



SECURING VOICE

IN AN IP ENVIRONMENT

DEFENSE-IN-DEPTH STRATEGIES FOR MAKING VOICE
AS SECURE AS ANY OTHER MISSION-CRITICAL APPLICATION



integrating voice services and systems with data IP networks has clearly won the hearts, minds, and wallets of enterprises. But as voice technologies meet the world of IP, many IT, telephony, and business managers are concerned about its safety from attack. Voice requires high security standards, equal to those of high-security data applications.

The information in voice calls—strategic, personal, or financial—can be just as proprietary or damaging if intercepted as that in data. Moreover, no enterprise or service provider can afford a denial-of-service (DoS) attack that shuts down voice communications. Not only is voice still the lifeblood of most businesses, users absolutely must be able to get through to emergency services.

BY JANET KREILING

SPENCER TOY

Many enterprises have implemented programs to ensure data security—which, of course, also protect voice traveling as data—based on Cisco SAFE guidelines. To focus specific attention on voice security, Cisco has further developed comprehensive SAFE guidelines for IP voice that build on those for data networks and focus on the same three areas: secure connectivity, managing trust and identity, and threat defense.

Secure connectivity encompasses not only the underlying data infrastructure that carries voice—there are specific provisions that augment safety for voice. The SAFE blueprints for IP networks carrying voice pay special attention to protecting the four main voice systems: the IP phone, the call-processing manager, the voice-mail system, and the voice gateway. Similarly, there are specific provisions within trust and identity management and threat defense for voice. For example, there are measures to segment and separate voice calls from data, to secure IP phones, to prevent infiltration of voice platforms by viruses that have penetrated the data network, and

to broker connections between the voice and data segments of the network. (In this article, the term “IP voice” includes both voice over IP or VoIP calls that may begin in analog form and are converted to digital for transit, and IP telephony—voice calls that travel in IP form from start to finish.)

Points out Roger Farnsworth, senior marketing manager and long-time security specialist at Cisco, “A broad and integrated approach is essential to securing both data and voice. While no security program is 100 percent foolproof, careful adherence to the SAFE guidelines will make your Cisco IP voice communications as safe as they can be. Cisco’s leadership and expertise in data security solutions make its solutions unique in their ability to protect IP telephony and voice over IP.”

Secure Connectivity

The first step should be developing a security policy for voice, paralleling the one that you should already have developed for data.

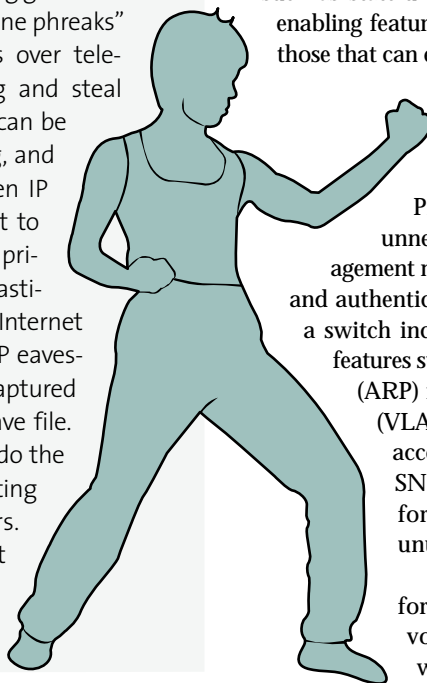
Only after this policy has been created should you give your attention to protecting IP voice. Jason Halpern, manager of technical marketing for security at Cisco, notes that many existing data security steps also protect this emerging technology, and should be implemented before addressing voice security specifically. First, says Halpern, “You need secure connectivity, which requires a secure underlying data network—that is, one hardened wherever possible at Layer 2 and Layer 3.” Among hardening measures, he says, are “increasing security on routers and switches by taking advantage of security features built into Cisco IOS® Software such as stateful firewalls and intrusion detection, enabling features that promote security, disabling those that can expose the network, and hardening device configurations.”

Hardening a router includes actions such as locking down Simple Network Management Protocol (SNMP) access, turning off unneeded services, using secure management methods such as Secure Shell (SSH), and authenticating routing updates. Hardening a switch includes Layer 2 hardening through features such as Address Resolution Protocol (ARP) inspection or private virtual LANs (VLANs), using IP permit lists to restrict access to management ports such as SNMP, using a dedicated VLAN ID for all trunk ports, and disabling unused ports.

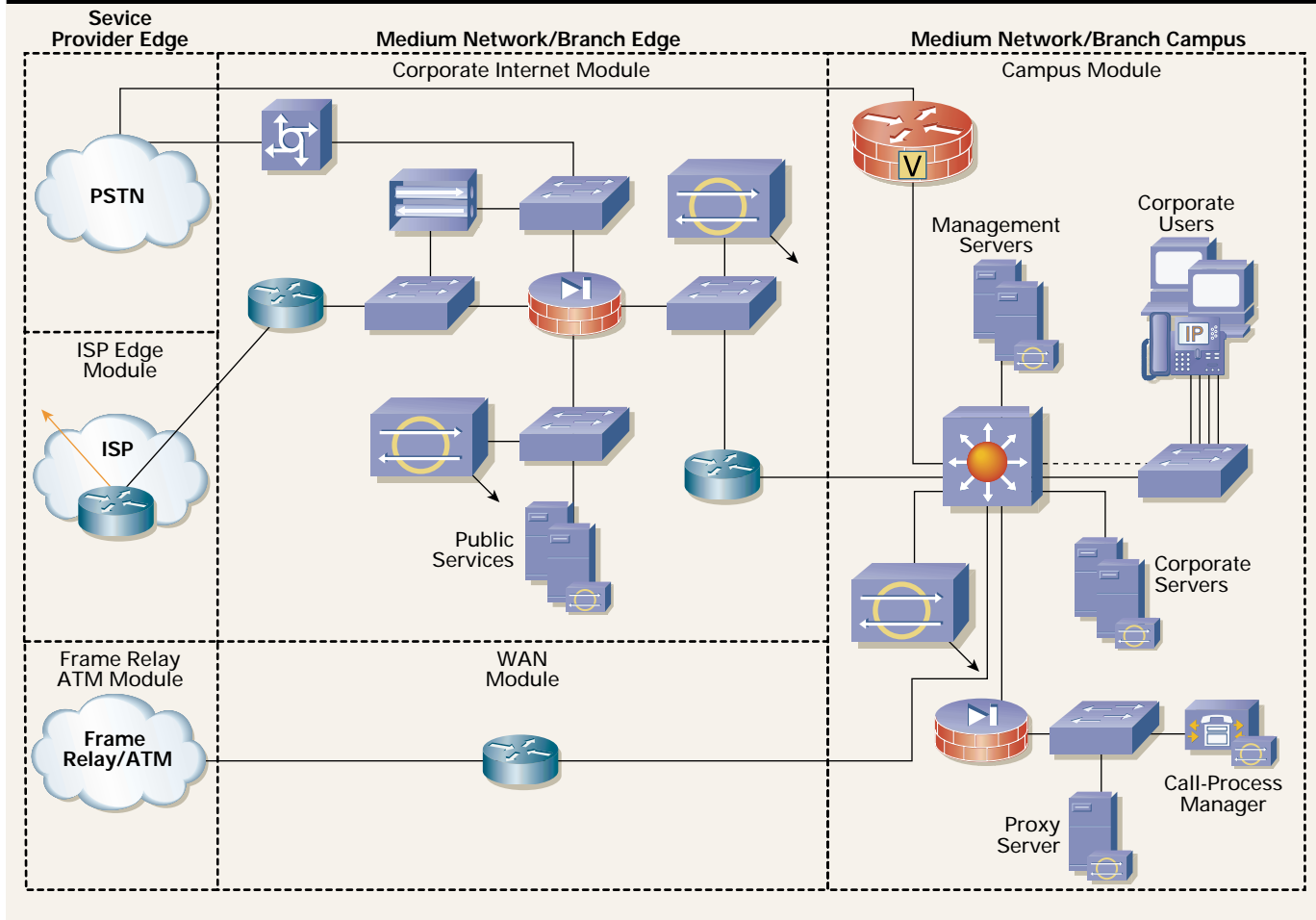
Similar hardening should be performed on call-processing managers, voice mail systems, and voice gateways. “It’s crucial that these appli-

THE THREATS

Many threats to IP voice are, like DoS, familiar from data communications: viruses, worms, Trojan horses, man-in-the-middle attacks, packet sniffing, IP spoofing, password attacks, trust exploitation, and the like. Then there are threats such as toll fraud explicitly directed at voice. Actually, attacks against voice calls and voice-related systems are not new. (In fact, hacking got its start in the exploitation of telephony systems as “phone phreaks” sent dual-tone multifrequency [DTMF] signals over telephone lines to simulate call control signaling and steal phone calls.) Traditional voice communications can be vulnerable to DoS attacks, fraud, eavesdropping, and other security breaches; these can also threaten IP voice. In an IP network, a hacker might attempt to get into a voice gateway for “free” calls. To violate privacy, he or she might employ a bit of software nastily acronymed VOMIT (voice over misconfigured Internet telephones), designed as a proof-of-concept VoIP eavesdropping tool, to reassemble an IP voice trace captured by the UNIX tool tcpdump into a listenable wave file. Many commercially supported diagnostic tools do the same thing more legitimately for troubleshooting voice quality and other service parameters. Application-layer attacks can specifically target call management, voice mail, and unified messaging systems.



SAFE BLUEPRINT FOR MEDIUM-SIZED ENTERPRISE NETWORK



cations are configured properly according to the vendor's best practices," Halpern adds—a step missed by administrators who assume the systems are shipped with all security aspects enabled. Given the diverse ways they are deployed, these systems must be tailored to each installation.

Hardening the network helps secure it against all the ills data can fall prey to—DoS, spoofing, packet sniffing, viruses, worms, and the like. The next step, segmenting network functions, helps make sure that even if an invader gets into the data network, it won't affect voice traffic, by providing more effective access control and successful attack mitigation. As a first step, the network should be segmented into function modules. A campus network, for example, might be segmented into a management module, building module (users), server module, lab module, building distribution, core, and edge distribution.

Once that's done, Halpern says, segment voice from data and segment voice users into coherent groups by grouping them into VLANs set up on your Ethernet LAN switches. Connections between the

voice and data segments of the network (which is still converged, as these are all logical, not physical, separations) should be limited to specific points, such as the call processing and voice mail systems.

"Segmentation is especially valuable in today's age where worms are becoming more prevalent," Halpern points out. "Sequestering data from voice renders it less likely that attacks in the data segment will affect the voice segment. For example, voice streaming occurs over the Real-Time Transfer Protocol [RTP], which uses a very large range of ports—anywhere from 16,384 to 32,768. Without proper filtering and segmentation, an attack could traverse from data into voice through one of them."

You will also want to turn off system features that can automatically allow would-be users onto the network or restricted segments. For example, many call-processing managers provide an automatic phone registration feature that bootstraps an unknown phone with a temporary configuration and then allows it onto the network. The danger is obvious: It's possible that that phone, or a device appearing to

FIGURE 1: SAFE divides the network into modules for security and manageability. It has been designed to support IP phones, PC-based IP phones, voice services, proxy services, PSTN for WAN backup and local calls, and VLANs for segmentation.

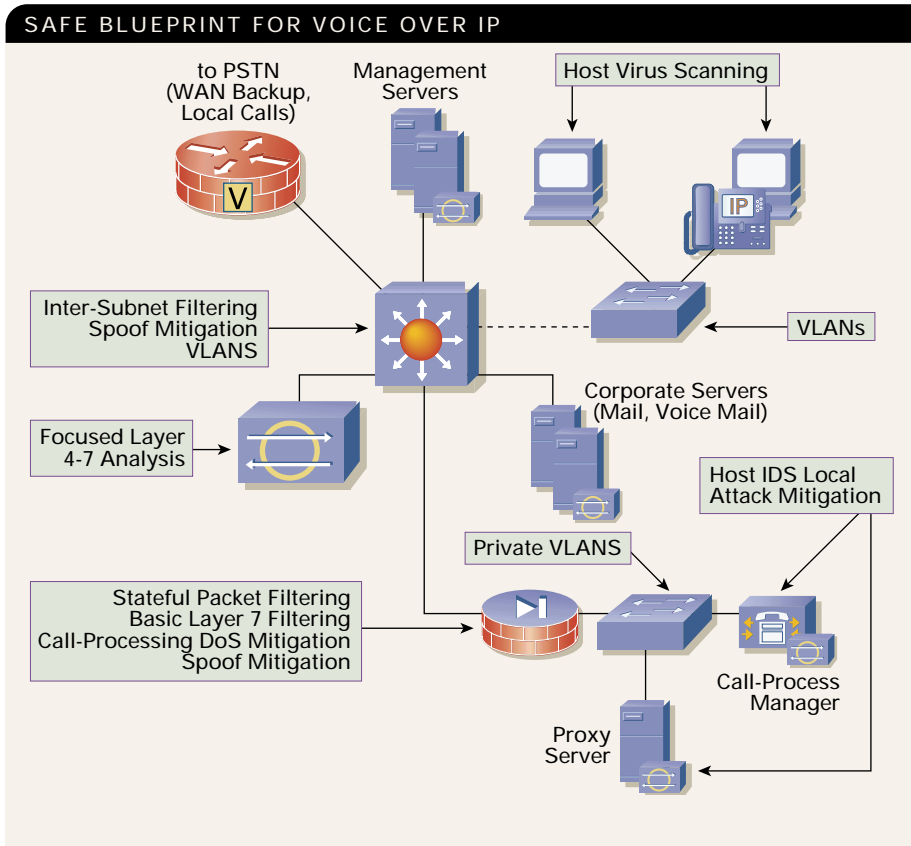


FIGURE 2: The SAFE blueprint details the security elements deployed and the systems involved in a secure IP voice network.

be a phone, may exploit this to gain additional privileges or access to proprietary data. Turn this feature off except during initial mass provisioning, advised Halpern. Another feature allows the PCs plugged into IP phones access to carry out trunking, a feature not necessary in most deployments. A third allows the IP phone to copy all voice packets to the phone's data port for local voice troubleshooting or other applications. Again, this is not necessary in most cases and could lead to snooping should the PC plugged in the data port be remotely compromised. Turn these two off as well.

Finally, access control lists (ACLs) also help secure connectivity by enforcing the separation between Layers 2 and 3. Embedded in the software of all Cisco routers and firewalls and many switches, ACLs allow or deny access between voice and data VLANs based on the requestor's IP address and protocol/port information. If you're not on the list, you don't get in. They help to prevent unauthorized access from data to voice VLANs, among voice VLANs, or among modules—particularly useful against worms or viruses that automatically propagate themselves across the network. Halpern suggests that ACLs be activated in every capable device to enforce the segmentation.

Managing Trust and Identity

Once connectivity is as secure as you can make it, you should focus on identity and trust management: How do you know that your caller—or the person you're calling—is who he or she claims to be? New technologies and features from Cisco such as the combination of Dynamic Host Configuration Protocol (DHCP) snooping, IP Source Guard, and Dynamic Address Resolution Protocol Inspection (DAI) help you be sure. Mediating access through Cisco routers and switches, these technologies specifically protect against spoofing attacks by authenticating devices requesting access to the network.

DHCP snooping intercepts untrusted DHCP messages—which originate outside the network or beyond the firewall—to thwart basic and DoS starvation attacks against DHCP servers. With DHCP, you can statically assign an IP phone's IP addresses to a known MAC address so the IP phone always has the same MAC address; it's very difficult for a hacker to coordinate both addresses.

IP Source Guard is similar in that it blocks and filters all IP packets going through a specified port except for DHCP packets (which are vetted by the DHCP snooper). It passes only those with a DHCP-assigned address, preventing, for example, a malicious host from attacking a network by hijacking a neighboring host's IP address. DAI limits MAC addresses to one per port, mitigating sniffing attacks of various kinds.

For protection at the end user level, Cisco's newest IP phones can validate the veracity of downloaded software images through the use of digital signatures, a very important new feature. "A hacker could attempt to load invalid images on an IP phone in an attempt to make it inoperable or change it's mode of operation altogether," Halpern says. "The latter is more unlikely, but it is a concern we addressed." With the digital signature, the IP phone is able to verify the origin of the image.

Threat Defense

The third focus is the management and prevention of threats; the key technologies are stateful firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs). Halpern recommends that stateful firewalls be deployed primarily in two places—wherever voice and data segments meet, and wherever a stateful monitor is needed to protect voice services. "Protecting every system and every voice segment in the network with a stateful firewall isn't

manageable,” he says. “It’s better to use Cisco PIX® appliances to broker connections between, for example, a voice mail system in the voice segment and an email server in the data segment; IP phones on one voice segment connecting to a call processor in another; PC-based IP phones linking to the call processor; and where the voice gateway meets converged traffic.”

The PIX appliance’s role as stateful monitor comes into play when ACLs are charged with filtering dynamic port addresses rather than static ones. ACLs are not stateful, so when dynamic ports are used, as

Cisco offers IPS functionality via Cisco Security Agent (CSA), which is now supported on many Cisco voice products as well as on the Cisco VPN Client, to provide an additional layer of “day-zero” protection. Available in two versions, desktop and server, CSA provides intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation. Wherever Cisco SoftPhone is deployed, Halpern recommends deploying CSA to provide security in the data to voice segment interaction.

CISCO’S LEADERSHIP AND EXPERTISE IN DATA SECURITY SOLUTIONS MAKE ITS SOLUTIONS UNIQUE IN THEIR ABILITY TO PROTECT IP TELEPHONY AND VOICE OVER IP.

with the RTP protocol, large ranges must be opened to allow connectivity. Using protocol awareness capabilities, a stateful firewall provides single-port accuracy so large ranges of ports need not be opened. Cisco firewalls, both IOS and PIX-based, Halpern says, have extensive enhancements to address specifically the issues presented by IP voice.

IDSs are another must-have—both network-based IDSs (NIDSs) in the network and host-based IPSs (HIPSs) on hosts. Each provides a different type of protection. NIDSs watch packet streams for signatures, or sequences of bits, of known attackers, and like antivirus systems—also recommended—protect a network from known attacks whose signatures have already been mapped. They also detect protocol and other anomalies. “IDSs should be deployed to protect all key systems in the network, including voice mail and call-processing systems,” Halpern says.

HIPSs complement NIDSs. They take a behavioral, non-signature approach, looking for extraordinary events on hosts, and offer “day-zero protection from attacks,” Halpern says. “Even if the vulnerability patch isn’t applied to the host or an attack signature doesn’t even exist yet for the new attack, IPSs still mitigate the attack.” They work by monitoring behavior and detecting anomalies, and can actually prevent a variety of attacks before they occur, as in these examples, according to Halpern: “Why would a Web server’s port 80 process modify its configuration settings in the registry? Why would a Web server copy the shell executable cmd.exe into its Web script directory? Would a Web server ever need to run shell commands? These things should never happen, but we’ve seen both recently in worms that infected systems. IPSs stop these types of events from occurring.”

Filter, Filter, Filter

Once you’ve made provisions for secure connectivity, identity and trust management, and threat management and prevention, your overarching strategy should be “defense in depth,” Cisco’s mantra. Apply any or all security technologies across the network in any and all systems where they’re appropriate. Never rely on a sole mechanism for security. Thus, IDSs should be activated on routers, switches, servers, even on client systems such as PCs. ACLs, of course, should be employed on most of the same systems; Cisco IOS-based and appliance firewalls, where they’re of value—multiple technologies on multiple systems layered throughout the network.

Building a secure IP voice network is clearly possible, Halpern says. Already-available security technologies and products, careful design and implementation, and attention to detail will help to guarantee success. However, he points out, Cisco is the only vendor offering a comprehensive set of security products, strategies, and blueprints. (See “Further Reading” box for related URL links.) Finally, he notes, your byword should be “filter, filter, filter—whenever and wherever possible in the network.” ▲▲

FURTHER READING

- **SAFE: IP Telephony Security in Depth:**
cisco.com/packet/161_6c1
- **SAFE: A Security Blueprint for Enterprise Networks:**
cisco.com/packet/161_6c2



Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912

www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)