PART III

CASE STUDY: SHUTTING DOWN A VENDOR'S VOIP SYSTEM

BigOil is the largest oil and gas company in the United States and is #1 in revenue and profits for 2006. BigOil also has the largest implementation of VoIPTel's (we made up a name so as not to pick on one vendor) VoIP product. BigOil uses VoIPTel's products at all of their facilities, including a very large deployment at the company headquarters. You can find VoIPTel's IP phones just about everywhere you look, including the company's spacious visitors center.

Andy, a part-time hacker, is tired of paying BigOil $150 every time he fills up his poorly tuned Hummer, so he's decided to teach BigOil a lesson. Andy knows from some simple Google searches that BigOil uses VoIPTel's products. He even verified this by walking casually through their visitors center, where there are no less than five fancy IP phones. BigOil's visitors center is so large that no one noticed Andy sitting down and opening up his laptop next to one of the IP phones. There are cameras in the visitors center, but they monitor the security check-in area only.

Andy starts his mischief by forcing the IP phone to reboot by disconnecting and reconnecting its RJ-45 cable. During the bootup process, this poorly protected IP phone offers a chance to enter the administration menu by pressing the * key. Andy does this and now has access to all of the IP phone's configuration. He's interested in a couple of key parameters, including the IP PBX to which the IP phone connects, the IP address of a backup IP PBX, and its DHCP server. There are plenty of other interesting parameters, but this is more than he needs.

When he is sure no one is looking, Andy inserts the IP phone's RJ-45 cable into his laptop. He knows that VoIPTel will use some number of servers to distribute IP phone processing. These IP addresses are normally contiguous, so he builds a list of IP addresses that are likely to be used for the servers. He then uses Nmap to verify that the systems are present and that they are indeed servers used for the IP PBX.

Andy knows from experience that VoIPTel IP PBXs often have telnet enabled by default. Sure enough, he is able to use telnet to connect to each server. He tries several well-known default passwords, but has no luck until, using the last IP address, he finds a password where the default hasn't been changed! Andy can now log in and do all sorts of nasty things, but decides that would be too easy. Plus, he could only affect one server, which won't take down the entire VoIP system.

Andy knows that VoIPTel uses a variant of H.323. He also knows that this protocol is exchanged over ports 1719 and 1720, using UDP and TCP. He then runs several well-known tools—`udpflood` and `tcpsynflood`, which hammer the IP PBX servers. Andy runs several instances of these tools, so he can impact each of the servers.

For good measure, Andy runs dhcpx and targets the DHCP server used by the IP phones. This command consumes all available dynamically assigned IP addresses. This way, if the IP phones reboot, they won't be able to get IP addresses.

During the attacks, service to all of the IP phones connected to the servers is disrupted. Existing calls stay up, but no one can make new calls. Andy knows that his attack is working, because the security guard can't call visitors. He also checks the various other

IP phones in the visitors area and is thrilled to see that all are trying to reconnect with the IP PBX. Andy shuts off the DoS attack, so he won't be pinched. He is pleased to see that none of the IP phones are rebooting properly because they can't get IP addresses. Andy further tests his attack's success by calling a handful of numbers he saved from his Google searches. None of the calls connect. He slips quietly out of the visitors center, confident that he has significantly disrupted BigOil's VoIP system and knowing that it will be a very long day for the VoIP system administrators….

CHAPTER 7

CISCO UNIFIED CALLMANAGER

Cisco CallManager (CCM) is the software-based call-processing component of the Cisco IP telephony solution which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Cisco CallManager 3.3 and earlier, 4.0, and 4.1 are vulnerable to Denial of Service (DoS) attacks, memory leaks, and memory corruption which may result in services being interrupted, servers rebooting, or arbitrary code being executed. Cisco has made free software available to address these vulnerabilities.

—Cisco Security Advisory: Cisco CallManager Memory Handling Vulnerabilities, July 2005
http://www.cisco.com/warp/public/707/cisco-sa-20050712-ccm.shtml

---

From home Linksys VoIP-enabled routers all the way to enterprise CallManager clustered deployments, Cisco's *Architecture for Voice, Video, and Integrated Data (AVVID)* portfolio includes a wide range of software, hardware, and applications to cater to almost any VoIP market. In deciding what Cisco products to concentrate on in this chapter, we wanted to remain focused on the enterprise. Even narrowing down to general enterprise deployments, we were still left with many options. Our test deployment described in the following sections is fairly general and includes attacks and countermeasures that are relevant to other Cisco VoIP product lines and versions.

The layout of this chapter follows the previous material in the book by revisiting many of the attacks we've already defined but presented in a Cisco-specific environment. Correspondingly, the countermeasures here are specific to a Cisco environment in order to provide more focused recommendations. All of the general countermeasures previously covered for each attack still apply; however, we chose to include only those countermeasures that significantly helped augment some of those recommendations with Cisco-specific guidelines.

We would like to thank and acknowledge the help of Troy Sherman from Cisco's Security Group for his assistance and feedback on this chapter.

Vendor Comment

Cisco Systems takes a comprehensive systems approach to security for Unified Communications. Products and technologies from Cisco provide security at all levels of a Unified Communications System—the Infrastructure, Call Management, Endpoints, and Applications. For a system to be considered secure, the security issues for each of these levels must be addressed, and they must be addressed in a systemic manner with all the different components designed to work together. Cisco security for Unified Communications takes advantage of security functions inherent in Cisco voice, networking, and security products and technologies at all levels of a Unified Communications system to ensure safe, reliable communications.

Unified Communications security must work in concert with security measures taken for an organization's entire network. Cisco's approach builds on the Self-Defending Network strategy of a network designed to adapt to new threats as they arise.

INTRODUCTION TO THE BASIC CISCO VOIP (AVVID) COMPONENTS

Before launching into the attacks and countermeasures, we'll provide an overview of the basic Cisco AVVID components.

IP PBX and Proxy

Cisco's VoIP PBX, otherwise known as the Cisco Unified CallManager, was originally released as Multimedia Manager 1.0 in 1994 as a videoconferencing signaling controller. In 1997, it was renamed Selsius-CallManager and had evolved into a VoIP call router. Cisco then acquired Selsius in 1998, at which time the product was built on Windows NT 3.51 and was subsequently renamed Cisco CallManager. Even though Cisco CallManager is a software application, it is installed and sold on customized hardware platforms called *Cisco Media Convergence Servers (MCS)* (http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html or http://tinyurl.com/djao3).

In March 2006, Cisco added the "Unified" moniker to all of its VoIP and video products, and the newly dubbed Cisco Unified CallManager was released under versions 4.2 and 5.0. The 5.*x* branch is a major departure from the traditional Windows-based 3.*x* and 4.*x* installations in that the CallManager software actually runs on a Linux appliance instead of an MCS. While users of the 3.*x* and 4.*x* CallManager had fairly open access to the underlying Windows Server 2003 or Microsoft Windows 2000 Server, the 5.*x* Linux appliances are locked down with only a management interface for most administrative functions. Also available from Cisco is the Cisco Unified CallManager Express (http://www.cisco.com/en/US/products/sw/voicesw/ps4625/index.html or http://tinyurl.com/o6kw7), which is a slimmed-down version of CallManager that is embedded on certain supported routers running IOS. Each CallManager Unified Express installation can support up to 240 lines in comparison to the standard Unified CallManager deployment that can support up to 30,000 lines per server.

At the time of this book's publication, the majority of large enterprise deployments were still running versions 4.*x*, so we decided to concentrate on those instead of the fairly new 5.*x* deployments. With the exception of the OS-specific attacks, most of the other exploits and countermeasures are also applicable to the 5.*x* branch of CallManager as well.

Hard Phones

Cisco sells a plethora of VoIP phones. As of the time of this book's publication, these are the most popular:

- **Cisco Unified IP Phone 7985G** A personal desktop videophone that enables instant, face-to-face communications, the Cisco Unified IP Phone 7985G incorporates a camera, LCD screen, speaker, keypad, and handset into a single, easy-to-use unit.

- **Cisco Unified IP Phones 7971G-GE, 7961G-GE, and 7941G-GE** A suite of IP phones that delivers Gigabit Ethernet Voice over IP.

- **Cisco Unified IP Phones 7970G, 7961G, 7960G, 7941G, and 7940G** These phones feature high-resolution display capabilities, XML applications, multiple lines, and an intuitive interface for business professionals.

- **Cisco Unified IP Phones 7912G, 7911G, and 7905G** These phones feature a single-line, pixel display for XML capabilities.

- **Cisco Unified Wireless IP Phone 7920** This phone delivers up to six extensions, a menu-driven graphical interface, and faster roaming.

- **Cisco Unified IP Phone 7902G** This single-line, entry-level IP phone does not have a display and is designed to meet basic calling requirements for environments such as lobbies, laboratories, manufacturing floors, and hallways.

A complete list of phones is available on Cisco's website at http://www.cisco.com/en/US/products/hw/phones/ps379/index.html.

Softphones

Cisco provides a softphone client called Cisco IP Communicator that runs on a Windows PC and integrates with your existing CallManager deployment (http://www.cisco.com/en/US/products/sw/voicesw/ps5475/index.html or http://tinyurl.com/g24lc). The client has most of the basic features of the hard phones and is targeted at remote workers or road warriors.

Communication Between Cisco Phones and CallManager with SCCP (Skinny)

Skinny Client Control Protocol (SCCP but nicknamed "Skinny") is Cisco's proprietary lightweight H.323-like signaling protocol used between Cisco Unified CallManager and Cisco Unified phones. Because the Skinny protocol is proprietary to Cisco, there are not many public references on its internals or format. There are, however, some open source implementations of SCCP including an Asterisk SCCP module, as well as a Wireshark SCCP dissector.

Cisco IP phones are, in general, fairly dependent on the CallManager to perform most of their functions. For instance, if a phone is taken off the cradle, it will communicate this fact to the CallManager, which will then instruct the phone to play the appropriate dial-tone. By itself and disconnected from the CallManager, the phone can't play the tone.

A Skinny client (in other words, the IP phone) uses TCP/IP over port 2000 to communicate with the CallManager and all messages are nonencrypted. The following is a list of valid Skinny messages:

```
Code  Station Message ID Message
0x0000                 Keep Alive Message
0x0001                 Station Register Message
0x0002                 Station IP Port Message
0x0003                 Station Key Pad Button Message
```

```
0x0004              Station Enbloc Call Message
0x0005              Station Stimulus Message
0x0006              Station Off Hook Message
0x0007              Station On Hook Message
0x0008              Station Hook Flash Message
0x0009              Station Forward Status Request Message
0x11                Station Media Port List Message
0x000A              Station Speed Dial Status Request Message
0x000B              Station Line Status Request Message
0x000C              Station Configuration Status Request Message
0x000D              Station Time Date Request Message
0x000E              Station Button Template Request Message
0x000F              Station Version Request Message
0x0010              Station Capabilities Response Message
0x0012              Station Server Request Message
0x0020              Station Alarm Message
0x0021              Station Multicast Media Reception Ack Message
0x0024              Station Off Hook With Calling Party Number Message
0x22                Station Open Receive Channel Ack Message
0x23                Station Connection Statistics Response Message
0x25                Station Soft Key Template Request Message
0x26                Station Soft Key Set Request Message
0x27                Station Soft Key Event Message
0x28                Station Unregister Message
0x0081              Station Keep Alive Message
0x0082              Station Start Tone Message
0x0083              Station Stop Tone Message
0x0085              Station Set Ringer Message
0x0086              Station Set Lamp Message
0x0087              Station Set Hook Flash Detect Message
0x0088              Station Set Speaker Mode Message
0x0089              Station Set Microphone Mode Message
0x008A              Station Start Media Transmission
0x008B              Station Stop Media Transmission
0x008F              Station Call Information Message
0x009D              Station Register Reject Message
0x009F              Station Reset Message
0x0090              Station Forward Status Message
0x0091              Station Speed Dial Status Message
0x0092              Station Line Status Message
0x0093              Station Configuration Status Message
0x0094              Station Define Time &amp;amp; Date Message
0x0095              Station Start Session Transmission Message
0x0096              Station Stop Session Transmission Message
0x0097              Station Button Template Message
```

```
0x0098              Station Version Message
0x0099              Station Display Text Message
0x009A              Station Clear Display Message
0x009B              Station Capabilities Request Message
0x009C              Station Enunciator Command Message
0x009E              Station Server Respond Message
0x0101              Station Start Multicast Media Reception Message
0x0102              Station Start Multicast Media Transmission Message
0x0103              Station Stop Multicast Media Reception Message
0x0104              Station Stop Multicast Media Transmission Message
0x105               Station Open Receive Channel Message
0x0106              Station Close Receive Channel Message
0x107               Station Connection Statistics Request Message
0x0108              Station Soft Key Template Respond Message
0x109               Station Soft Key Set Respond Message
0x0110              Station Select Soft Keys Message
0x0111              Station Call State Message
0x0112              Station Display Prompt Message
0x0113              Station Clear Prompt Message
0x0114              Station Display Notify Message
0x0115              Station Clear Notify Message
0x0116              Station Activate Call Plane Message
0x0117              Station Deactivate Call Plane Message
0x118               Station Unregister Ack Message
```

SCCP Call Flow Walk Through

The following diagrams illustrate the call setup of a phone call between two SCCP-enabled phones. Figure 7-1 shows an initial call setup as a user dials the extension 3068.

Figure 7-2 illustrates the next stage of the phone call in which the RTP media setup occurs. The StartMediaTransmission or OpenLogicalChannel message is the one that actually signifies when the media stream is established; only after both phones have received this message can the conversation begin.

Figure 7-3 illustrates the call teardown scenario once the receiving party hangs up the phone.

Making Sense of an SCCP Call Trace

Wireshark (http://www.wireshark.org) is a great tool for deciphering Skinny traffic that has been sniffed from the network. Because Skinny messages are unencrypted, it's relatively easy to make sense of the communication going on between a phone and the CallManager. As an example, we've made available a packet trace from our own Cisco VoIP lab of the standard communication that occurs between a Skinny phone and the CallManager when a call is placed. The trace is available at http://www.hackingvoip.com/traces/skinny.pcap. When you open the trace in Wireshark, it will look like Figure 7-4. The IP address of our Cisco 7912 IP phone is 172.16.3.247 and the IP address of our CallManager server is 172.16.3.18.

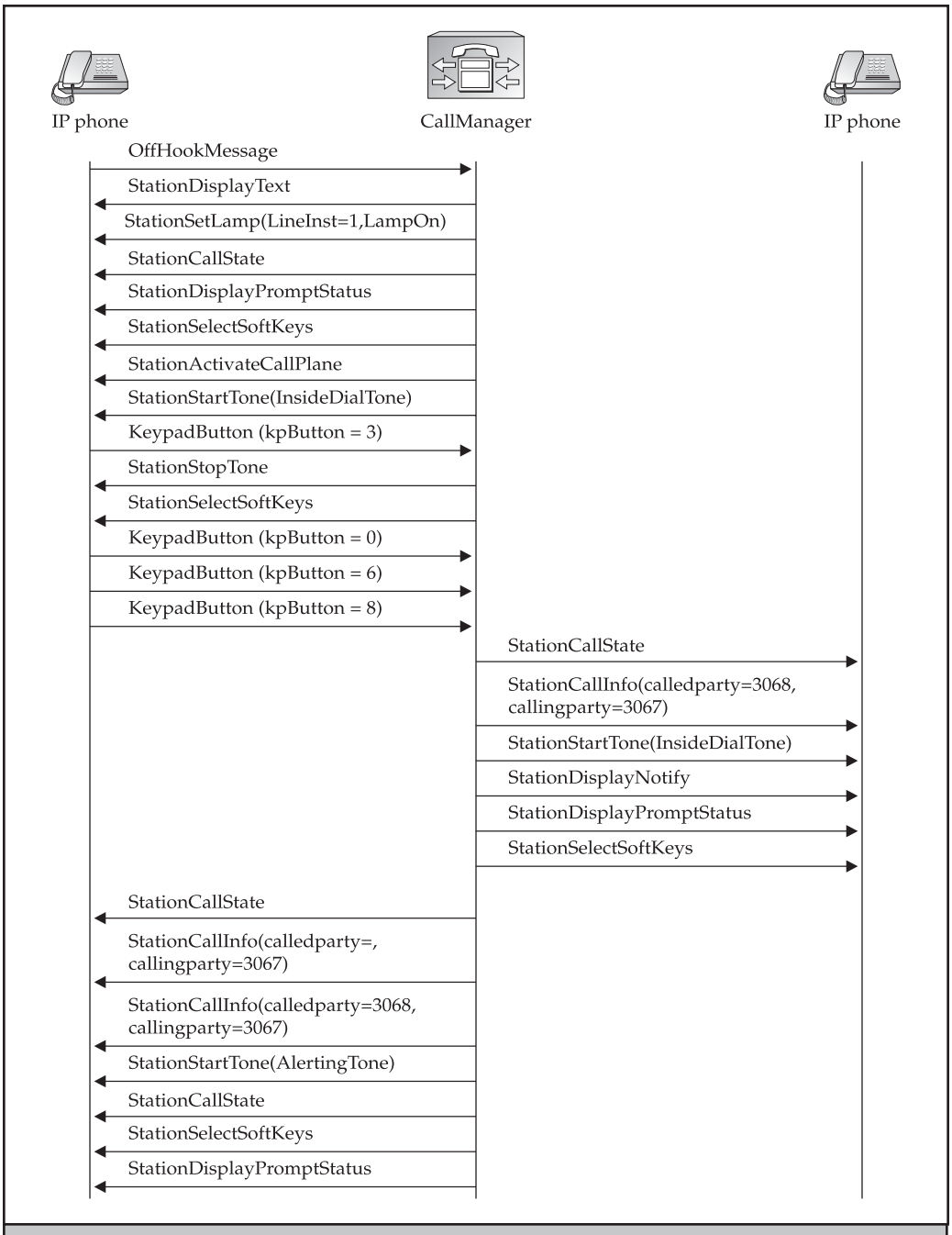

Figure 7-1 The SCCP call setup

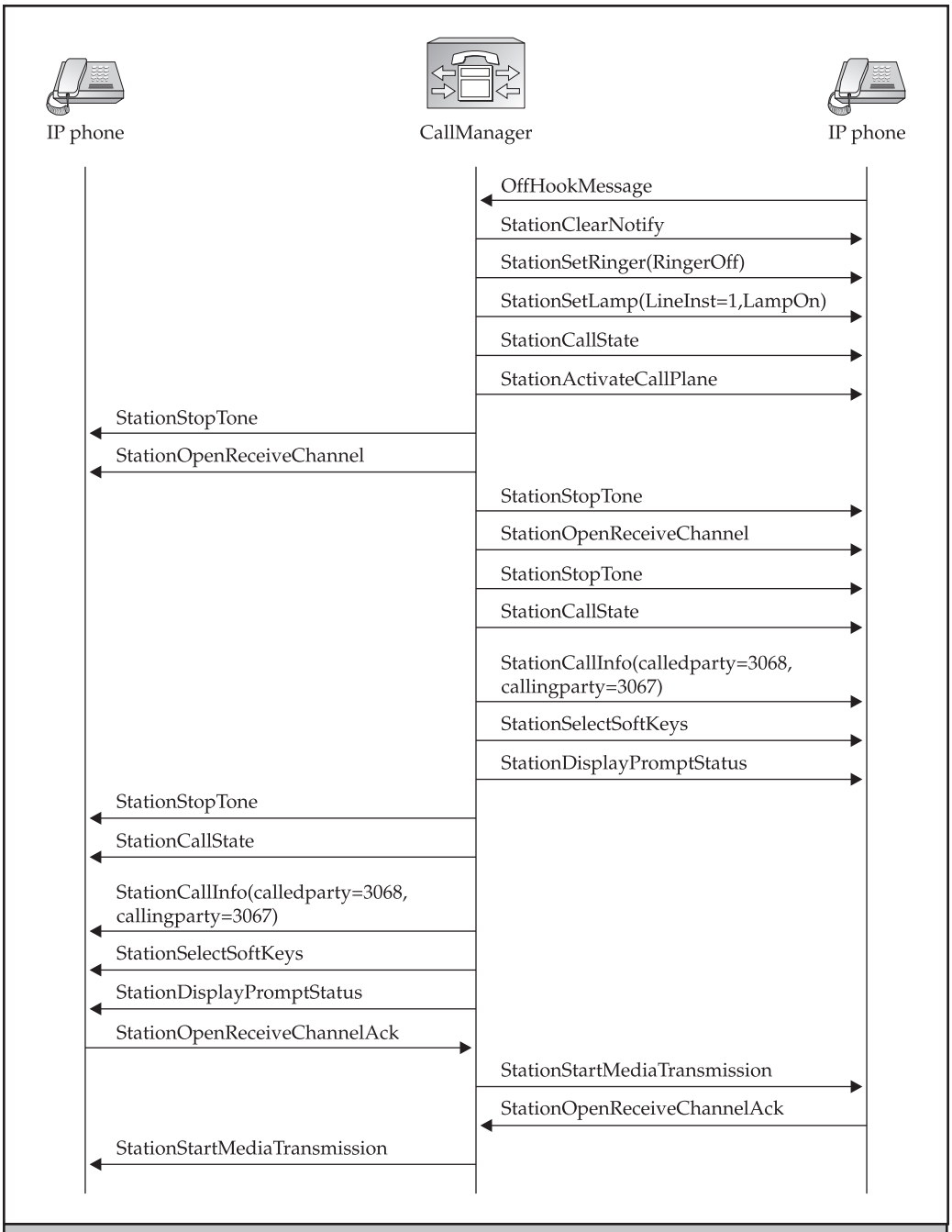

Figure 7-2 The media setup

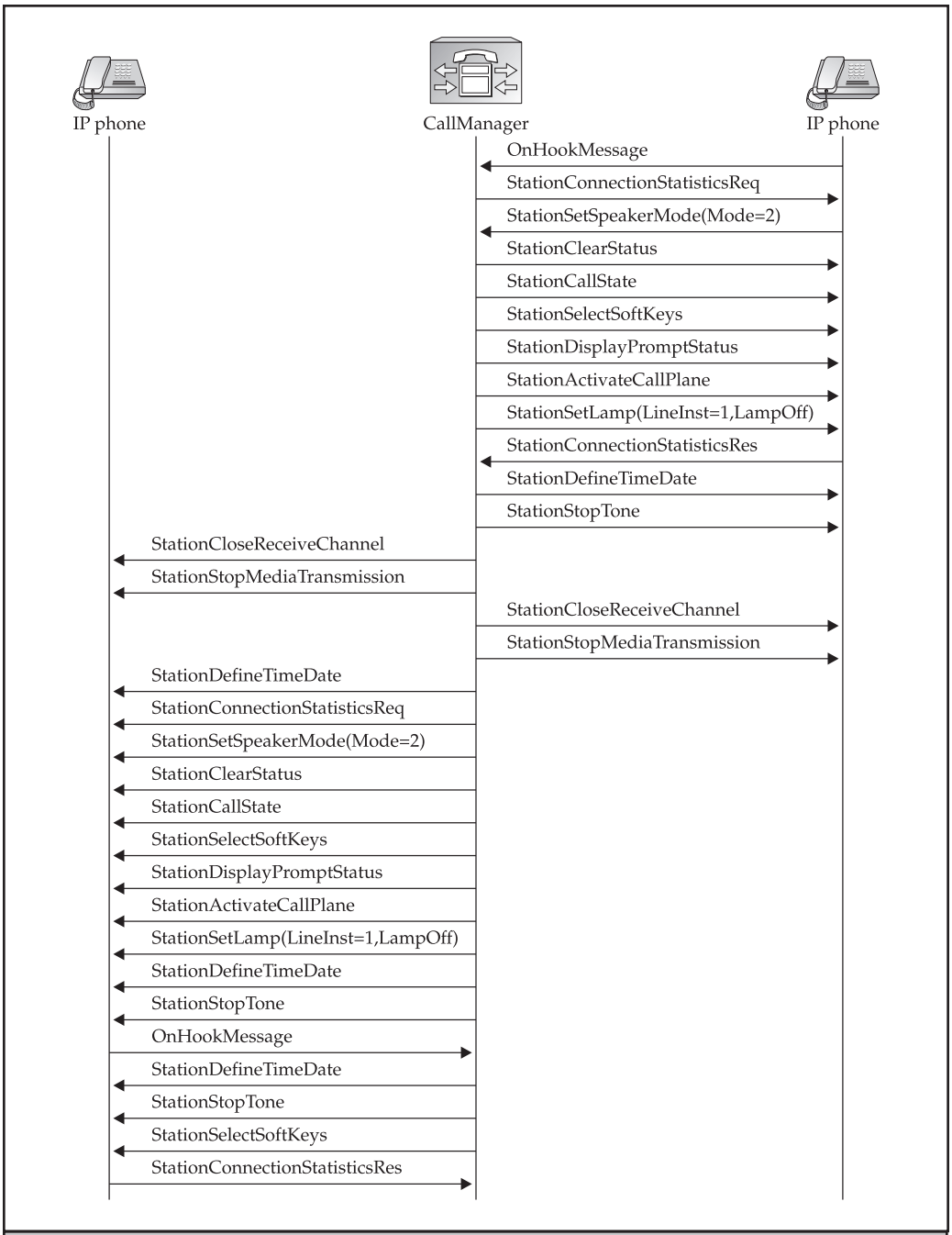

Figure 7-3 The session teardown

Lifting the Phone from the Cradle The first thing that happens in the trace once we lift the phone off the cradle is a Skinny OffHookMessage is sent in packet 7 to the CallManager. This, in turn, triggers a flurry of Skinny messages (packets 8–17) from the CallManger to the phone, ending on the Skinny StartToneMessage message, which tells the phone to play a standard dial tone.

Dialing Numbers In the example recorded in the trace, we dialed extension 2012. Notice that once we press the 2 button, a KeypadButtonMessage is sent from the phone to the CallManager in packet 18. If you click the packet and expand the details in Wireshark, you can clearly see the number 2 in the KeypadButton field (0x000000002). The CallManager sends two Skinny messages in response: the first one is a StopToneMessage in packet 19, which stops the dial-tone sound being played on the phone; and the second Skinny message, shown in packet 20, tells the phone the appropriate tone to play for the number that we pressed. The remaining numbers that we dialed—0, 1, and 2—are illustrated in packets 23, 25, and 27 respectively.

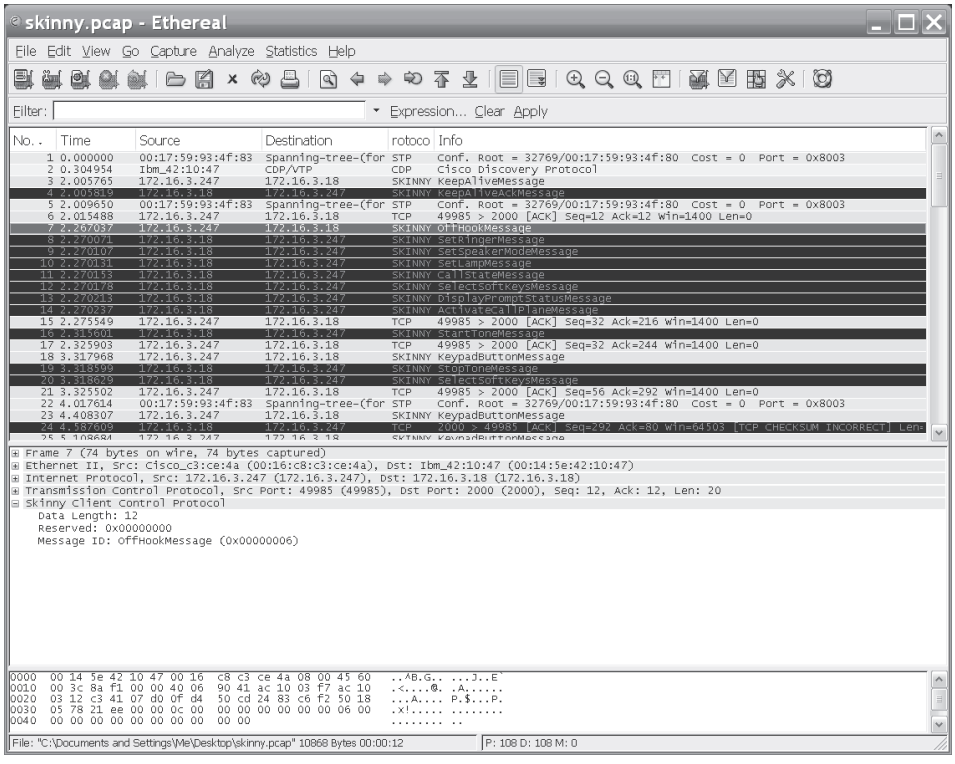

Figure 7-4 Loading the traffic capture of Skinny communications in Wireshark

Call in Progress Starting at packets 31–33, the CallManager updates the LCD display and dial tone of the phone to indicate that the call is being initiated and the receiving phone (x2012) is ringing. Through Skinny messages in packets 34–42, the CallManager communicates with the phone at extension 2012 (IP address 172.16.3.248) in order to set it to ring. For more information on how SCCP works, check out the book *Troubleshooting Cisco IP Telephony* by Paul Giralt, Addis Hallmark, and Anne Smith (Cisco Press, 2002).

Voicemail

Cisco Unity is Cisco's voicemail solution that integrates with preexisting data stores such as Microsoft Exchange and Lotus Domino, for instance. Most Unity installations are sold by resellers on top of Media Convergence Servers or compatible IBM servers as is the CallManager. The Cisco Unity 4.*x* software runs on Windows Server 2003 or Microsoft Windows 2000 Server.

Switches and Routing

For the purposes of this chapter in examining the typical Cisco enterprise VoIP deployment, we're assuming that most switches and routers are Cisco branded as well. Therefore, the countermeasures and exploits will be specific to Cisco networking devices.

You can find more information on Cisco's line of switches and routers at the following links:

- http://www.cisco.com/en/US/products/hw/switches/index.html
- http://www.cisco.com/en/US/products/hw/routers/index.html

As you will see for many Cisco-specific recommendations in the following sections, it is necessary to have an almost homogenous Cisco network environment in order to implement many of them. This has its plusses and minuses, of course, depending on whether or not you've already spent the money to upgrade your networking environment to all Cisco.

CISCO'S SOLUTION REFERENCE NETWORK DESIGN (SRND) DOCUMENT FOR VOICE SECURITY

Cisco maintains a set of best practices collected in a *Solution Reference Network Design (SRND)* document that provides guidelines for deployment and installation of Unified CallManager. In this document, Cisco devotes an entire chapter to voice security and covers some mitigation techniques to many of the attacks we've outlined so far in the book (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a008063742b.html or http://tinyurl.com/gd5r4). This link is a must read for anyone about to deploy a Cisco VoIP deployment.

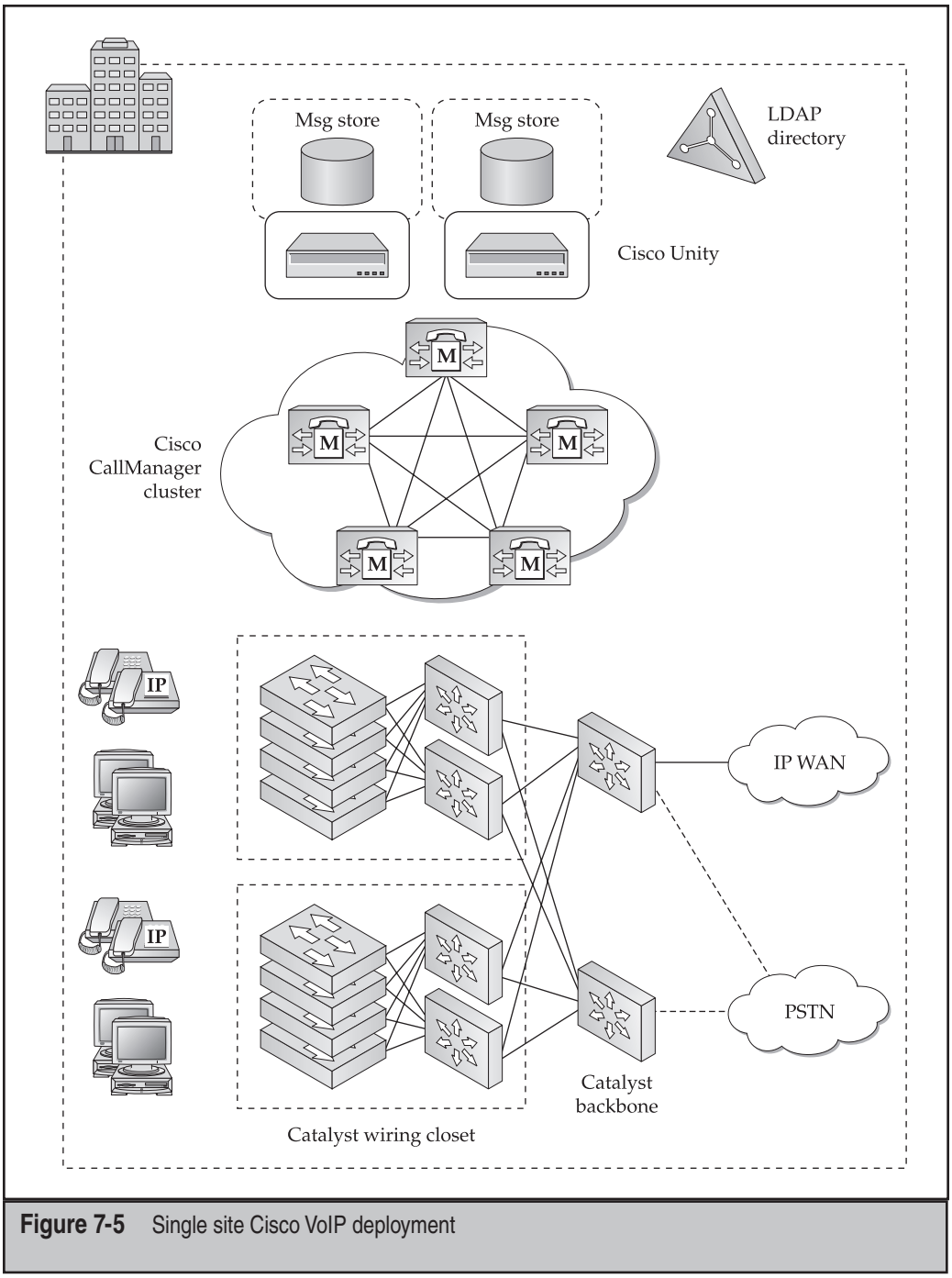

Figure 7-5 Single site Cisco VoIP deployment

BASIC DEPLOYMENT SCENARIOS

For simplicity, most of our attack scenarios will target a single site Cisco VoIP deployment as depicted in Figure 7-5 adapted from Cisco's own deployment guide (*IP Telephony Deployment Models*, http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a0080447510.html).

A typical centralized multisite deployment might not veer off too much from this topology, as shown in Figure 7-6, also adapted from Cisco's deployment guide.

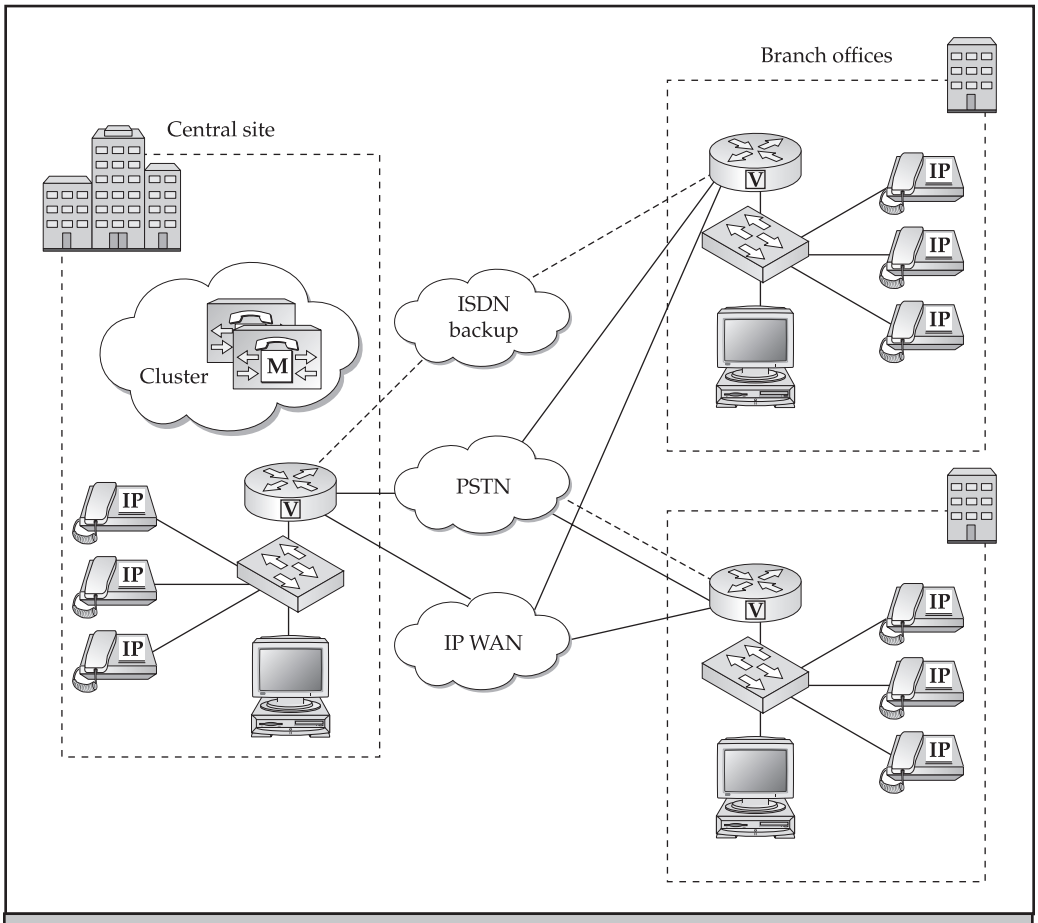

Figure 7-6 Centralized multisite VoIP deployment

SIMPLE NETWORK RECONNAISSANCE

Using the default installation, most of the VoIP components are fairly easy to recognize on the network either by uncovering their web interface or by simple port scanning.

Google Hacking Cisco Devices

Popularity:	*8*
Simplicity:	*9*
Impact:	*6*
Risk Rating:	***7***

As you saw in Chapter 1, it is fairly easy to use search engines such as Google to find exposed VoIP devices with web interfaces. We maintain a fairly up-to-date VoIP Google Hacking Database on our website at http://www.hackingvoip.com. For generic non-VoIP Cisco devices (routers, switches, VPN concentrators, and so on) not covered in our list, you can find many of them at http://johnny.ihackstuff.com in the Google Hacking Database. Removing the `site:yourcompany.com` from the query will reveal all exposed devices on the Internet that Google has archived.

For Google Hacking Cisco Unified CallManager, type the following in Google:

```
intitle:"Cisco CallManager User Options Log On"
"Please enter your User ID and Password in the spaces provided below and
click the Log On button to continue." site:yourcompany.com
```

For Google Hacking Cisco IP Phones, type the following into Google:

```
inurl:"NetworkConfiguration" cisco site:yourcompany.com
```

Google Hacking Countermeasures

Obviously the easiest way to ensure that your VoIP devices don't show up in a Google hacking web query is to disable the web management interface on most of those devices. There's honestly no good reason why any of your phones should be exposed externally to the Internet.

The next easiest step is to restrict access to those web interfaces from specific IP addresses. To disable the web interface on an IP phone from the CallManager interface, follow these steps:

1. In Cisco Unified CallManager Administration, select Device | Phone.
2. Specify the criteria to find the phone and click Find, or click Find to display a list of all phones.
3. To access the Phone Configuration window for the device, click the device name.
4. Locate the Web Access Setting parameter, as shown in Figure 7-7.

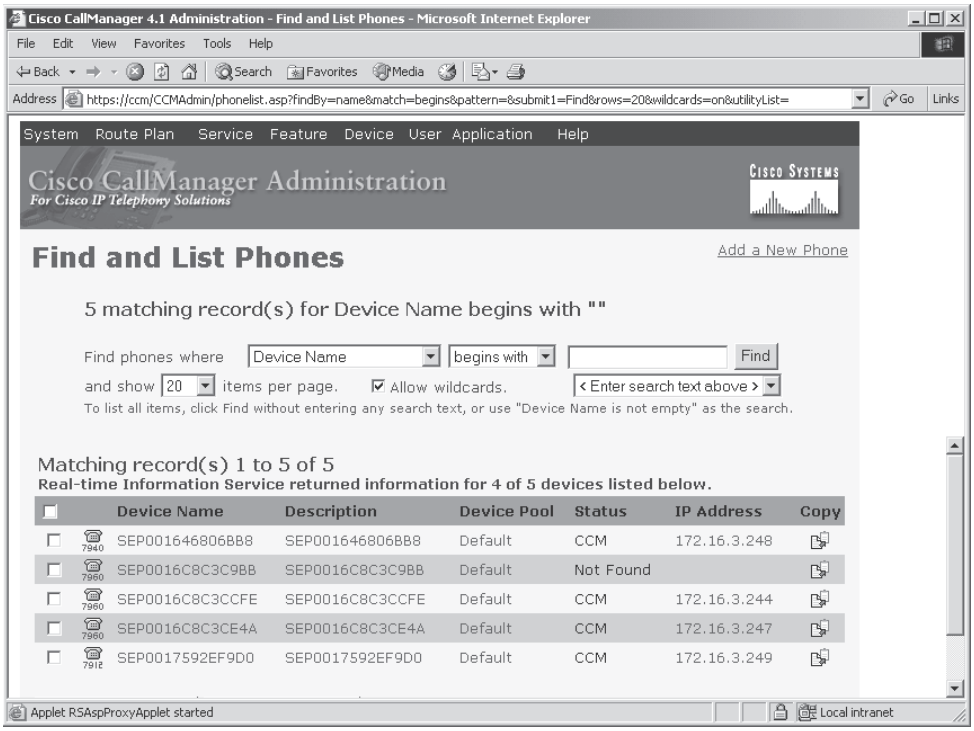

Figure 7-7 Finding the phones in order to disable the web browser

Sniffing

If an attacker is an insider or already has partial access to your internal network, there are a variety of passive host discovery techniques specific to a Cisco VoIP deployment that she can perform.

Cisco Discovery Protocol (CDP)

Popularity:	*6*
Simplicity:	*7*
Impact:	*4*
Risk Rating:	***5***

Cisco Discovery Protocol (CDP) is a proprietary Layer 2 network management protocol built in to most Cisco networking devices, including VoIP phones. CDP is used

particularly in a CallManager environment to discover and remove IP phones dynamically, for dynamic allocation of VLANs to IP phones, and other management functions. CDP packets are broadcast on the local Ethernet segment and contain a wealth of useful reconnaissance information transmitted in plaintext about Cisco devices, including IP address, software versions, and VLAN assignments. Most network sniffers can easily decode CDP traffic, as shown in Figure 7-8.

Looking at a plaintext dump of the entire packet gives us the following:

```
Frame 450 (130 bytes on wire, 130 bytes captured)
IEEE 802.3 Ethernet
Logical-Link Control
Cisco Discovery Protocol
    Version: 2
    TTL: 180 seconds
    Checksum: 0xf1d6
    Device ID: SIP001562EA69E8
        Type: Device ID (0x0001)
        Length: 19
        Device ID: SIP001562EA69E8
    Addresses
        Type: Addresses (0x0002)
        Length: 17
        Number of addresses: 1
        IP address: 192.168.1.52
    Port ID: Port 1
        Type: Port ID (0x0003)
        Length: 10
        Sent through Interface: Port 1
    Capabilities
        Type: Capabilities (0x0004)
        Length: 8
        Capabilities: 0x00000010
    Software Version
        Type: Software version (0x0005)
        Length: 16
        Software Version: P003-07-5-00
    Platform: Cisco IP Phone 7960
        Type: Platform (0x0006)
        Length: 23
        Platform: Cisco IP Phone 7960
    Duplex: Full
        Type: Duplex (0x000b)
        Length: 5
        Duplex: Full
    Type: Unknown (0x0010), length: 6
        Type: Unknown (0x0010)
        Length: 6
        Data
```

You can also find some more CDP examples in the trace we provide at http://www.hackingvoip.com/traces/skinny.pcap, specifically in packet number 2.

CDP Sniffing Countermeasures

Most schools of thought recommend turning off CDP on Cisco devices where the environment is mostly static. However, in a VoIP environment, CDP can offer so much management functionality that keeping it enabled where absolutely needed might be an acceptable trade-off.

From a strict security perspective, however, CDP can provide attackers with a wealth of data about your network and should be disabled. A physical insider to your organization can also attach a hub to a VoIP phone and sniff this broadcast traffic in order to glean valuable information about the network. Depending on the physical location where the VoIP phone is installed in your environment, there are also a few other techniques that can be applied as outlined in Cisco's lobby phone deployment example (http://tinyurl.com/q38z8).

Applying a proper VLAN strategy of segmenting your data and voice traffic can also help mitigate the risk of an attacker sniffing these packets.

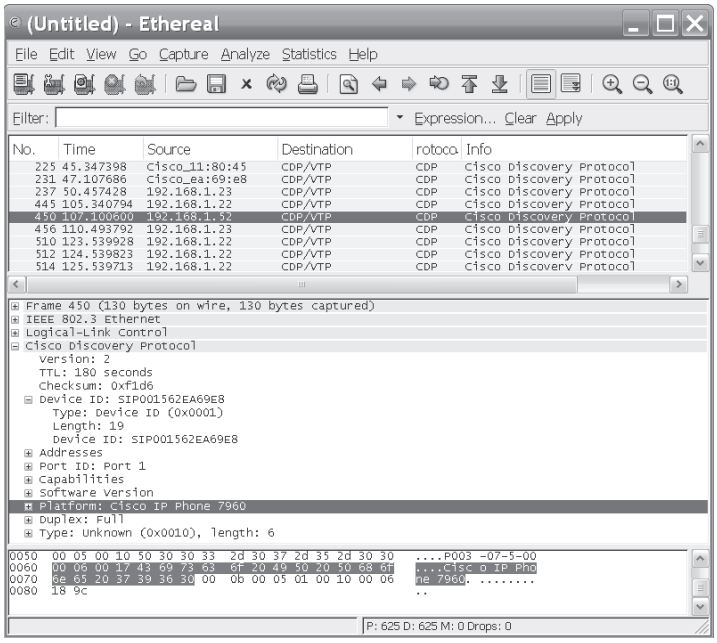

Figure 7-8 CDP dump in Wireshark of a Cisco SIP 7960 phone

DHCP Response Sniffing and Spoofing

Popularity:	*4*
Simplicity:	*8*
Impact:	*3*
Risk Rating:	***5***

Typically, a DHCP server will send its responses to each node on a subnet to facilitate the gathering of this information for other devices on the subnet. Besides just ARP to IP address mappings, DHCP responses can also reveal other juicy tidbits to a hacker, such as the IP address of the TFTP server used to configure the phones on the network, as well as DNS server IP addresses. In some cases, an attacker could masquerade as a rogue DHCP server and respond to the client's request before the legitimate DHCP server.

DHCP Response Sniffing and Spoofing Countermeasures

Most Cisco switches and routers have a security feature called DHCP snooping that will cause the device to act as a DHCP firewall/proxy between trusted and untrusted network interfaces (see http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a008014f341.html or http://tinyurl.com/b3evq). When DHCP snooping is enabled, the Cisco switch can prevent a malicious or spoofed DHCP server from assigning IP addresses by blocking all replies to a DHCP request unless the specific port has been configured ahead of time to allow replies.

Scanning and Enumeration

The following section goes along with the hacking techniques we outlined in Chapters 2 and 3.

UDP/TCP Port Scanning

Popularity:	*10*
Simplicity:	*8*
Impact:	*4*
Risk Rating:	***7***

Port scanning most CallManager and Unity servers will result in a variety of standard Windows or Linux services (depending on the version) responding as well. Table 7-1 is a useful listing of Cisco Unity Server ports active for a default installation of the various

Cisco VoIP components (http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_chapter09186a0080441e35.html).

Server Source Port	Protocol or Service	Port Usage Description
TCP 25	SMTP	Used by Microsoft Exchange when installed on the Cisco Unity server.
TCP and UDP 53	DNS	Accesses the DNS server for name resolution. Used when the DNS server is running.
UDP 67	DHCP/BOOTP (when Cisco Unity is a DHCP client) DHCP/BOOTP (when Cisco Unity is a DHCP server)	If using DHCP instead of static IP addresses, sends DHCP or BOOTP requests. Receives DHCP or BOOTP requests.
UDP 68	DHCP/BOOTP (when Cisco Unity is a DHCP client) DHCP/BOOTP (when Cisco Unity is a DHCP server)	If using DHCP instead of static IP addresses, receives DHCP or BOOTP replies. Sends DHCP or BOOTP replies.
TCP 80	HTTP	Accesses the Cisco Unity Administrator, the Cisco Personal Communications Assistant, and Microsoft Internet Information Services (IIS).

Table 7-1 Cisco Unity Server Active Ports

Server Source Port	Protocol or Service	Port Usage Description
TCP 135	MS-RPC	Negotiates access to the Media Master, Cisco Unity ViewMail for Microsoft Outlook, the Exchange server, and other DCOM services.
UDP 137	NetBIOS	NetBIOS Name Service—resolves name for NetBIOS or WINS.
UDP 138	NetBIOS	NetBIOS Datagram Service for browsing Windows networks.
TCP 139	NetBIOS	Accesses Windows file shares and performs NetBIOS over TCP/IP connections. Accesses Cisco Unity reports and Microsoft Windows file shares.
UDP 161	SNMP	Sends SNMP notifications and provides SNMP information when the host agent is queried.
UDP 162	SNMP Trap	Sends SNMP Traps.
TCP 389	LDAP with AD-DC	Accesses LDAP directory services. Used when running on the domain controller providing LDAP directory services.

Table 7-1 Cisco Unity Server Active Ports *(continued)*

Server Source Port	Protocol or Service	Port Usage Description
Configurable (TCP 390 or any unused TCP port recommended.)	LDAP with Exchange 5.5	Accesses LDAP directory services. Used when running on the domain controller providing LDAP directory services.
TCP 443	HTTP/SSL	Performs system administration on a remote Cisco Unity server when it's configured for HTTP/SSL. Accesses Cisco Unity Administrator, IIS, or the Cisco PCA when the Cisco Unity server is configured for HTTP/SSL.
TCP 445	SMB	Accesses Windows file shares and performs NetBIOS over TCP/IP connections. Accesses Cisco Unity reports and Microsoft Windows file shares.
TCP 636	LDAP/SSL	Accesses LDAP directory services over SSL. Used when running on a domain controller providing LDAP directory services over SSL.
TCP 691	SMTP/LSA	Used by Exchange server when it is accepting SMTP with LSA.

Table 7-1 Cisco Unity Server Active Ports *(continued)*

Server Source Port	Protocol or Service	Port Usage Description
TCP 1432	TDS proxy (CiscoUnityTdsProxy)	Local processes use to access the SQL server or MSDE database.
TCP 1433 (default)	MS-SQL-S	Accesses the SQL server or MSDE database and performs replication when Cisco Unity failover configured.
UDP 1434	MS-SQL-M	Accesses the SQL server or MSDE database.
TCP 2000 (default)	Skinny (SCCP)	Accesses Cisco CallManager.
TCP 3268	LDAP with AD-GC	Accesses LDAP directory services when the global catalog server is on another server. Used when running on the global catalog server providing LDAP directory services.
TCP 3269	LDAP/SSL with AD-GC	Accesses LDAP directory services over SSL when the global catalog server is on another server. Used when running on the global catalog server providing LDAP directory services over SSL.

Table 7-1 Cisco Unity Server Active Ports *(continued)*

Server Source Port	Protocol or Service	Port Usage Description
TCP 3372	MSDTC	Accesses the SQL server or MSDE database when Cisco Unity failover configured.
TCP 3389	Windows Terminal Services	Performs remote system administration on a Cisco Unity server.
TCP 3653	Node Manager	Sends manual keep-alive packets (or pings) between the primary and secondary servers when Cisco Unity failover configured.
TCP 4444	Kerberos authentication	Performs Kerberos authentication.
TCP 5060 (default)	SIP	Connects to SIP endpoints or SIP proxy servers.
TCP 5060+	SIP	Connects to PIMG units. (Requires one port per PIMG unit.)
TCP 8005	Server Life Cycle (JMX)	Accesses the Tomcat server.
TCP 8009	AJP	Used by IIS.
TCP and UDP dynamic (in the range of 1024–65535)	DCOM	Media Master uses to play and record voice messages and used when the Cisco Unity server is a domain controller supporting member servers.

Table 7-1 Cisco Unity Server Active Ports *(continued)*

Server Source Port	Protocol or Service	Port Usage Description
UDP dynamic (in the range of 1024–65535)	MAPI notifications	Notifies Cisco Unity of changes to subscriber mailboxes when Exchange is the message store.
UDP dynamic (in the range of 22800–32767)	RTP	Sends and receives VoIP traffic with SCCP or SIP endpoints.
Not applicable	ICMP	Used by Cisco Unity Telephony Integration Manager (UTIM) to ping Cisco CallManager.

Table 7-1 Cisco Unity Server Active Ports *(continued)*

Table 7-2 is adapted from the Cisco online guide at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/udp_tcp/ and includes a description of Cisco Unified CallManager 5.*x* active ports. Remember that Cisco CallManager 5.*x* installations are installed on Linux.

Server Source Port	Port Usage Description
Common Service Ports	
7	Internet Control Message Protocol (ICMP); carries echo-related traffic
22 / TCP	Secure FTP service, SSH access
53 / UDP	CallManager acts as a DNS server or DNS client
67 / UDP	Cisco Unified CallManager acts as a DHCP server
68 / UDP	Cisco Unified CallManager acts as a DHCP client
69 / UDP	Trivial File Transfer Protocol (TFTP)
111 / TCP and UDP	Remote Procedure Call
80,8080 / TCP	HTTP

Table 7-2 Cisco Unified CallManager 5.*x* Active Ports

Server Source Port	Port Usage Description
123 / UDP	Network Time Protocol (NTP)
161, then 8161 / UDP	SNMP service response (requests from management applications)
162 / UDP	Sends SNMP trap to management application
443, 8443 / TCP	HTTPS
6161 / UDP	Native SNMP service response (requests from management applications)
6162 / UDP	Sends native SNMP trap to management application
32768 / TCP	Internet networking daemon
Intracluster Ports Used Between Cisco Unified CallManagers	
514 / UDP	System logging service
1099 /TCP	Cisco AMC Service for RTMT performance monitors, data collection, logging, and alerting
1500,1501 / TCP	Connects database (1501 / TCP is the secondary connection)
1515 / TCP	Replicates database between nodes during installation
2535 / UDP	Allows hosts to request multicast address allocation services from a DHCP server
2555 / TCP	Real-time Information Services (RIS) database server
2556 / TCP	Real-time Information Services (RIS) database client for Cisco RIS
3000 / UDP	Receives change notification from CallManager database
4040 / TCP	DRF master agent
4343 / TCP	DRF local agent
5001 / TCP	SOAP monitor
5555 / TCP	License Manager listens to license request
7000 / TCP	RTMT Trace Collection Tool Service (TCTS)

Table 7-2 Cisco Unified CallManager 5.*x* Active Ports *(continued)*

Server Source Port	Port Usage Description
7070 / TCP	Certificate Manager Service
7727 / TCP	Application database change notification, CTI, voice messaging, and so on
7999 / TCP	Cellular Digital Packet Data Protocol
8001 / TCP	Client database change notification
8002 / TCP	Intracluster Communication Service
8003 / TCP	Intracluster Communication Service (to CTI)
8004 / TCP	Intracluster communication between Cisco Unified CallManager and CMIManager
8009 / TCP	Internal Tomcat requests
8500 / UDP	Intracluster replication of system data by IPSec Cluster Manager RIS
8888 – 8889 / TCP	Service Manager status request and reply
Signaling, Media, and Other Communication Between Phones and Cisco Unified CallManager	
69, then Ephemeral / UDP	Trivial File Transfer Protocol (TFTP) for downloading firmware and configuration files
8080 / TCP	Phone URLs for XML applications, authentication, directories, services, and so on; these ports are configurable on a per-service basis
2000 / TCP	Skinny Client Control Protocol (SCCP)
2443 / TCP	Secure Skinny Client Control Protocol (SCCPS)
3804 / TCP	Certificate Authority Proxy Function (CAPF) listening port for issuing Locally Significant Certificates (LSCs) to IP phones
5060 / TCP and UDP	Session Initiation Protocol (SIP) phone
5061 / TCP and UDP	Secure Session Initiation Protocol (SIPS) phone
16384 _ 32767 / UDP	Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP)

Table 7-2 Cisco Unified CallManager 5.*x* Active Ports *(continued)*

NOTE Cisco Unified CallManager uses only 24576–32767, though other devices use the full range of ports.

Table 7-2, while not a complete listing of ports, should be enough to assist in device identification based on Nmap results. A more complete list of active ports can be found at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/udp_tcp/.

Table 7-3 is a listing of Cisco Unified CallManager 4.*x* active ports, and while not a complete listing, it should also be enough to assist in device identification based on Nmap results. A more complete list of active ports can be found at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/udp_tcp/. Remember that Cisco CallManager 4.*x* installations are installed on Windows.

Server Source Port	Port Usage
Common Service Ports	
7	Internet Control Message Protocol (ICMP); carries echo-related traffic
53 / UDP	CallManager acts as a DNS server or DNS client
67 / UDP	Cisco Unified CallManager acts as a DHCP server
68 / UDP	Cisco Unified CallManager acts as a DHCP client
69 / UDP	Trivial File Transfer Protocol (TFTP)
80 / TCP	HTTP
123 / UDP	Network Time Protocol (NTP)
161 / UDP	SNMP service response (requests from management applications)
162 / UDP	Sends SNMP trap to management application
2535 / UDP	Allows hosts to request multicast address allocation services from a DHCP server
3389 / TCP	Microsoft Windows Terminal Services
5900 / TCP	VNC Viewer

Table 7-3 Cisco Unified CallManager 4.*x* Active Ports

Server Source Port	Port Usage
Intracluster Ports Used Between Cisco Unified CallManagers	
135 / TCP	
137 /TCP & UDP	Microsoft NetBIOS name service
138 / UDP	Microsoft NetBIOS datagram service
139 / TCP	Microsoft NetBIOS session service
445 / TCP	Microsoft Server Message Block (SMB)
1433 / TCP	SQL requests
2552 / TCP	CallManager database change notification
2555 / TCP	Real-time Information Services (RIS) database server
2556 / TCP	Real-time Information Services (RIS) database client
3000 / UDP	Receives change notification from CCM database
3001 / UDP	Database change notification from publisher to applications
3020 / UDP	Dialed Number Analyzer plug-in database change notification
3372 / TCP	SQL Distributed Transaction Coordinator
7727 / TCP	Application database change notification, CTI, voice messaging, and so on
8001 / TCP	Client database change notification
8002 / TCP	Intracluster Communication Service
8003 / TCP	Intracluster Communication Service
8009 / TCP	Internal Tomcat requests
8111 / TCP	IP Manager / Assistant (IPMA) web requests
8222 / TCP	Extension Mobility (EM) web requests
8333 / TCP	WebDialer web requests
8444 / TCP	Extension Mobility (EM) service
8555 / TCP	Apache-SOAP web requests
8666 / TCP	IP Manager / Assistant (IPMA) web requests for nondefault locales

Table 7-3 Cisco Unified CallManager 4.*x* Active Ports *(continued)*

Server Source Port	Port Usage
8777 / TCP	Tomcat manager web requests
9007 / TCP	CDR Analysis and Recording (CAR) web requests

Table 7-3 Cisco Unified CallManager 4.*x* Active Ports *(continued)*

Port Scanning Countermeasures

As discussed in Chapters 2 and 3, it's a good idea to disable as many default services as possible on your VoIP devices to avoid giving away too much information about your infrastructure; however, this is not really an option on CallManager 5.*x* servers as Cisco has locked them down much more than the 4.*x* predecessors running on Windows. Configuring your switches and routers with the proper ingress and egress filtering rules through best practices is also important. To help automate this task, Cisco IOS networking devices have a nifty "autosecure" feature that launches a variety of other functions that are detailed in the following list (see http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/cas11_ds.htm or http://tinyurl.com/y7jpqz):

1. Disables the following Global Services:
   - Finger
   - PAD
   - Small servers
   - Bootp
   - HTTP service
   - Identification service
   - CDP
   - NTP
   - Source routing
2. Enables the following Global Services:
   - Password-encryption service
   - Tuning of scheduler interval/allocation
   - TCP synwait-time
   - tcp-keepalives-in and tcp-keepalives-out
   - SPD configuration
   - No IP unreachables for null 0

3. Disables the following services per interface:
   - ICMP
   - Proxy-Arp
   - Directed broadcast
   - MOP service
   - ICMP unreachables
   - ICMP mask reply messages
4. Provides logging for security:
   - Enables sequence numbers and timestamp
   - Provides a console log
   - Sets log buffered size
   - Provides an interactive dialogue to configure the logging server IP address
5. Secures access to the router:
   - Checks for a banner and provides a facility to add text to automatically configure: login and password, transport input and output, exec-timeout, local AAA, and SSH timeout and SSH authentication retries to a minimum number
   - Enables only SSH and SCP for access and file transfer to and from the router
   - Disables SNMP if not being used
6. Secures the forwarding plane:
   - Enables Cisco Express Forwarding (CEF) or distributed CEF on the router, when available
   - Anti-spoofing
   - Blocks all IANA-reserved IP address blocks
   - Blocks private address blocks if customer desires
   - Installs a default route to null 0, if a default route is not being used
   - Configures TCP intercept for connection-timeout, if the TCP intercept feature is available and the user is interested
   - Starts interactive configuration for CBAC on interfaces facing the Internet, when using a Cisco IOS firewall image
   - Enables NetFlow on software-forwarding platforms

Part of Cisco's SRND recommends segmenting the voice and data networks with logically separate VLANs. This will help restrict access to the phones and critical servers.

TFTP Enumeration

Popularity:	*5*
Simplicity:	*9*
Impact:	*9*
Risk Rating:	***8***

As we demonstrated in Chapter 3, the TFTP server used to provision VoIP phones can often contain sensitive configuration information sitting out in cleartext. This is less of a threat with TFTP servers dedicated solely to non-SIP Cisco phones. However, the TFTP server can be used to identify a Cisco Unified CallManager device correctly if the following files exist: `/MOH/SampleAudioSource.xml`, `RingList.xml`, and `Annunciator.xml`. You can easily enumerate these files with the TFTPbrute.pl exploit demonstrated in Chapter 3 or even with the latest version of Nessus (http://www.nessus.org).

SNMP Enumeration

Popularity:	*7*
Simplicity:	*7*
Impact:	*10*
Risk Rating:	***8***

As you saw in Chapter 3, most networked devices support SNMP as a management function. An attacker can easily sweep for active SNMP ports on a device, and then query with specific Cisco OIDs in order to glean sensitive information from the device. As you can see in Figure 7-9, it's fairly easy to point any SNMP browser at a Cisco CallManager with a default public community string.

SNMP Enumeration Countermeasures

Best practices for network design suggest that SNMP access should be fairly limited within an enterprise network from the VoIP phone access ports. This means that an attacker shouldn't be allowed to simply unplug a VoIP phone, plug in his laptop to the access port, and start arbitrarily querying SNMP devices on the VLAN. Strict access control can be applied on the switch to make sure the only SNMP management traffic allowed is from controlled locations.

SNMP v3 should be used for SNMP read/write authentication, assuming AuthPriv is used on both sides. Also, hard-to-guess community strings should be used rather than the defaults that come installed with the device. Applying intelligent access control to SNMP (UDP port 161) is trivial to bypass, but better than nothing in many cases.

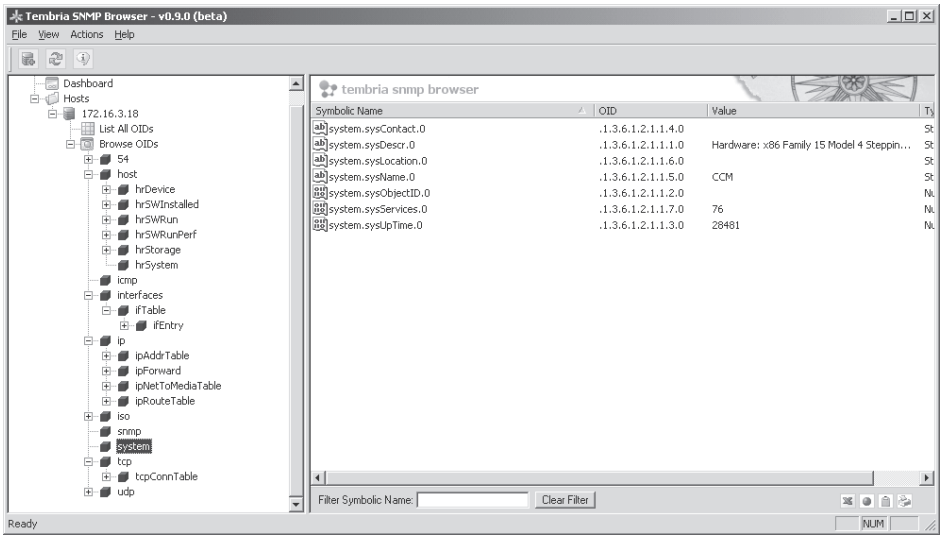

Figure 7-9 SNMP browsing of a Cisco CallManager

In CallManager 4.*x* itself, you can change the community strings by clicking Start | Programs | Administrative Tools | Services | SNMP Service and then following these steps:

1. Click Start to enable the service if it is not already started.
2. Click the Security tab, as shown in Figure 7-10.
3. Click Add.
4. Select READ ONLY from the Community Rights list.
5. Enter your community string name.
6. Click Add.
7. Select READ WRITE from the Community Rights list.
8. Enter your community string name.
9. Click OK.

To restrict which hosts (Network Management Systems) can communicate to the CallManager server, still on the Security tab, continue with these steps:

10. Select Accept SNMP Packets from These Hosts.
11. Click Add.
12. Enter the IP address of the host(s).
13. Click OK.

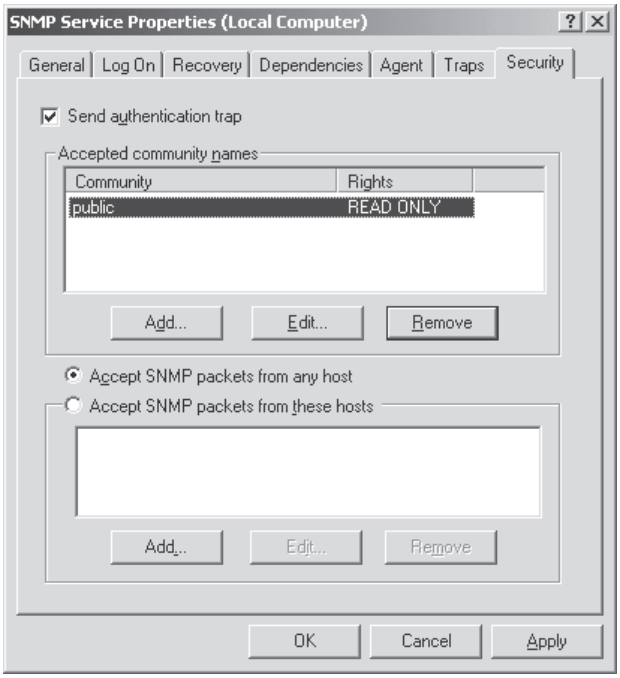

Figure 7-10 SNMP Service Properties window editing the Public string

VNC Enumeration

Popularity:	*6*
Simplicity:	*5*
Impact:	*10*
Risk Rating:	***7***

Virtual Network Computing (VNC) is included with the CallManager 4.*x* software in the `C:\utils` directory. VNC is a remote desktop sharing/control program similar to PCAnywhere or Remotely Possible. Best practices dictate that after an administrator has finished using VNC on a Windows CallManager 4.*x* server, he or she should disable it. Sometimes, however, they might forget to disable the service, leaving open an attractive service to brute force. A running VNC installation can be identified by getting a response from TCP port 5900 on the Windows server. A tool by the Phenoelit group called VNCrack gives an attacker the ability to brute force the password on a VNC service (http://www.phenoelit.de/vncrack/download.html).

VNC Countermeasures

Really, the best countermeasure is to remember to disable it! However, if VNC or any type of remote access management software is needed, another best practice is to limit access to this service from specific controlled locations in the network through strict ACL settings on the switch and firewalls within your network.

EXPLOITING THE NETWORK

This section follows along with the networking-based attacks we outlined in Chapters 4, 5, and 6.

Infrastructure Flooding Attacks

Popularity:	*8*
Simplicity:	*6*
Impact:	*7*
Risk Rating:	***7***

All of the flooding denial of service attacks that we outlined in Chapter 4 can have just as damaging an impact in a Cisco VoIP deployment. As a reminder, these included UDP flooding, TCP SYN flooding, ICMP flooding, and established connection flooding attacks.

Flooding Attacks Countermeasures—AutoQoS

The defenses to most of these flooding attacks involves many of the general countermeasures we covered in Chapter 4, including VLANs, anti-DDoS solutions, hardening the network perimeter, and finally quality of service enforcement by configuring the network infrastructure itself to detect and prioritize VoIP traffic properly.

Perhaps the most important Cisco-specific countermeasure for mitigating flooding attacks is to ensure that quality of service settings are properly configured across your infrastructure. Cisco's IOS Quality of Service Solutions Guide provides a step-by-step list for enabling and tuning QoS parameters for your entire enterprise on IOS-supported devices; go to http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a0080435d50.html.

The last section of this guide introduces a fairly new feature in IOS, available since release 12.2(15)T. Called AutoQoS, this feature "simplifies QoS implementation and speeds up the provisioning of QoS technology over a Cisco network. It reduces human error and lowers training costs. With the AutoQoS VoIP feature, one command (the `auto qos` command) enables QoS for VoIP traffic across every Cisco router and switch"

(http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455a3d.html).

For a mid-size to large enterprise, the IOS AutoQoS features are compelling because setting up effective QoS for applications can be challenging and time consuming for an IT admin.

Additionally, some Cisco switches also have the ability to apply a feature called *scavenger class* quality of service. Scavenger class QoS allows the administrator to rate shape certain types of traffic so low that prioritized applications within the network will be unaffected. This is typically a common mitigation technique to some DDoS attacks when bursty worm traffic is detected in the network. More information on scavenger class QoS features is available in Cisco's *Enterprise Solution Reference Network Design Guide* (http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf or http://tinyurl.com/kh5bq).

Denial of Service (Crash) and OS Exploitation

Popularity:	*9*
Simplicity:	*8*
Impact:	*10*
Risk Rating:	***9***

The majority of problems that CallManager has faced over the years has had more to do with its underlying operating system than the VoIP application itself. Most of the worms and viruses that have affected CallManager 4.*x* have done so because of a vulnerable Windows component. Consider the following security advisories:

- "MS Windows W32.Blaster.Worm Affects Cisco CallManager and IP Telephony Applications," http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801ae3dc.shtml or http://tinyurl.com/y3fxa3
- "Defend Against the Sasser Virus on the MCS Servers," http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_tech_note09186a0080223c65.shtml or http://tinyurl.com/y4ppkl
- "Cisco Security Advisory: 'Code Red' Worm—Customer Impact," http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml or http://tinyurl.com/yyxpcp
- "Cleaning Nimda Virus from Cisco CallManager 3.*x* and CallManager Applications Servers," http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00800941e4.shtml or http://tinyurl.com/y8wcay

The free Metasploit framework (http://www.metasploit.com) is a fairly easy-to-use exploit tool that comes preinstalled with Microsoft exploits that have at one time or another affected most CallManager 4.*x* installations (see Figure 7-11).

Additionally, as with any software product, the CallManager application itself has been prone to various security issues as exhibited by the quote at the beginning of the

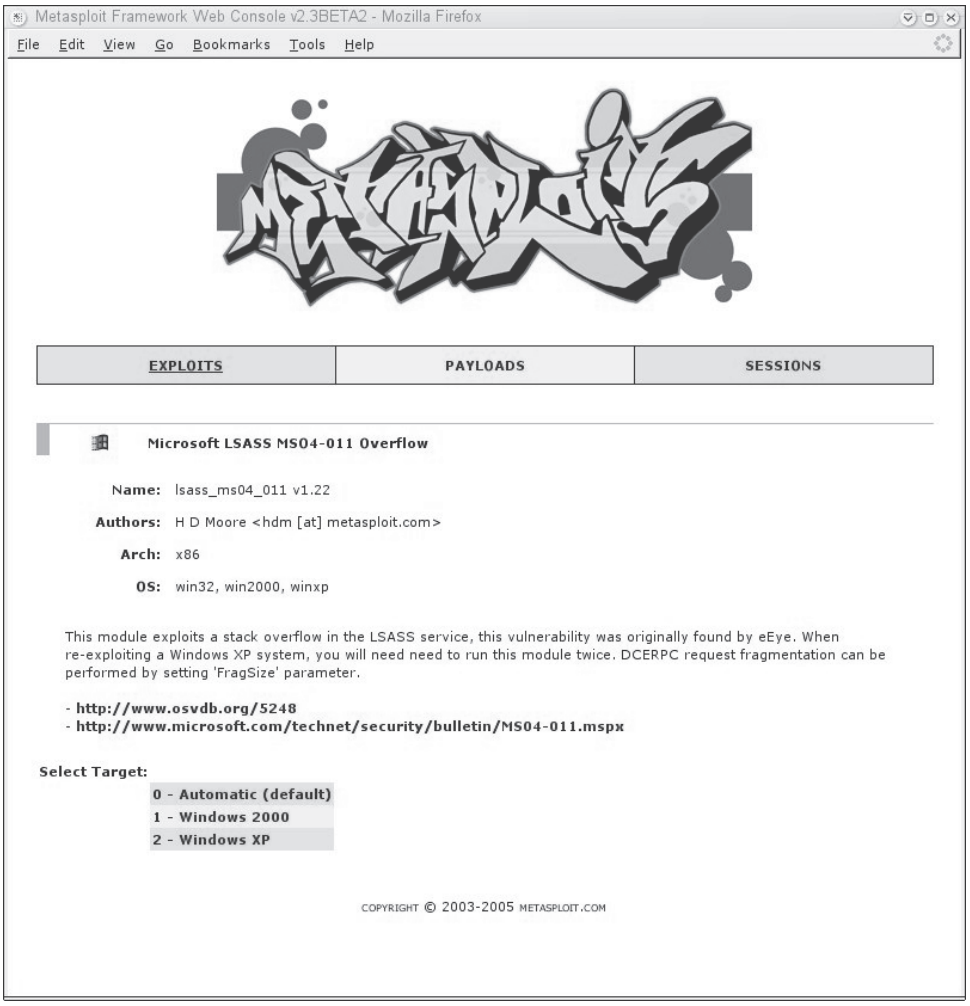

Figure 7-11 Metasploit Framework with the infamous LSASS vulnerability

chapter taken from one such advisory. All of the specific security issues that have affected CallManager 4.*x* and 5.*x* are available at "Cisco Unified CallManager Security Advisories, Responses, and Notices," http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_security_advisories_list.html.

Denial of Service (Crash) and OS Exploitation Countermeasures

The following are general strategies for mitigating new and existing vulnerabilities in the underlying operating system of CallManager.

Patch Management

Patch updating is the most important task in staying ahead of the shrinking window of time for worm and exploit releases after a new vulnerability is discovered. One of the inherent problems in relying on Cisco for updates is the slight delay incurred in packaging up the latest Microsoft bulletin patches into MCS OS upgrades (http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/osbios.htm). The three main categories for updates to CallManager include the underlying Windows OS, Microsoft SQL Server, and the BIOS updates to the MCS, which are all available from the previous link. The Cisco Voice Technology Group Subscription Tool (http://www.cisco.com/cgi-bin/Software/Newsbuilder/Builder/VOICE.cgi) is a nice notification system that will update you when a patch or software upgrade is available for your particular deployment flavor (see Figure 7-12).

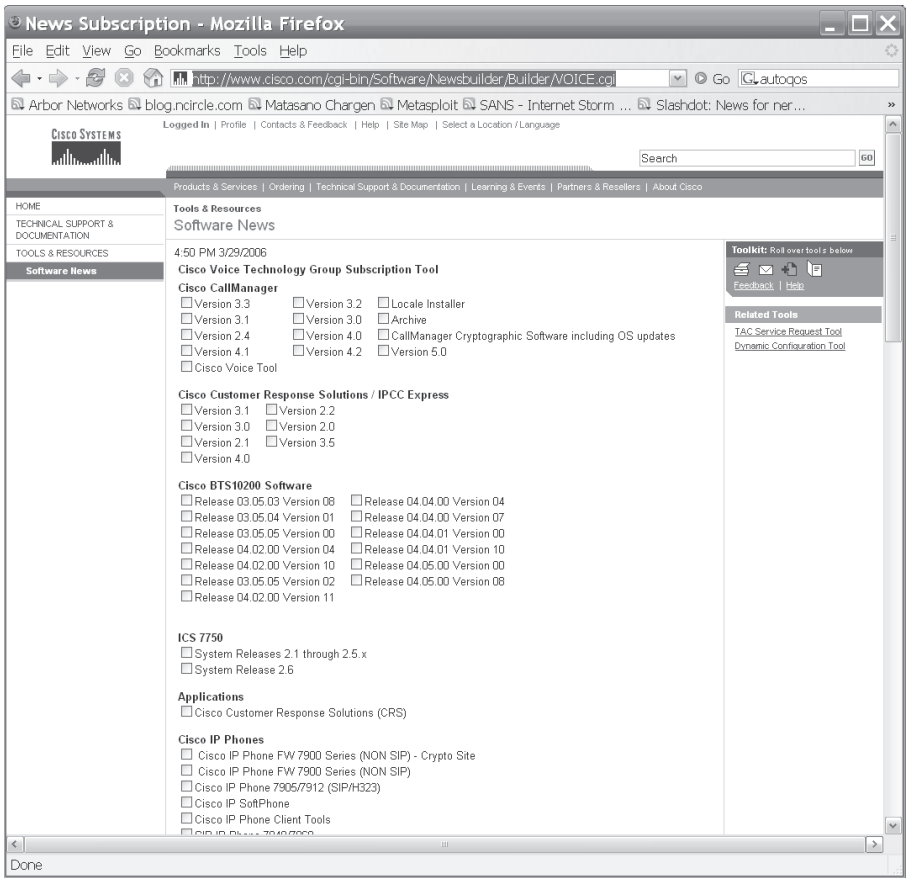

Figure 7-12 Cisco Voice Technology Group Subscription Tool

Additionally, the rest of the Cisco infrastructure (routers, switches, phones, and so on) requires constant updating. These alerts can be set using the Product Alert Tool found on Cisco's website at http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do and shown in Figure 7-13. A login is required to access this tool.

Install Cisco Security Agent and Anti-Virus on CallManager 4.*x*

Cisco acquired the host-based intrusion prevention system (HIPS) company Okena in January 2003. Okena's HIPS software product was eventually renamed to Cisco Security Agent (http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html). Cisco Security Agent (CSA) is able to prevent proactively certain types of security flaws from being exploited on a Windows host, regardless of whether or not that host has been fully patched. CSA is included free with most CallManager 4.*x* installations these days and is a useful defense-in-depth tool.

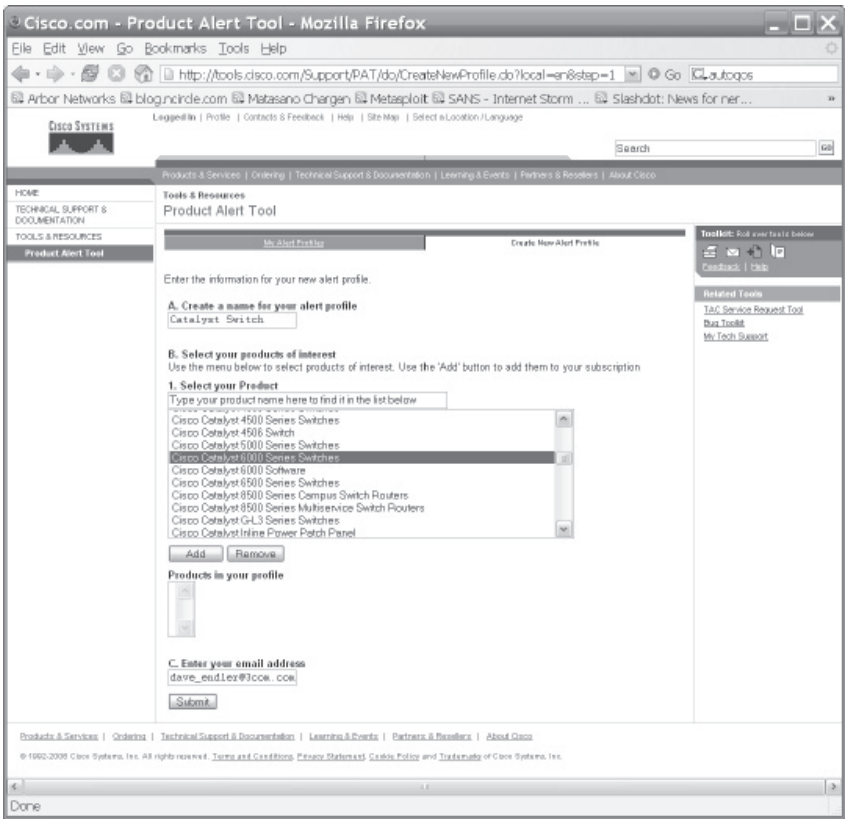

Figure 7-13 Cisco Product Alert Tool

While CSA is meant for preventing exploitation of vulnerabilities, it is not a panacea for all malware. You should also install your favorite anti-virus software on the CallManager server to prevent malware (worms, viruses, bots, and so on) from creeping in through a variety of other ways besides vulnerability exploitation (network shares, default passwords).

On Cisco CallManager 5.*x*, CSA is installed by default with the OS image.

Network-Based Intrusion Prevention

As discussed in Chapter 4, network-based intrusion prevention systems (NIPS) are inline network devices that detect and block attacks at wire speed. A NIPS can be deployed in a network in much the same way as a switch or a router, and it is one of the most effective ways to provide a "virtual patch" while you're waiting to apply a software update.

Disable IIS in CallManager 4.*x*

The Microsoft IIS web server that comes installed on Cisco CallManager 4.*x* is also connected to the FTP, web, and email services. IIS has historically been associated with numerous security issues in the past, and is best left disabled when not performing an upgrade.

Eavesdropping and Interception Attacks

Popularity:	*5*
Simplicity:	*7*
Impact:	*7*
Risk Rating:	***6***

As you hopefully remember from Chapters 5 and 6, we demonstrated a variety of attacks that took advantage of weaknesses in network design and architecture in order to eavesdrop and alter VoIP signaling and conversations. To summarize, the preliminary attacks to first gain access to sniffing the network traffic are

- Causing a switch to fail open
- Circumventing VLANs (VLAN hopping)
- ARP poisoning (man-in-the-middle)

Once an attacker has the ability to sniff or alter the network traffic, then there are a variety of VoIP application-level attacks possible including but not limited to

- Number harvesting
- Conversation eavesdropping
- Conversation modification
- DTMF reconstruction
- Call redirection

Eavesdropping and Interception Countermeasures

The following countermeasures cover these two classes of attacks by first walking through how to harden the networking fabric. Next, we'll delve into enabling encryption features across CallManager phones and servers (enabling SRTP and SCCP/TLS) to address the application layer attacks.

Cisco Switch Hardening Recommendations

Many of these recommendations are gleaned from various Cisco best practices documents. Of course, however, they all assume that you have Cisco gear to begin with.

Enabling Port Security on Cisco Switches to Help Mitigate ARP Spoofing Port security is a mechanism that allows you to allocate legitimate MAC addresses of known servers and devices ahead of time specific to each port on the switch. Thus, you can block access to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address detected is not on the preassigned list. This will help prevent ARP spoofing attacks. Some of the advantages and disadvantages to enabling port security are covered in Cisco's SRND best practices document on voice security (http://tinyurl.com/ngz330). In general, there are two types of port security, the static entry flavor and the "dynamic" learning flavor. With the dynamic type, the port can be configured to learn the correct amount of MAC addresses that are allowed on that port so that an administrator does not need to type in the exact MAC address.

Dynamically Restrict Ethernet Port Access with 802.1*x* Port Authentication Enabling 802.1x port authentication protects against physical attacks whereby someone walking around inside your organization plugs a laptop into an empty network jack in order to sniff traffic. Enabling 802.1x authentication on your switch ports obviously requires that most of your network clients support it—one of the main challenges with implementing this feature widely today.

Enable DHCP Snooping to Prevent DHCP Spoofing As you learned in Chapter 6, DHCP spoofing is a type of man-in-the-middle attack that occurs when an attacker masquerades as a valid DHCP server in order to reroute traffic to his machine. This is typically done by advertising a malicious DNS server with a valid IP address assignment. DHCP snooping is a feature that blocks DHCP responses from ports that don't have DHCP servers associated with them. You can also put static entries in the DHCP-snooping binding table to be used with Dynamic ARP Inspection and IP Source Guard (see next sections) that do not use DHCP. More information on the DHCP snooping feature is available on Cisco's site at http://tinyurl.com/oz4hw.

Configure IP Source Guard on Catalyst Switches The IP source guard (IPSG) feature uses DCHP snooping to prevent IP spoofing on the network by closely watching all DHCP IP allocations. The switch then allows only the valid IP addresses that have been allocated by the DHCP server on that particular port. This feature mitigates the ability of an attacker trying to spoof an IP address on the local segment. More information on enabling this feature is available on Cisco's site at http://tinyurl.com/oz4hw.

Enable Dynamic ARP Inspection to Also Thwart ARP Spoofing Dynamic ARP inspection (DAI) is a switch feature that intercepts all ARP requests and replies that traverse untrusted ports. The purpose of this feature is to block inconsistent ARP and GARP replies that do not have the correct MAC to IP address mapping. In turn, this prevents a man-in-the-middle attack. Some of the advantages and disadvantages to enabling DAI are covered in Cisco's SRND best practices document on voice security (http://tinyurl.com/ngz330).

NOTE You must have DHCP snooping enabled to turn on Dynamic ARP inspection (DAI) and IP source guard (IPSG). If you turn DAI or IPSG on without DHCP snooping, you will end up causing a denial of service for all hosts connected on the switch. Without a DHCP snooping binding table entry, hosts will not be able to ARP for the default gateway, and therefore, traffic won't get routed.

Configure VTP Transparent Mode The VLAN Trunking Protocol (VTP) is a Cisco protocol that enables the addition, deletion, and renaming of VLANs in your network. By default, all Catalyst switches are configured to be VTP servers and any updates will be propagated to all ports configured to receive VLAN updates. If an attacker were able to corrupt the configuration of a switch with the highest configuration version, any VLAN configuration changes would be applied to all other switches in the domain. Put simply, if an attacker compromised your switch with the central configuration on it, she could delete all VLANS across that domain. To alleviate this threat, you can configure switches not to receive VTP updates by setting the ports to VTP transparent mode (see http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_20/config/vtp.htm#wp1020711).

Change the Default Native VLAN Value to Thwart VLAN Hopping Most switches come installed with a default native VLAN ID of VLAN 1. Because attackers can sometimes perform VLAN hopping attacks if they know the VLAN IDs ahead of time, it is usually a good idea to never use VLAN 1 for any traffic. Also, change the default native VLAN ID for all traffic going through the switch, from VLAN 1 to something hard to guess (see http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm).

Disable Dynamic Trunk Protocol and Limit VLANs on Trunk Ports to Thwart VLAN Hopping If a Cisco switch is set for autotrunking, an attacker can perform a VLAN hopping attack by sending a fake Cisco Dynamic Trunking Protocol (DTP) packet. In doing so, the victim switch port might become a trunk port and start passing traffic destined for any VLAN. The attacker would then able to bypass any VLAN segmentation applied to that port. To mitigate against this attack, DTP should be turned off on all switches that do not need to trunk (see http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml).

Phone Hardening Recommendations

The following is a simple procedure for removing some of the services that are enabled by default on the IP phone, as illustrated in Figure 7-14:

1. In Cisco Unified CallManager Administration, select Device | Phone.

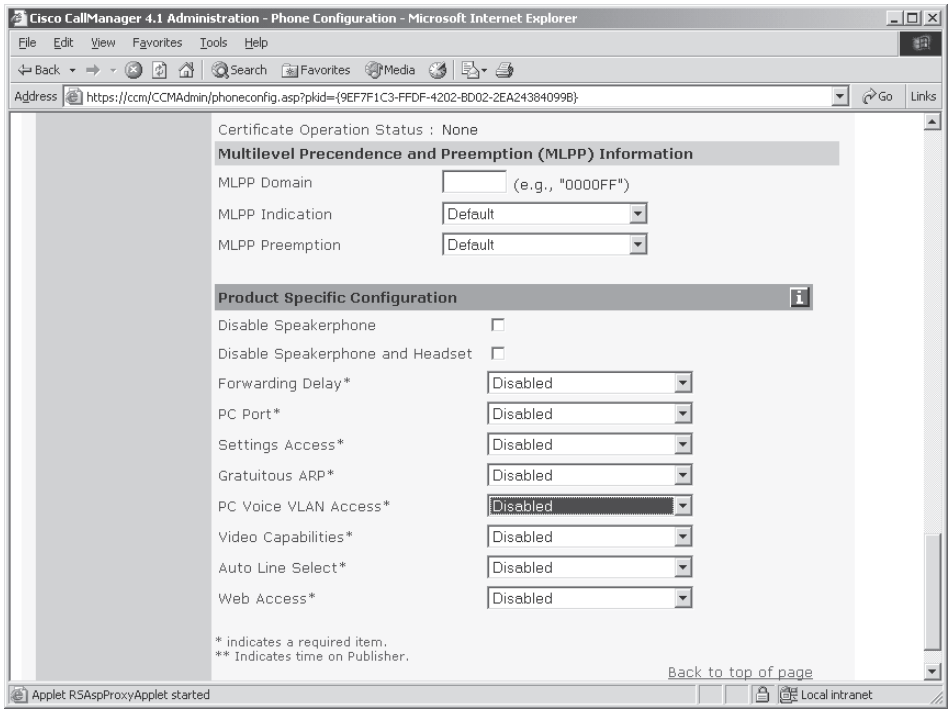

Figure 7-14 Disabling features on a Cisco hard phone

2. Specify the criteria to find the phone and click Find, or click Find to display a list of all the phones.
3. To access the Phone Configuration window for the device, click the device name.
4. Locate and disable the following product-specific parameters:
   - PC port
   - Settings access
   - Gratuitous ARP
   - PC Voice VLAN access

NOTE Disabling GARP only helps protect the phone from man-in-the-middle attacks; obviously the router and other network elements can be prone to attack as well.

Activating Authentication and Encryption

Cisco provides a detailed checklist in order to activate authentication and encryption on your CallManager and phones to ensure that the Skinny signaling sessions require

authentication and that they pass over an encrypted TLS tunnel. This also activates SRTP, (RFC 3711) which enables encryption of the actual phone conversations.

1. Activate the Cisco CTL Provider service in Cisco CallManager Serviceability on each server in the cluster (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuauth.htm#wp1054915 *or* http://tinyurl.com/y4ecgh).
2. Activate the Cisco Certificate Authority Proxy service in Cisco CallManager Serviceability to install, upgrade, troubleshoot, or delete locally significant certificates on the publisher database server (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secucapf.htm#wp1082177 *or* http://tinyurl.com/yyprse).
3. Configure ports for the TLS connection if you do not want to use the default settings (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuauth.htm#wp1028905 *or* http://tinyurl.com/y8dmf5).
4. Obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the Cisco CTL client (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuauth.htm#wp1029015 *or* http://tinyurl.com/sfvbb).
5. Install the Cisco CTL client (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuview.htm#wp1028867 *or* http://tinyurl.com/y7ds78, http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuview.htm#wp1029357 *or* http://tinyurl.com/w7vj7, and http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuauth.htm#wp1028944 *or* http://tinyurl.com/vbpn6).
6. Configure the Cisco CTL client (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuauth.htm#wp1029015 *or* http://tinyurl.com/sfvbb).
7. Configure CAPF to issue certificates (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuview.htm#wp1028867 *or* http://tinyurl.com/y7ds78, http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secucapf.htm#wp1082192 *or* http://tinyurl.com/yle4rt, and http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secucapf.htm#wp1067959 *or* http://tinyurl.com/ycjcyj).
8. Verify that the locally significant certificates are installed on supported Cisco IP phones (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuview.htm#wp1028867 *or* http://tinyurl.com/y7ds78, http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secucapf.htm#wp1044293 *or* http://tinyurl.com/yzem45, and http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secutrbl.htm#wp1058630 *or* http://tinyurl.com/ylwcl9).

9. Configure supported phones for authentication or encryption (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuphne.htm#wp1033627 *or* http://tinyurl.com/yy6mw2).
10. Perform phone-hardening tasks (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuphne.htm#wp1028813 *or* http://tinyurl.com/y7cv49).
11. Configure voicemail ports for security (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuvmp.htm *or* http://tinyurl.com/yxwd8a).
12. Configure security settings for SRST references (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secusrst.htm *or* http://tinyurl.com/y75ldh).
13. Configure IPSec in the network infrastructure, and configure Cisco IOS MGCP gateways for security (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secumgcp.htm *or* http://tinyurl.com/y5rt2w and http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secumgcp.htm#wp1060100 *or* http://tinyurl.com/y5rt2w).
14. Reset all phones in the cluster (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuview.htm#wp1032075 *or* http://tinyurl.com/yes4e3).
15. Reboot all servers in the cluster (*see* http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuview.htm#wp1032075 *or* http://tinyurl.com/yes4e3).

For more details on any of these specific steps, we recommend reading *Cisco CallManager Best Practices* by Salvatore Collora (Cisco Press, 2004).

SUMMARY

Cisco is one of the few vendors that actually manufactures most of the networking infrastructure that supports their VoIP phones and servers. Correspondingly, there are a variety of checklists, tools, and best practices available from Cisco to ensure that your VoIP deployment is hardened to the most prevalent attacks.

REFERENCES

References are included throughout the chapter.