing tool creates a self-healing and self-optimizing WAN network infrastructure through a comprehensive approach to network monitoring, application-based assessment, and network optimization.
- **Enterprise Network Management.** For enterprises with mid- to large-scale branch-office VoIP deployments, Enterprise Management includes the essential tools needed to centrally manage provisioning and installation, secure access, software upgrades, and trouble shooting for branch-office locations.
- **Voice over IP Monitoring.** With VoIP Monitoring Manager, voice quality problems are identified faster, affected users and areas are identified quickly, and key information is available to help troubleshoot and fix problems.
- **VPNmanager Series.** These tools centralize deployment and management of widely distributed networks of remote access VPN users, VPN gateways, and firewalls in two editions: Enterprise Client and Service Provider Client.

Avaya Global Services Solutions

Avaya Global Services provides an array of professional product support and managed services for organizations that lack adequate resources or expertise to design, implement, or

maintain security in a VoIP environment. Avaya also provides complete services support for Juniper and Extreme security solutions.

Security consulting

Avaya provides several security consulting services. The most popular services include the following:

- **VoIP Security Assessment.** Identifies network and policy gaps that can be exploited by an attacker and provides the expertise needed to close these gaps.
- **Security Policy Development.** Defines procedures, responsibilities, controls, and security measures required to protect assets in a converged environment.
- **Security Architecture & Design.** Designs a secure information infrastructure and ensures that the security measures defined in a policy are designed into the security framework.
- **Business Continuity Consulting.** Provides the analysis, planning, and procedures necessary to ensure network availability during a disaster. These services include risk evaluation, risk reduction, and ongoing support that help businesses identify vulnerabilities and lower risks.

Communications system security

An important step in securing a converged communications network is securing, or hardening, of the applications. Avaya delivers the expertise needed to assist customers with the assurance that all possible measures have been taken to secure their Avaya systems and applications. This helps to minimize the threats that can compromise information and system integrity. Avaya can help determine and develop security controls for internal IT security audits to help achieve legislative or industry regulatory requirements. Security hardening solutions include the following:

- **System Access Controls:** These include password management, account management, user/group access level, file permissions and administration.

- **Application Controls:** These are recommended security controls that are available at the application layer.
- **Operating System:** Avaya helps mitigate vulnerabilities and apply appropriate security configuration and/or apply operating system–specific security patches.
- **Network Services:** Network services that may potentially pose security risks to a system resource are disabled.

Secure access and control

Another important consideration for maintaining security in a converged environment is securing access to the network and network-based applications for maintenance and repair purposes. Traditionally, modem connections were used to obtain access, but they have increasingly been viewed as potentially vulnerable to security breaches.

Avaya has addressed remote modem access vulnerability through its Secure Access and Control (SAC) solution. SAC is a software-based service that connects to your network via a secure VPN, thus eliminating reliance on modems and the public switched telephone network (PSTN). This ensures a secure path between Avaya and your site. SAC provides greater control over access and a more detailed audit trail. This solution delivers real-time management and control over remote access to your network and includes authentication (who gets in), authorization (what they can access), and accounting (audit trail — who, what, where, when and why).

Secure network monitoring and management services

Avaya's IP Support Services provide secure, real-time monitoring and management of your converged network infrastructure — supporting Avaya Communication Manager solutions and multi-vendor data devices. These services are built on the Avaya Enterprise Service Platform (ESP), which leverages the Avaya EXPERT Systems Diagnostic Tools — all working to identify, isolate, and remediate network issues within the shared accountability model.

Securing the Bank of Ireland

As a banking institution, the ability to conduct business is completely dependent on the reliability and security of the bank's communications technology. The Bank of Ireland's competitive reputation in the market is absolutely tied to its ability to safeguard a customer's financial and personal information assets.

The bank's Retail Financial Services division launched *Banking 365,* which broke ground as Ireland's first telephone banking offer. Providing around–the-clock personal banking every day of the year, 365 has expanded rapidly since its launch. Given the bank's focus on ensuring the integrity of the 365 network, it's not surprising that security was a prominent consideration in all aspects of the project. Avaya performed a major upgrade to Banking 365's voice network. Avaya Global Services designed and implemented appropriate measures to ensure Banking 365's security needs were met, beginning with a detailed risk analysis and using the results to develop a specific set of recommendations to fortify Banking 365's voice hardware and software. Collaborating with Bank of Ireland's information security team, voice and data services security were coordinated every step of the way to ensure consistency and reliability. Avaya's engineers employed a thorough methodology that focused on every area of network security, from administrative passwords to TCP protocols and LDAP functionality. The end result was a significantly heightened level of voice security when the bank's security team conducted a follow-up security assessment.

Here are the results:

Improved security through a detailed analysis of the bank's security audit and specific recommendations, which were implemented to fortify 365's voice hardware and software.

Enhanced customer trust by providing a highly secure way for Bank of Ireland's customers to manage their financial transactions.

Realized key business objectives such as retention, growth, and profitability.

Another key component of the Avaya service delivery architecture is the Secure Intelligent Gateway (SIG). The SIG provides visibility into the network components that are being monitored and managed in the converged environment. The SIG is set up between firewalls and transmits only the forensic analysis data back to the Avaya Network Operations Center — all in an effort to optimize the security of your confidential data. The Avaya Enterprise Service Platform, along with

Avaya's expert engineers, can help to significantly reduce the critical time associated with fault isolation in order to optimize network availability and quality of service.

Avaya's Strategic Partners

Avaya is building an ecosystem requiring the integration and collaboration of information and processes from thousands of developers, system integrators, customers, business partners, and more. In this system, each segment affects, and is affected by, the others. All the members of the ecosystem determine the fortune of the ecosystem as a whole.

Avaya has formed an alliance with strategic partners to ensure that all facets of the VoIP security spectrum are covered for your business.

Extreme Networks

Extreme Networks is an Avaya global strategic alliance partner as well as a DevConnect member. Extreme Networks provides the following cost-effective IP infrastructure product solutions:

- **Ethernet switches:** In the IP telephony world, Ethernet switches provide the switching and routing of VoIP calls as well as other applications on the network.
- **Wireless LAN:** Including VoIP roaming on wireless.
- **Security solutions:** Comprehensive LAN security on switches and the Sentriant security appliance which mitigates Day Zero attacks and worm storms.

Avaya's Developer*Connection* (DevConnect) is a community of companies that offers applications, services, and hardware solutions that further enhance Avaya's products and services.

Extreme Networks provides excellent VoIP performance in four key areas:

- High-quality voice connections
- Voice class availability
- Comprehensive security
- Simplified management

Juniper Networks

Juniper Networks is a global strategic alliance partner as well as an Avaya DevConnect member. Its portfolio includes industry leading security and network infrastructure. Juniper's products enable enterprises to run mission-critical applications such as VoIP and video on a single converged network.

Juniper Networks leads the industry in enabling secure, assured communications over a single IP network.

Juniper Networks provides superior VoIP support through:

- Best-in-class enterprise security products
- Superior performance through purpose-built high-performance platforms
- High availability and reliability of network infrastructure

In particular, Juniper Networks infrastructure products provide seamless interoperability and several unique attributes including:

- **Custom application-layer gateway (ALG):** Juniper Networks' support for Avaya H.323 ALG enhances network security because it is able to work with the Avaya H.323 protocol to open pinholes for incoming and outgoing calls rather than opening a range of static ports to handle VoIP traffic.
- **Protection against Session Initiation Protocol (SIP) anomalies:** Juniper Networks' Intrusion Detection and Prevention (IDP) systems protect against known SIP anomalies to provide additional security for Avaya IP telephony applications.
- **Customized WAN Optimization:** Juniper Networks' WAN acceleration products work specifically with Avaya IP telephony applications to provide additional bandwidth without incurring additional cost.
- **Support for Avaya IP Softphone and IP Agent:** Juniper Networks' secure sockets layer (SSL) VPN products have been tested with Avaya IP Softphone and IP Agent to ensure secure and reliable access for authorized remote users.

Part IV

Ten Reasons to Look to Avaya for VoIP Security

In This Part

- A complete solution
- Security consulting
- Trusted Communications Framework
- Secure products
- Partnerships
- Application security
- Managed security
- SIP security
- Secure access
- Credentials

Avaya is the leading solutions provider in the enterprise VoIP industry and has invested heavily in developing security strategies for its customers. The result is a reliable and secure VoIP solution. Here are the ten best reasons to look to Avaya for secure VoIP solutions.

Avaya Has the Complete Solution

Avaya sees the big picture and can deliver the total solution when it comes to VoIP security. What does that mean?

To begin with, Avaya considers the entire converged environment when it comes to VoIP security — this means the network and all applications. VoIP requires not only traditional, reactive data security, it also requires complete security of every link, user, server, and device. And security must be designed in from the beginning. By looking at an entire multi-vendor environment, Avaya creates a comprehensive plan of action to minimize risk for voice and data, as well as to comply with complex security and privacy regulations.

Another critical point is that Avaya has been a voice company since inception. Why is that important? Because voice is the most real-time of real-time mediums out there, demanding the highest standards of performance. Who better to trust for the security of voice over IP than the voice and application experts at Avaya?

Security Consulting

Effective security for VoIP starts with proper planning, including the development, implementation, and communication of security policies tailored to specific business priorities. Avaya brings the combination of skills and expertise required for planning and policy setting in converged communications environments — skills that have not coexisted in the past.

Avaya starts with a vulnerability assessment to identify network and policy gaps that an attacker can exploit. Avaya then provides security policy development consulting that helps the IT organization to define the procedures, responsibilities, controls, and security measures required to protect assets in a converged environment. Avaya brings its expertise to the complex task of designing a secure information infrastructure and ensures that the security measures defined in a policy are designed into the security framework.

Secure Products

Avaya products are secure by design and default. Avaya stays abreast of security best practices and issues and

incorporates best-of-breed protection measures into its products.

Security functionality incorporated into Avaya products includes

- SSH for secure administration instead of using older telnet and FTP protocols that send password credentials in the clear
- SNMPv3 for secure monitoring
- AES encryption to ensure voice confidentiality and signaling protection
- Standards-based registration via H.235.5 for secure authentication to avoid impersonation
- Virus protection by minimizing operating and network services that can be exploited by harmful worms and viruses

These measures keep your VoIP network secure without sacrificing performance or manageability.

SIP Security and Leadership

Avaya is a *thought leader* with the SIP protocol and its security; Avaya has long known SIP's potential and has incorporated it into many of its products already.

In converged networks, particularly in the case of SIP, more intelligence is moved away from the guarded center to the edge of the network. Avaya provides the fundamental security services required for the SIP protocol to address critical areas such as preserving the confidentiality and integrity of messaging, preventing replay attacks or message spoofing, providing for the authentication and privacy of the participants in a session, and preventing Denial-of-Service attacks.

Secure Access

Secure access means many things to many people. Avaya has secure access covered on all fronts:

- **Avaya Media Servers:** Support secure access for users as well as for administrators, whether personnel are located on-site or off-site. Products support Secure Shell (SSH), Secure Copy (SCP/SFTP), and secure Web access (using SSL or HTTPS). Unsecure services, such as telnet and FTP, are disabled.
- **Avaya Secure Access and Control Service (SAC):** Provides a secure path between Avaya and its customer sites and supports remote delivery of services — either by Avaya personnel or its patented remote diagnostics tool, Avaya EXPERT Systems.
- **Access Security Guard (ASG):** Provides protection for administrative accounts through challenge/response handshakes and one-time passwords.

To maintain security in a converged business communications environment, you must eliminate unauthorized external access to the network and network-based applications. These external communication connections are designed to facilitate maintenance and repair operations, but increasingly they are viewed as potential security vulnerability gaps in the enterprise communications environment. Avaya can help you address these potential security concerns.

Trusted Communications Framework

A *communication framework* is a fancy term for a set of standards that an organization uses for communication.

Avaya has developed a Trusted Communications Framework based on open standards. This approach provides security for communication and helps avoid being locked into a single vendor's proprietary architecture and solutions.

Avaya's Trusted Communications Framework is based on security best practices including defense in depth, high availability, and least privilege. Security is always a part of the design, from the very beginning of every new product.

Partnerships

Avaya has long known that no single company has the best of everything in communications security — or in other technologies, for that matter. Recognizing that, Avaya has formed numerous strategic partnerships in the VoIP market space, including Extreme Networks and Juniper Networks.

Avaya's partnership with Extreme Networks leverages Avaya's voice expertise in converged environments with Extreme Networks' expertise in high-performance, resilient Ethernet networks to collaborate in technology and product development.

Avaya's partnership with Juniper Networks uses Juniper's routing and security solutions, resulting in seamless, continuous, and secure communications delivered through any device to workers in any branch, remote, or mobile location.

Managed Services

After your shiny new converged network is built, who is going to operate it? Ongoing security management is a serious task that is a bigger job than many organizations want to take on alone.

Avaya Support Services provide the experienced resources needed to effectively monitor and manage a complex converged network communications platform. These services leverage the Avaya exclusive Enterprise Service Platform (ESP) and EXPERT Systems technology to proactively identify, isolate, and resolve potential network issues. Using the ESP, Avaya can help to significantly reduce the critical time and cost of fault isolation and ensure less downtime for communications equipment.

The Secure Intelligent Gateway (SIG), another key component of the Avaya service-delivery architecture, provides a secure access point and visibility for all network components being monitored and managed in your converged environment. The SIG receives events from devices in the network for continuous, real-time analysis while also providing other functionality

critical to the management of the environment. This level of intelligent monitoring greatly increases the probability of detection before problems affect service, thus increasing network uptime.

Application Security

Avaya understands that protecting VoIP doesn't stop with protecting the network. Certainly every device on the network must be secure, but don't forget about securing applications as well.

It used to be true to say that protecting the network was enough to protect the applications within it. But those good ol' days (or were those bad old days?) are over. The protection of applications in their own right is a vital part of the total solution.

Like servers and network devices, applications require their own hardening. Avaya applications have security features, including hardening, enabled by default. The following are some noteworthy examples:

- Avaya Communication Manager and Media Servers have additional resilience included in the form of protection against Denial of Service (DoS) attacks.
- Avaya S8700/S8300 Media Servers also support many security monitoring and alarming features.
- Avaya S8700 and S8300 servers can store backup copies of critical configuration information, including authentication and account information, on external systems.
- The S8700 and S8300 servers can encrypt all backup data, thus making use of the data impossible, even if access to the data is compromised.
- For other PBX systems and adjunct systems (call management, messaging IVR, and so on), Avaya provides the expertise to assure that all possible measures have been taken to secure them, while providing the proof points necessary for industry and government regulation complaince.

Avaya has the specific system knowledge, security expertise, and industry experience to deliver system security hardening of Avaya communications systems and other vendor systems that address the level of security required by organizations.

Avaya Credentials

From its security consultants to the R&D staff at Avaya Labs Research, Avaya's level of expertise is unparalleled. Avaya security consultants have an average of 10–15 years of security experience in many industries.

Many Avaya consultants also possess industry-recognized certifications including

- Certified Information Systems Security Professional (CISSP)
- National Security Agency INFOSEC Assessment Methodologies (IAM)
- Checkpoint Certified Security Associate (CCSA)
- Cisco Certified Firewall Specialist (CCFS)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Design Professional (CCDP)
- Cisco Certified Design Associate (CCDA)
- Alteon Certified Expert (ACE)
- Microsoft Certified Systems Engineer (MCSE+I)

WE'RE AT THE HEART OF OVER A MILLION COMPANIES WORLDWIDE.

IS YOURS NEXT?

Avaya is the world leader in IP Telephony, Mobility Solutions and Contact Centers.

But really, we're revolutionaries at heart.

Avaya not only delivers the reliability and robustness of voice—we embed it right at the heart of business.

Let us assess your network for VoIP readiness. Let us show you how embedded communications can transform your business.

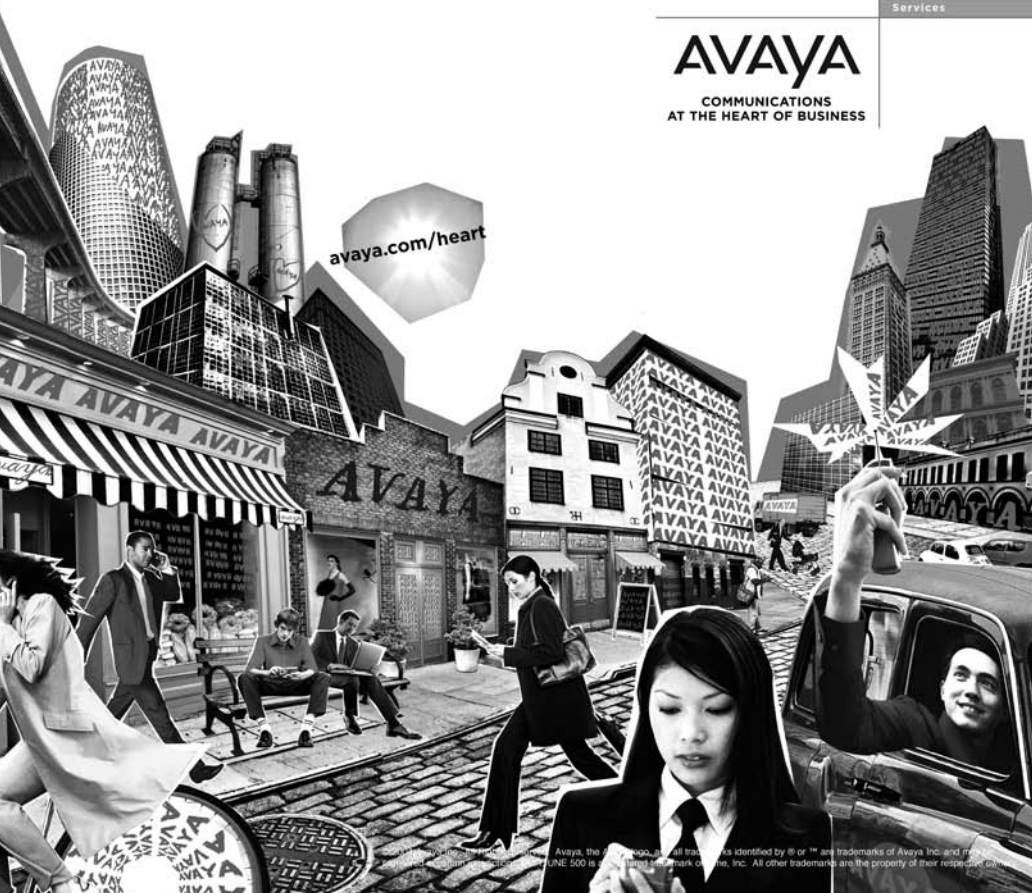
Go to avaya.com/heart for more possibilities.

Some may actually quicken your pulse.

IP Telephony
Contact Centers
Mobility
Services

AVAYA

COMMUNICATIONS
AT THE HEART OF BUSINESS



Enjoy all the benefits of VoIP with enterprise-grade security

Protect your converged networks from known and unknown risks!

This Avaya limited edition of *VoIP Security For Dummies* shows how risks are identified, analyzed, managed, and minimized in your converged voice and data networks. Find out how security best practices — and Avaya products and services — can make your VoIP network as secure as a traditional telephone network. IT managers will appreciate the jargon-free coverage of VoIP and converged network security, and end users will easily understand the benefits of securing VoIP. See how an Avaya solution can help you implement VoIP without sacrificing the security and stability you are accustomed to.

Discover how to:

- ***Understand VoIP security issues and how they are solved***
- ***Make decisions about how to better secure your converged network and applications***
- ***Improve security in your entire converged environment***

THE DUMMIES WAY®

- ***Explanations in plain English***
- ***"Get in, get out" information***
- ***Icons and other navigational aids***
- ***Top ten lists***
- ***A dash of humor and fun***

Get smart! @www.dummies.com

- ***Find listings of all our books***
- ***Choose from many different subject categories***
- ***Sign up for eTips at etips.dummies.com***

ISBN: 0-470-00987-X
Part #: MIS3005
Not for resale

For Dummies®
A Branded Imprint of
WILEY