# Voice Security Primer: Protecting the Voice Infrastructure, Call-Management System, Applications, and Endpoints

Security ranks high as a selection criterion for voice systems. Whether a company deploys a traditional time-division multiplexing (TDM)-based PBX or an IP telephony system, IT personnel and voice administrators need to take appropriate measures to prevent threats such as toll fraud and eavesdropping. Cisco® Unified Communications systems can be as secure - or even more secure - than traditional PBX systems. Voice traffic travels over the same IP network that companies use for data traffic, and so a company that has deployed a secure network infrastructure has already made much of the investment it needs to protect its voice system, as well. In independent tests by Miercom, Cisco IP telephony solutions are rated the most secure in the industry.1

## Executive Summary

Companies of all sizes are adopting unified communications to boost productivity, increase mobility, and enhance flexibility in terms of telephony capabilities. Before adopting unified communications, however, companies want to take precautions to secure their call-management system, applications, and endpoints, as well as the underlying IP network infrastructure.

Security has been a perpetual concern for voice systems since the days of party lines, when eavesdropping was a constant threat. In fact, hacking got its start with voice systems in the 1970s, when individuals used devices to simulate call-control signaling and make free phone calls. Today, the most common attacks on TDM phone systems, as well as IP telephony systems, are denial-of-service (DoS) attacks, toll fraud, and eavesdropping.

The good news is that IP telephony is essentially just another service running on a network, and all of the security technologies and policies that companies have deployed for their data networks can protect voice services, as well. This differentiates IP telephony and unified communications from traditional telephone systems, which often lack general-purpose, cost-effective security measures that can be easily adapted as business conditions change.

Security is among the most important differentiators of Cisco IP telephony solutions. Independent tests by Miercom rate Cisco voice security as the best in the industry. To date, Cisco Systems® is the only IP telephony vendor to earn Miercom's highest rating of "Secure" for its proven ability to defend an IP telephony service against malicious attacks.2 An expert team of hackers, assembled and supervised by Miercom, could not disrupt, or even disturb, phone service or features after three days of continual, sophisticated attacks.

Unlike vendors whose security offerings protect individual devices in the voice system, Cisco provides comprehensive, integrated security that protects the entire network over which voice traffic travels. Multiple layers of defense - for the infrastructure, call management, applications, and endpoints - protect against known threats, as well as constantly emerging unknown threats.

This white paper, intended for IT personnel and voice system managers in midsize companies, provides an overview of today's voice security requirements and solutions. It begins by summarizing the types of voice security risks, many of which apply to both TDM and IP telephony

systems. Next it explains how Cisco security solutions protect the voice infrastructure, call management system, applications, and endpoints. The paper concludes with Cisco Websites that provide more in-depth information on different components of the multilayered Cisco voice security solution. Companies interested in implementing the network security solutions described in this paper have the option to outsource the project to Cisco or a Cisco partner, both of whom will follow the steps in the Cisco Smart Business Roadmap.

## Types of Voice Threats

### Toll Fraud

Toll fraud refers to internal or external users using the corporate phone system to place unauthorized toll calls. Toll fraud can occur with both TDM and IP-based voice systems.

### Denial of Service

In a DoS attack, hackers use automated tools to send a deluge of nuisance traffic to IP phones, call-processing servers, or infrastructure elements. The goal is to exhaust network resources so that calls are interrupted or cannot be processed. A common motive is to distract the IT group for the purpose of executing other attacks.

### Impersonation or "Spoofing"

In impersonation exploits, a hacker steals a legitimate user's identity so that the hacker's phone calls appear to come from another user. For example, someone might pose as an employee of the IT group and call a company executive to ask for a password. If a legitimate-seeming phone number appears as the caller ID, which is easy to accomplish with either TDM or IP telephony systems, the victim might be fooled. Hackers can either spoof an IP address or the Dynamic Host Configuration Protocol (DHCP) server, which distributes IP addresses.

### Eavesdropping, or Man-in-the-Middle Exploits

In man-in-the-middle attacks, an internal user spoofs the IP address of a router or PC to spy on voice traffic as well as data entered on the phone keypad during a voice conversation, such as passwords. After quickly copying the information, the user forwards the voice traffic to the intended destination so that neither the sender nor the recipient knows that the conversation was intercepted. Typical motives include espionage or harassment. Eavesdropping has become easier because of widely available packet-sniffing tools. It is also relatively easy to prevent.

**Cisco Earns Highest Security Rating**

In independent testing conducted by Miercom, Cisco Systems proved that it could build and deploy a Cisco Unified Communications Manager-based, IP telephony network that a sophisticated hacker assault team could not break – or even noticeably disturb – even after days of continual assaults, including dozens of the most insidious DoS attacks. The assault team systematically attacked all layers: the Layer 2 infrastructure (MAC-level, switches, forwarding), the Layer 3 infrastructure (IP routing level), and then Layer 4 and above, targeting the voice-over-IP (VoIP) and IP telephony

## Infrastructure Security

The same proven Cisco integrated security solutions that protect data traffic can also be used to protect voice traffic (see sidebar). Organizations that have deployed a Cisco Self-Defending Network already have the foundation for a secure voice communications solution.

Following is a selection of Cisco secure infrastructure technologies that are especially useful for protecting voice systems.

**Virtual LAN**

Cisco VLAN technology, built into Cisco routers, Cisco Catalyst® switches, and Cisco Aironet® wireless access points, separate the physical network into multiple logical networks - for example, one each for a company's HR, sales, marketing, engineering, and finance organizations. A basic technique for voice security is to create a separate VLAN for voice. One advantage is that traffic sent over the voice VLAN is not visible to insiders or outsiders connected to data VLANs, and data traffic cannot cross over to the voice VLAN. Another advantage is that IT can assign a unique class of service for the voice VLAN to ensure that voice traffic receives priority over data traffic.

Following are some of the ways that VLANs protect the voice system from security threats:

- Preventing toll fraud - Companies can apply different access control policies to their voice VLAN; for example, authorizing employees on the manufacturing floor to access the data segment but not the voice segment. Establishing a separate voice VLAN also prevents employees from trying to use another department's VLAN for toll calls to avoid increasing their own phone bills.
- Preventing DoS attacks - Most DoS attacks are originated from a PC and, therefore, cannot affect IP phones and call-processing servers connected to a separate voice VLAN.
- Preventing eavesdropping and interception - Hackers typically eavesdrop on conversations using a PC with special software to connect to the same VLAN as one or more parties in the conversation. If voice participants are logically cordoned off, however, a hacker cannot connect to the voice VLAN with a PC.

**Voice and Video-Enabled VPN**

Preventing unauthorized access to the network is a smart first step in a voice security program. For an additional layer of protection, in case somebody does gain unauthorized access, organizations can also encrypt voice traffic. Voice and video-enabled VPN (V3PN) technology, available in many Cisco routers and security appliances, encrypts voice as well as data traffic using IP Security (IPsec) or Advanced Encryption Standard (AES). Encryption is performed in hardware so that firewall performance is not affected. Neither does a V3PN solution affect voice quality, because the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco firewall solutions provide quality of service (QoS) mechanisms that help ensure that voice packets receive priority over data packets as they travel through VPN tunnels.

Following are some of the ways that Cisco V3PN technology protects voice traffic:

- Preventing toll fraud - To perpetrate toll fraud, a hacker needs to obtain information about the telephony system and its legitimate users, such as the MAC and IP addresses of Cisco Unified IP phones and the Cisco Unified Communications Manager server. Encrypting this information as it travels across the network - especially after also logically separating it on its own VLAN and controlling access - makes it more difficult to obtain.

- Preventing eavesdropping and interception - Many companies use V3PN technology to encrypt voice traffic that will travel across the public Internet before arriving at its destination, such as voice traffic between the home office and branch offices. Cisco routers, firewall solutions, VPN concentrators, and adaptive security appliances also

encrypt data that users enter with their telephone keypads during voice conversations, such as passwords or credit card numbers requested by interactive voice response (IVR) systems.

**Access Control Lists**

Access control lists (ACLs), present in all Cisco network infrastructure devices, restrict access to a specific resource, such as a Cisco Unified Communications Manager server, to specified users or network segments. Companies can set up voice ACLs for departments, workgroups, or even for individuals.

ACLs protect voice security in the following ways:

- Preventing toll fraud - Companies can use ACLs to control which users can access the voice system, and from which locations. For example, a company might authorize only certain users to access the voice gateway to make long-distance or international calls, and even deny those users access from less trusted areas of the network. Denying access from building lobbies, for example, prevents an outsider from using a laptop with softphone software to make long-distance calls, or from using port-scanning software to find out the address of the call-processing server for later use. ACLs and VLANs together are an even more powerful combination for preventing toll fraud. Suppose an employee in one department wants to use Cisco IP Communicator on a laptop to impersonate an employee in another department, with the goal of reducing the first department's phone bill. VLAN technology prohibits the user from making voice calls from the other department's VLAN. For added security, the employee's own ACL can be set up to prevent his or her traffic from traversing from one department's VLAN to another.
- Preventing eavesdropping and interception - ACLs prevent voice traffic from crossing over to an untrusted portion of the network.
- Preventing DoS attacks - Companies can use ACLs to prevent inbound data packets, such as DoS attacks, from entering the voice VLAN. Separate ACLs are set up for inbound and outbound traffic, enabling companies that block inbound data packets on the voice VLAN to allow outbound data traffic onto the voice VLAN. This distinction makes it possible to deploy XML applications on Cisco Unified IP phones - for example, for logging in and out of shifts.

**Port Security**

Whereas Cisco firewall solutions provide access control for external users, port security provides access control for internal users. A built-in feature on Cisco routers and switches, port security limits the services that network users can access based on the physical port to which they connect, and helps protect the voice system in the following ways:

- Preventing toll fraud - The most basic step in preventing toll fraud is denying network access to unauthorized users. Port security enables organizations to restrict access to the voice network to particular ports. For example, a company might disallow access to the voice system from ports in locations where employees ordinarily do not use phones, such as custodial areas or the manufacturing floor. Another way that port security controls access is by directing a user into the appropriate VLAN based on the user's voice privileges. An unknown user, for example, might be directed to a guest VLAN with no or limited voice privileges, and also be subject to ACLs that prevent access to the voice system. A known user, in contrast, would be directed to the voice VLAN for that user's department.

- Preventing DoS attacks - The port does not turn on until it receives confirmation that both the user and device are trusted. This helps prevent an untrusted user from connecting to the network from a private location in the company, such as a basement or custodial closet, and launching a DoS attack. To protect against DoS attacks launched by employees' computers and laptops without their knowledge, companies can combine port security with Network Admission Control (NAC) to verify that the PC or laptop is protected with the latest versions of antivirus software and Cisco Security Agent.

- Preventing impersonation, spoofing, or eavesdropping - Port security can be used to limit the number of MAC addresses authorized to access the network through a given port. This eliminates the potential for someone to, for example, disconnect a legitimate IP phone, connect in its place a hub with two or more ports, and then connect an unauthorized IP phone or PC softphone to one of the hub ports to impersonate another user. The port rejects all MAC addresses other than the single known MAC address.

**Cisco Secure Access Control Server**

Cisco Secure Access Control Server (ACS) provides dynamic, user-based ACLs that specify the actions that individual users are allowed to take. The company can specify how the users are identified, usually by some combination of who the users are (name or ID number), what they have (token or dynamic key), and what they know (password). Say Jennifer works in HR and is authorized to use both data and voice services, whereas Jason works on the manufacturing floor and is authorized for data only. No matter where Jennifer goes in the building or campus, after she is authenticated, she can log on to the intranet or a Cisco Unified IP phone. Similarly, Jason is prevented from accessing the voice network even if he connects a laptop with softphone software to a VLAN belonging to a department where all employees have voice access.

Cisco Secure ACS protects the security of the voice system in the following ways:

- Preventing toll fraud - Cisco Secure ACS provides control over the actions that individual users are authorized to perform. The company can specify whether certain users can make local, national, or international calls; use a softphone such as Cisco IP Communicator; and have the same privileges from home or during travel that they have in the office.
- Preventing DoS attacks - Cisco Secure ACS works in conjunction with NAC, which checks the security posture of a PC or laptop before allowing it onto the network. If an employee brings home a laptop over the weekend, and it becomes infected or is recruited to execute DoS attacks, NAC detects the malware and denies access until the malware is removed.
- Preventing eavesdropping - By authenticating user identities, Cisco Secure ACS helps prevent users from impersonating others with the goal of eavesdropping.

**DHCP Snooping**

In one type of man-in-the-middle attack, a user impersonates the DHCP server in order to redirect all network traffic through a device under the user's control. The motive might be eavesdropping or executing a DoS attack. To prevent DHCP spoofing, companies can use the DHCP Snooping feature of Cisco Catalyst switches to define trusted ports that can send DHCP requests and acknowledgements, as well as untrusted ports that can only forward DHCP requests. If a malicious user attempts to send a DHCP acknowledgement packet into the network over an untrusted port, the request is not allowed, preventing the snooping attempt.

### Cisco Firewall Solutions

Cisco firewall solutions restrict the ports that outsiders can use to access the network using particular protocols. Access by outsiders is typically restricted to port 80 for HTTP traffic. Among the features of Cisco firewall solutions is "stateful inspection," or ensuring that no packets enter the LAN from the Internet unless they were explicitly requested or come from an address preconfigured for allowed access. This helps prevent unauthorized access to the voice network.

### Intrusion Prevention

Cisco intrusion prevention systems (IPSs) are available as standalone sensor appliances or as modules in the Cisco ASA 5500 Series and Cisco Catalyst 6500 Series, and complement Cisco firewall solutions to prevent misuse of port 80 to compromise the voice system or any other network assets. Whereas a firewall enforces policies that specify the protocols and applications allowed through a given port, an IPS inspects all traffic flowing through the network, regardless of whether it originated outside or inside the perimeter, to determine if it is malicious. The IT group can specify allowed behaviors for each application, such as Cisco Unified Communications Manager. Unlike an antivirus solution that looks for known signatures, Cisco IPS sensor appliances and modules look for any anomalous pattern, whether or not it has been seen previously. This enables the IPS to detect malicious traffic, even if it is part of a brand-new exploit. Companies can configure Cisco IPSs to automatically take action when a threat is detected, such as resetting a port or shutting down an interface.

### Wireless Security

When companies send voice traffic over their wireless LANs, they can protect the voice traffic with the same techniques used to protect wireless data traffic. That is, data in transit can be protected from eavesdropping using Cisco VPN technology, which supports Wi-Fi Protected Access (WPA) and WPA-2 encryption. Another option is to use Advanced Encryption Standard (AES), part of the 802.11i encryption capabilities in the Cisco Unified Wireless Network.

To authenticate voice users on the wireless network as part of NAC, companies can take advantage of the 802.1X authentication in the Cisco Unified Wireless Network to communicate with a centralized RADIUS server.

### Application Security

Cisco Unified Communications applications include Cisco Unified Communications Manager, Cisco Unity® Unified Messaging, and Cisco Unified MeetingPlace®. Following are techniques to protect the applications:

- Multilevel administration - Organizations can assign read-only privileges to most administrators, reserving read-write privileges for a few trusted individuals.
- Secure management - Administrators should be authenticated before managing the voice applications. Another security technique is to require administrators to log on to a physical interface other than the call-processing interface, not accessible to most people. In addition, the Cisco Unified Communications Manager management interface uses HTTPS, not HTTP, because it uses 128-bit encryption to protect management transactions sent from the user to the application from snooping or alteration.
- Hardened operating system - Cisco has hardened the Windows operating system on servers used for Cisco Unified Communications Manager, Cisco Unity, and Cisco Unified MeetingPlace applications. Examples of hardening include disabling default features and

services that are not needed for a dedicated call-processing server. Cisco also provides an aggressive security patch and hot-fix policy.

- H.323 and Session Initiation Protocol (SIP) signaling - These protocols include built-in features to prevent unauthorized or illegitimate call setup or teardown.
- Media encryption - Cisco Unity and Cisco Unified MeetingPlace voice recordings are encrypted to prevent theft of information.

## Call Management Security

### Cisco Security Agent

Installed on voice-application servers (Cisco Unified Communications Manager servers, Cisco Unity servers, Cisco Unified MeetingPlace servers, and others) as well as desktops, Cisco Security Agent is a host-based IPS. When a voice application attempts an operation, Cisco Security Agent checks the operation against a centrally defined security policy and then, based on policy, either allows or denies the behavior. Uniquely, Cisco Security Agent does not look for disallowed applications or signatures, but rather for disallowed behaviors, such as changing the status of an untrusted IP phone. The behavior-based approach makes it possible to detect and stop actions that have not been seen before, sometimes called "day-zero" threats. It also eliminates the need for time-consuming and costly signature updates.

Cisco Security Agent helps protect voice security in the following ways:

- Preventing toll fraud - Installing Cisco Security Agent on Cisco Unified Communications Manager servers prevents attackers from installing back doors in the software that they can use to reconfigure the server to trust an untrusted device. It also prevents known and unknown viruses and exploits from compromising the server.
- Preventing DoS attacks - Cisco Security Agent intercepts and drops inappropriate traffic directed to Cisco Unified Communications Manager, helping to ensure that its resources remain available for call processing. When installed on desktop PCs, Cisco Security Agent prevents the PC from installing programs without the PC user's knowledge, such as programs that perpetrate DoS attacks. Protecting desktop computers with Cisco Security Agent is an especially useful security measure in companies that allow routing between the voice and data VLANs. In this case, protected PCs cannot become unwitting agents in sending DoS traffic over the voice VLAN.

## Hardened Operating System

Cisco has hardened the Windows operating system on servers used for Cisco Unified Communications Manager, Cisco Unity, and Cisco Unified MeetingPlace applications. Examples of hardening include disabling default features and services not needed for a dedicated call-processing server. Cisco also provides an aggressive security patch and hot-fix policy.

### Endpoint Security

Following are a few of the Cisco security technologies for protecting Cisco Unified IP phones and other endpoints:

- Media authentication and encryption - Cisco routers encrypt calls from Cisco Unified IP phones to the TDM or analog gateway and between gateways using a feature called

Secure Real-Time Protocol (SRTP). This protects voice conversations or fax calls from eavesdropping.

- X.509 version 3 certificates - These certificates, present in Cisco Unified IP phones and Cisco Unified Communications Manager, provide assurance that the device is not counterfeit. By providing reliable device authentication, X.509 certificates help prevent fraud by people who attempt to connect their own devices to the network.

### Secure Management

Organizations with secure IP networks use management software for logging, alerts, and traffic monitoring. Organizations can further improve their security posture by protecting the management tools from manipulation by attackers. Otherwise, clever attackers who obtain access to the management tools can obscure assaults by first sending traffic that is clearly not allowed, invoking multiple log entries and alerts that can divert IT's attention from the real attack.

Following are some of the best practices companies can use for secure management:

- Hardened platforms - A hardened operating system helps ensure that only authorized people can access and change information pertaining to the voice system. Cisco ships a hardened Windows operating system by default.
- Cisco Security Agent - Companies that install Cisco Security Agent on desktops and servers can push out new security policies in response to changing security environments.
- Access control - Administrators can access the management interface only after being authenticated and authorized for the task.
- HTTPS - Cisco voice applications are managed using HTTPS instead of HTTP because HTTPS uses 128-bit encryption to protect management transactions sent from the user to the application from snooping or alteration.

### How to Begin

Creating a secure network infrastructure provides excellent return on investment (ROI) because a single investment protects voice as well as data. Cisco provides industry-leading security technologies that companies need to build a solid foundation for today's voice requirements as well as tomorrow's. To help companies implement network-based voice security, Cisco has developed the Cisco Smart Business Roadmap, which Cisco or its partners can implement.

Cisco Systems and its partners provide a broad portfolio of end-to-end services and support that can help you improve network total cost of ownership, business agility, and network availability to increase your network's business value and ROI when deploying a Cisco Unified Communications solution. Cisco advocates the Lifecycle Services approach which defines the minimum set of activities needed to help you successfully deploy and operate your Cisco Unified Communications solution and optimize its performance throughout the six phases of the network lifecycle:

- Prepare - Make sound financial decisions by developing a business case that establishes the financial justification for making a technology change
- Plan - Assess the existing environment to determine whether it can support the proposed system
- Design - Develop a comprehensive detailed design that meets business and technical requirements

- Implement - Integrate devices without disrupting the existing network or creating points of vulnerability
- Operate - Maintain network health through day-to-day operations
- Optimize - Achieve operational excellence through ongoing improvement of system performance and functionality

For more information on the Cisco Lifecycle Services approach, visit:
http://www.cisco.com/go/services

For more information on the Cisco Smart Business Roadmap, visit:

http://www.cisco.com/go/sbr

For more information on integrated network security for Cisco Unified Communications, visit:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html

For more information on Cisco Business Communications, visit:
http://www.cisco.com/go/businesscommunications

1Miercom, Independent Lab Test Report: Security of Cisco Unified Communications Manager-based IP Telephony Against Malicious Hacker Attacks, May 2004
2Miercom

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



Printed in USA C11-342145-02 03/07

 