Moving from concepts to real solutions: Vulnerability Analysis and Best Practices for Adopting IP Communications

INTRODUCTION

The same IP technology that enables IP Communications to boost productivity, increase mobility and enhance flexibility can create manageable challenges to information security. These challenges exist whether the update is incremental or total. When appropriate security measures are taken, IP Communications can be as secure, or even more secure than traditional circuit-switched systems. Critical to this security is a systemic approach, taking into account both IP Communications technologies and traditional network security techniques. This paper describes issues relative to IP Communications security and the tools, techniques and technologies available from Cisco to mitigate the issues raised. The intent is to provide organizations examples of real-world solutions which can help them build secure IP Communications environments.

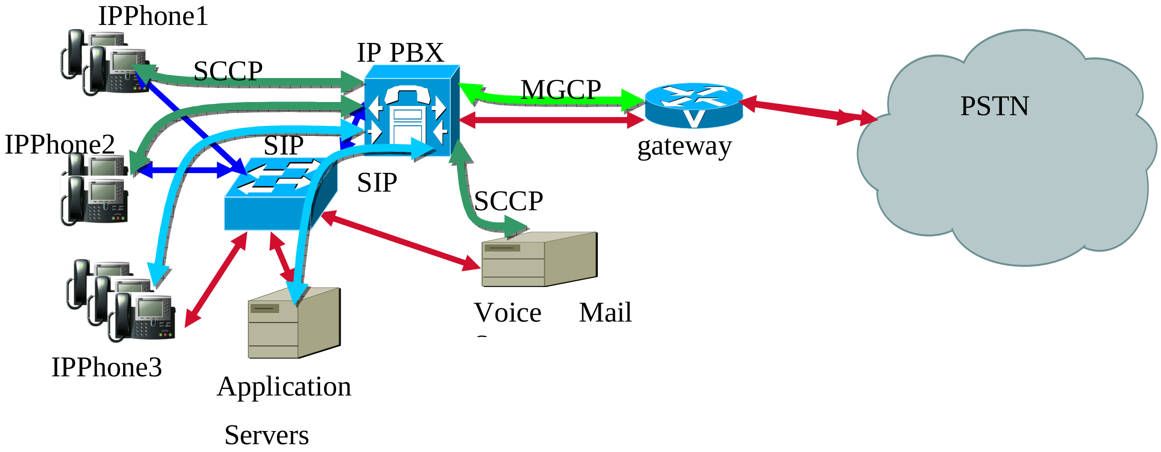


Figure 1: Example of an IP Communications setup in a typical organization

THE POTENTIAL THREATS

Threats to an IP Communications network depend on the specific manner in which the network is designed and deployed. In this section we discuss potential security issues and use these to build a foundation for a discussion on how these threats can be mitigated. This work is not meant to be an exhaustive risk assessment nor a framework for how one would thoroughly protect a specific IP Telephony system. A threat assessment for a given IP Telephony system would depend on a number of attributes specific to that particular system.

In the business communications world, threats to IP Communications are much the same as with TDM PBXs, but take a somewhat different form. With a traditional phone system, to eavesdrop on a call, an intruder typically had to have physical access to the phone line in order to attach a tapping device. Given the ubiquitous nature of the Internet Protocol (IP), unprotected IP-based phone conversations could theoretically be tapped from anywhere in the symmetrical path of packets traversing the network. IP-based systems are also subject to the same threats as data networks, including viruses, worms, password attacks, and DoS attacks.

Fortunately, many of the same principles, tools, and techniques used to protect data networks apply to voice systems. With IP-based systems, time-tested tools such as firewalls, VPNs, encryption, QoS, compartmentalization, AAA (Authentication, Authorization, and Audit/Accounting), multilevel redundancy, and high availability can be extended and used to protect IP Communications.

While there are a number of types of threats that can affect IP Communications, this paper will focus on solutions for the following commonly perceived threat categories.

V1	Protocol issues
V2	Application related security issues
V3	Operating System related security issues
V4	Eavesdropping and sniffing
V5	Spoofing
V6	Unauthorized components or users
V7	Unauthorized access to system data
V8	Theft of Service
V9	Man-in-the-Middle
V10	DoS and DDoS

Table 1: Summary of Commonly Perceived IP Telephony Threats

Customized Threat Analysis

Before going into the details of what can be done to minimize the risk from potential threats, it is important to look at what an IP Communications administrator should do in order to carry out a practical analysis of the threats to his/her specific environment.

Any actionable risk assessment needs five key factors considered – a comprehensive list of threats, the inter-dependencies between the threats, the feasibility of each of the threats, the quantitative impact of each threat, and finally a prioritization of mitigation actions for each of the potential threats.

1. **Creation of a Comprehensive Threat List:** A comprehensive listing of threats is critical since missing any important potential threat/attack vector could open the system to compromise.

2. **Creation of a List of Interdependencies:** Dependencies and inter-dependencies are important – since they show how the violation of one component could lead to a chain of consequences leading to a security compromise in other components. For example, spoofing risk in a closed system first requires access to the closed system. So there must be some way for the attacker to get into the system before a spoofed attack is possible.

3. **Quantification of the Threat**: Once the breadth and dependencies have been listed, each threat needs to be checked for the actual potential risk. Many organizations and security thinkers get lost trying to plug holes in every perceived security problems when in actuality the realistic chance of that threat vector ever being used is very small. This can lead to a less than efficient utilization of resources for protecting the IP Telephony environment.

4. **Quantification of the Potential Damage:** Once a threat has been identified as being potential and feasible, it should be weighted to measure the potential damage it could cause in a specific environment. This will help in the final steps where the threats are prioritized against one another to provide a map for mitigation actions. Please see ‘Note 3’ in the section of the document titled ‘additional notes’ for a more detailed discussion on how threat quantification may be done.

5. **Prioritization of Mitigation Work:** It is important to come up with a prioritized list of threat mitigation activities to undertake based on the above analysis for the given IP Telephony environment.

Listed above are the basics of any effective security risk assessment. Many security risk assessment methodologies include these steps in some manner. What is important is that a documented and repeatable methodology be created that others can review, compare, and execute.

Protecting against the threats

This section discusses various security features found in Cisco products. The focus is on providing clear mappings between the threats identified in the previous section and the security features in the products that protect against those threats.

1. Bootup Security enhancements

Cisco IP phones use TFTP during their boot process. Cisco has made significant security enhancements to safeguard the TFTP-based IP phone during the bootup process. TFTP in and of itself is a very simple protocol, and does not have security built into it. However, it is a protocol which has great value in an IP Telephony environment since it provides a very light-weight method for IP Phones to obtain initial images and configurations. Therefore, Cisco uses TFTP and provides object-level security of images and configuration files by utilizing the following:.

Signed Firmware Images: Phone images are digitally signed using Cisco's private key.

Signed Configuration Files: Configuration files are digitally signed using the private key of the CallManager.

The above mechanisms ensure that TFTP can be used for file download in the IP Telephony environment without security risk.

Further details on this topic can be had by reading the following topics in the chapter titled "Authentication, Integrity, and Encryption" in the document, "Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)"

Image Authentication

Device Authentication

File Authentication

(http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00801ed394.html

Here is a sample from the above chapter discussing the process IP phones follow to ensure security:

"If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in .sgn format. If none of the TFTP servers has a certificate, the phone requests an unsigned file.

The TFTP server does not sign any files if you configure the cluster for nonsecure mode. The TFTP server signs static files, such as ring list, localized, default .cnf.xml, and ring list wav, files in .sgn format. The TFTP server signs files in <device name>.cnf.xml format every time that the TFTP server verifies that a data change occurred for the file.

The TFTP server writes the signed files to disk if caching is disabled. If the TFTP server verifies that a saved file has changed, the TFTP server re-signs the file. The new file on the disk overwrites the saved file that gets deleted. Before the phone can download the new file, the administrator must restart affected devices in Cisco CallManager Administration.

After the phone receives the files from the TFTP server, the phone verifies the integrity of the files by validating the signature on the file."

These enhancements protect against the following list of security threats discussed earlier:

V1: Protocol related security issues (security enhancements for TFTP file manipulation)

V5: Spoofing (by allowing only verifiable devices to connect to a IP Telephony network)

V7: Unauthorized access to system data (by allowing only verifiable devices to connect to a IP Telephony network)

V10: DoS and DDoS (by preventing attachment of malicious devices to a IP Telephony network)

2. DHCP Security Enhancements

Enterprise and some SP IP Telephony systems depend on DHCP for various functions. While not directly related to IP Telephony security, violation of the DHCP service would create potential vulnerabilities in the IP Communications system. Cisco Ethernet switches have the ability to stop a number of well-known weaknesses in DHCP from being exploited[1]. In Cisco Catalyst switches the DHCP snooping feature is provided to:

Prevent Rogue DHCP Server Attacks

Prevent DHCP Starvation Attacks

Record Binding Information for limiting ARP responses for only those addresses that are DHCP-bound

Each of these well-known weaknesses require access to the collision/broadcast dominate to be effective. For example, someone connected to one Ethernet switch will not be able to impact another Ethernet switch if these two Ethernet switches do not share the same broadcast domain.

For details, please see the related sections about DHCP Snooping in the chapter titled, "Voice Security," in the document, "Cisco Unified Communications SRND Based on Cisco Unified CallManager 5.0" (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a008063742b.html).

Here is a quote from the above chapter for ready reference:

"When enabled, DHCP Snooping treats all ports in a VLAN as untrusted by default. An untrusted port is a user-facing port that should never make any reserved DHCP responses. If an untrusted DHCP-snooping port makes a DHCP server response, it will be blocked from responding. Therefore, rogue DHCP servers will be prevented from responding. However, legitimately attached DHCP servers or uplinks to legitimate servers must be trusted."

DHCP address scope starvation attacks from tools such as Gobbler are used to create a DHCP denial-of-service (DoS) attack. Because the Gobbler tool makes DHCP requests from different random source MAC addresses, you can prevent it from starving a DHCP address space by using port security to limit the number of MAC addresses. However, a more sophisticated DHCP starvation tool can make the DHCP requests from a single source MAC address and vary the DHCP payload information. With DHCP Snooping enabled, untrusted ports will make a comparison of the source MAC address to the DHCP payload information and fail the request if they do not match."

Another function of DHCP Snooping is to record the DHCP binding information for untrusted ports that successfully get IP addresses from the DHCP servers. The binding information is recorded in a table on the

Cisco Catalyst switch. The DHCP binding table contains the IP address, MAC address, lease length, port, and VLAN information for each binding entry. The binding information from DHCP Snooping remains in effect for the length of the DHCP binding period set by the DHCP server (that is, the DHCP lease time). The DHCP binding information is used to create dynamic entries for Dynamic ARP Inspection (DAI) to limit ARP responses for only those addresses that are DHCP-bound. The DHCP binding information is also used by the IP source guard to limit sourcing of IP packets to only those addresses that are DHCP-bound."

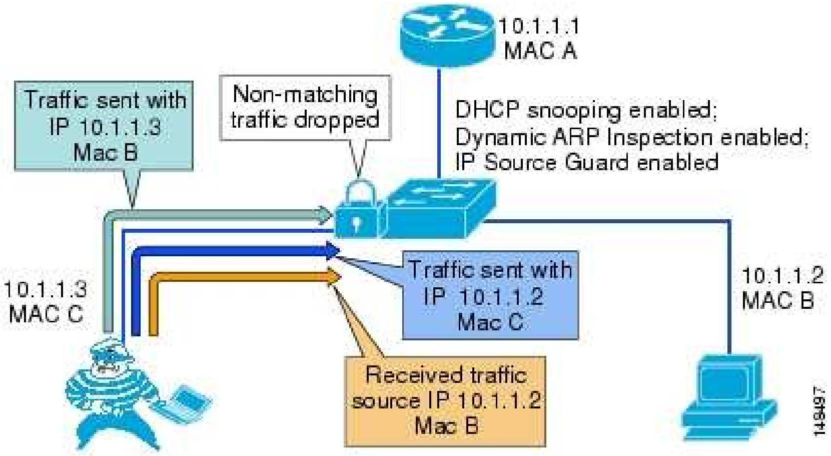


Figure 2: Preventing Address Spoofing

These enhancements protect against the following list of security threats listed in the previous section:

V1: Protocol Related Security Issues (security enhancements through DHCP protective mechanisms)

V5: Spoofing (security enhancements by switch security enhancements mapping mac addresses to specific ports)

3. HTTP Security Enhancements

Various enhancements are used in practice to secure HTTP transactions. Security mechanisms for enhancing HTTP are supported by Cisco in various products. Examples of such enhancements include: HTTPS, HTTP authentication/authorization.

The Cisco CallManager provides HTTPS for secure administration. More detail on this implementation can be found in the HTTPS section in the chapter, "Introduction" in the document, "Cisco CallManager Administration Guide, Release 4.1(3)" (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed648.html)

Here is a quote from this chapter describing the usage of HTTPS in the Cisco IP Telephony environment:

"Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the IIS server, uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS also ensures that the user login password transports securely via the web. The following Cisco CallManager applications support HTTPS, which ensures the identity of the server: Cisco CallManager Administration, Cisco CallManager Serviceability, the Cisco IP Phone User Option Pages, the Bulk

Administration Tool (BAT), TAPS, Cisco CDR Analysis and Reporting (CAR), Trace Collection Tool, and the Real Time Monitoring Tool.

When you install/upgrade Cisco CallManager, the HTTPS self-signed certificate, httpscert.cer, automatically installs on the IIS default website that hosts the Cisco CallManager virtual directories, which include CCMAdmin, CCMService, CCMUser, AST, BAT, RTMTReports, CCMTraceAnalysis, PktCap, ART, and CCMServiceTraceCollectionTool. The HTTPS certificate gets stored in the C:\Program Files\Cisco\Certificates directory. If you prefer to do so, you can install a server authentication certificate from a certificate authority and use it instead of the HTTPS self-signed certificate. To use the certificate authority certificate after the Cisco CallManager installation/upgrade, you must delete the self-signed certificate, as described in the Cisco CallManager Security Guide. Then, you install the server authentication certificate that is provided by the certificate authority, as described in the certificate authority documentation."

These enhancements protect against the following list of security threats listed in the previous section:

V1: Protocol Related Security Issues (security enhancements through HTTP protective mechanisms)

V4: Eavesdropping and sniffing (through encryption in HTTPS)

V5: Spoofing (through in-built security mechanisms in HTTPS)

V7: Unauthorized access to system data (through encryption in HTTPS)

V9: Man-in-the-Middle (through in-built security mechanisms in HTTPS)

4. IP Telephony Specific Protocol security enhancements

Cisco contributes to enhancements of various IP Telephony protocols in multiple standards development organizations. Current standards work in the area of SIP security is an example of Cisco leadership.

One Cisco white paper, titled "Security in SIP-Based Networks**"**, explores various network security threat models faced by today's SIP-based voice networks, and describes network security solutions based on Cisco SIP-enabled products. For more information, please refer to the link, http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml.

The leadership that Cisco provides in the standards space is reflected very well in its products.

Cisco provides multiple SIP-enabled products for supporting evolving security enhancements. Here is a list of links concerning security for SIP-based systems:

Cisco IOS SIP Gateway Signaling Support Over TLS Transport. (http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080614052.html)

SIP Phone Security Profile Configuration. (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a008063323b.html#wp1017512)

New Security, Scalability and Desktop Enhancements for Cisco SIP-Supported Customer Contact Solutions. (http://newsroom.cisco.com/dlls/2005/prod_062005d.html)

SIP Trunk Security Profile Configuration. (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a0080633287.html)

Cisco's work in improving the H.323 protocol's security framework is also worth mentioning: Cisco supports security extensions in H.323, especially H.235, for enhancing H.323-based environments. Here is a list of important Cisco solutions in this space:

Cisco H.323 Gateway Security and Accounting Enhancements. (http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a0080087acd.html)

Enabling H.323 Clear Text Authentication on an ATA Registered with Gatekeeper. (http://www.cisco.com/en/US/products/hw/gatecont/ps514/products_tech_note09186a008011b5ee.shtml)

Cisco provides security extensions to MGCP gateways. The chapter, "Configuring a Secure MGCP Gateway," in "Cisco CallManager Security Guide," outlines these extensions. For more information, please see (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803fe67b.html).

These enhancements protect against the following security threat:

V1: Protocol Issues (ongoing IP Telephony protocol security enhancements through a concerted and in synch standardization and productization effort)

5. Identity Enhancements

Establishing identity and then using it to improve network security a fundamental element of Cisco's approach to security. Identity related enhancements occur in a number of areas within Cisco's IP Communications solution.

5.1 Device Identification:

Cisco provides a number of enhancements in the IP communications environment to ensure that the identity of various components can be established and protected. Some of the most significant enhancements are outlined below:

Public key/private key pairs for call managers, other servers, as well as the IP phones: Every device generates its own pair so the private key NEVER crosses the wire. These pairs are subsequently used for creating signatures and become the basis for the provisioning of certificates in the system. Administrative access to CallManager is protected by a password and aspects of its provisioning are also protected by a physical eToken.

X.509v3 digital certificates: These are used in the telephony environment for establishing a device's identity, used to share a device's public key. These are signed by a trusted certificate authority. The call manager generates its own self signed certificate during installation. IP phones are available which come installed with a MIC (manufacturing installed certificate) which can be augmented by customer-authorized, site specific certificates using a separate public/private key pair. Authentication and Identity in Cisco CallManager are accomplished through a combination of the phone's identity and the phone's certificate, and the mutually-authenticated TLS connection from the phone to CallManager.

Certificate trust list: This is a digitally signed file held by every endpoint in the IP Communications system. It contains the roles, identities, and certificates of devices the endpoints should trust, including Cisco CallManagers, TFTP configuration file signers, and CAPF servers. The file is administratively created by using the CTL client **— a** plug-in downloadable from Cisco CallManager admin webpages. The file is signed using the private key of a Systems Administrator Security Token held by the network administrator. Identical CTL files are downloaded to every IP phone during the TFTP process. After the initial provisioning of this CTL file into the phone, subsequent CTL files, images, and configuration files are all validated using the public key contained in the existing CTL file. Any image, configuration file, or CTL file that fails validation is not used by the phone. Note that the Cisco CallManager uses whitelists for authorizing endpoints with the connection to CallManager, which can eliminate reliance on a certificate authority and eliminates the need to contact a CA in realtime or to keep the CRL (Certificate Revocation List) updated.

For more information, refer to:

"Authentication, Integrity, and Encryption" in "Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)" (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00801ed394.html);

"Certificate Authority Proxy Function" in "Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)" (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00802e4706.html); and

"Cisco CallManager Express Security for IP Telephony" in "Cisco CallManager Express Security Guide to Best Practices" (http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html#wp40225)

5.2 Forced Authorization Codes (FAC) and Client Matter Codes (CMC)

Forced Authorization Codes (FAC) and Client Matter Codes (CMC) allow management of call access and accounting. CMC assists with call accounting and billing for billable clients, while Forced Authorization Codes regulate the types of calls that certain users can place.

Client Matter Codes force the user to enter a code to specify that the call relates to a specific 'client matter code'. One can assign client matter codes to customers, students, or other populations for call accounting and billing purposes.

The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes, similar to a personal calling card.

For details, see: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803f3af7.html#wp1052254.

5.3 Layer 2 Identity Enhancements

Cisco recommends following a well defined set of best practices which allow data and voice traffic to be segregated on Layer 2. This is a fundamental design concept allowing for a reduction in the number of security issues from arising if voice segments were exposed to data segments. Please refer to Catalyst switch configuration guides for more details on how to setup VLANs. Below is a link on how to set up VLANs on the catalyst 6500 switch.

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/vlans.htm

There are number of security features available in Cisco switches to thwart various types of man-in-the-middle attacks which depend on an adversary assuming the identity of another device on the local area network. Two of these features are especially worth considering. Please note that both these features make use of the DHCP Snooping feature discussed in section 2 of this paper:

5.3.1 Dynamic ARP Inspection: Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports

- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination

- Drops invalid ARP packets

"Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid." Please see the following link for a more detailed discussion of this feature:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sec/3750scg/swdynarp.htm

5.3.2 IP Source Guard: "IP source guard prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, a port access control list (PACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP server; any IP traffic with a source IP address other than that in the PACLs permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address." Please see link below for a more detailed discussion of this feature:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_4/confg_gd/dhcp.htm#wp1083306

5.4 Access Control Server

Cisco Secure Access Control Server (ACS) Solution Engine is a highly scalable solution for providing multiple management functions in IP Communications. ACS Solution Engine is a highly scalable, 1–rack unit dedicated platform that serves as a high-performance access control server supporting centralized RADIUS or TACACS+. The Cisco Secure ACS Solution Engine provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. The solution engine helps ensure enforcement of assigned policies by allowing network administrators to control:

- Who can log into the network

- Privileges associated to each user

- Security audit or account billing information

- Access and command controls for each configuration's administrator

Cisco Secure Access Control Server (ACS) provides dynamic, user-based ACLs that specify actions that individual users are allowed to take. This can be used to 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).

For more information, please refer to Cisco Secure Access Control Server Solution Engine (http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html)

The enhancements in section 5 provide elements of protection against the following list of security threats:

V5: Spoofing (Strong identity deters attempts adversarial attempts to assume identity)

V6: Unauthorized components or users (Strong identity management ensures that components and users with verifiable identity can join the system. In addition the CMC prevents this type of event as well)

V7: Unauthorized access (Strong identity ensures that only authorized users and devices have access to various elements of data)

V8: Theft of service (Tying services to identity ensures protection against theft of service. In addition the FAC helps prevent theft of service as well)

V9: Man in the Middle Attacks (Through strong identity measures in general as well as through the use of Dynamic Arp Inspection and IP Source Guard features)

V10: DoS and DDoS (With the help of CMC and FAC)

6. Encryption enhancements in the Cisco CallManager

Both signaling encryption and media encryption protect the privacy of IP Telephony calls. Signaling encryption ensures that information pertaining to the parties - DTMF digits, call status, media encryption keys, and so on - are protected against unintended or unauthorized access. Media encryption ensures that only the intended recipient can interpret the media streams.

In Cisco CallManager, signaling encryption ensures that all signaling messages sent between the device and the Cisco CallManager server are encrypted. Signaling encryption is supported through TLS with mutual authentication. IP phones, using identity mechanisms listed in previous sections, can establish TLS connections with their CallManager and redundant CallManagers. This allows for signaling to be encrypted between IP phones and the CallManager. The TLS sessions use AES-128 as the encryptor with HMAC-SHA-1 as the authentication/integrity mechanism. Between the CallManager and the IP Gateways, signaling is protected using IPSec. The encryptor for the IPSec sessions is 3DES with HMAC-SHA-1 as the authentication/integrity validation mechanism.

Media encryption, which uses SRTP, ensures that only the intended recipient can interpret the media streams between supported devices. Media encryption includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport. Each session has a unique key. SRTP supports the AES-128 encryption algorithm and is an IETF RFC 3711 standard. In the Cisco CallManager (CCM) solution, SRTP is supported in the CallManager and multiple other devices, such as:

- IP phones

- Voice gateways (Cisco Integrated Services Routers)

- Voice mail servers

For further details, please see:

"Authentication, Integrity, and Encryption" in Cisco IP Phone Authentication and Encryption for Cisco CallManager (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00801ed394.html)

"Cisco CallManager Security Guide," (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803fe67b.html)

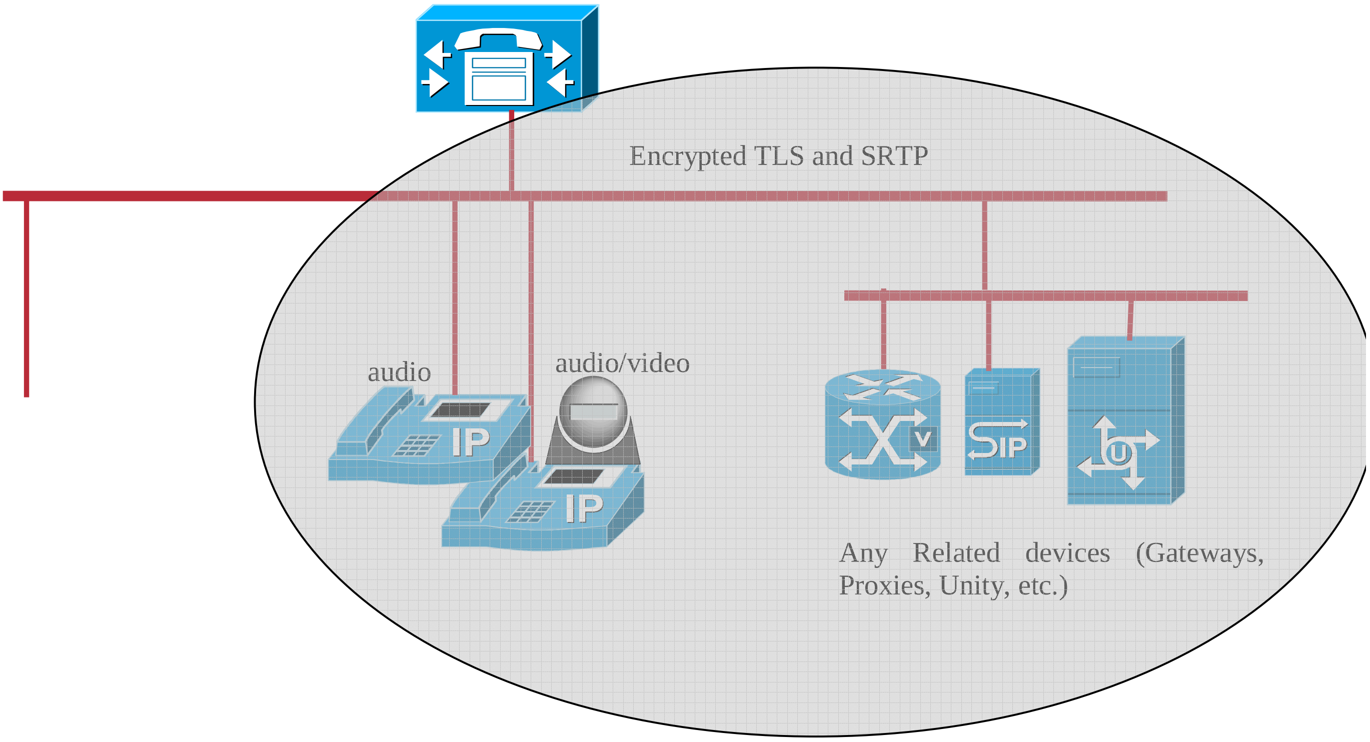
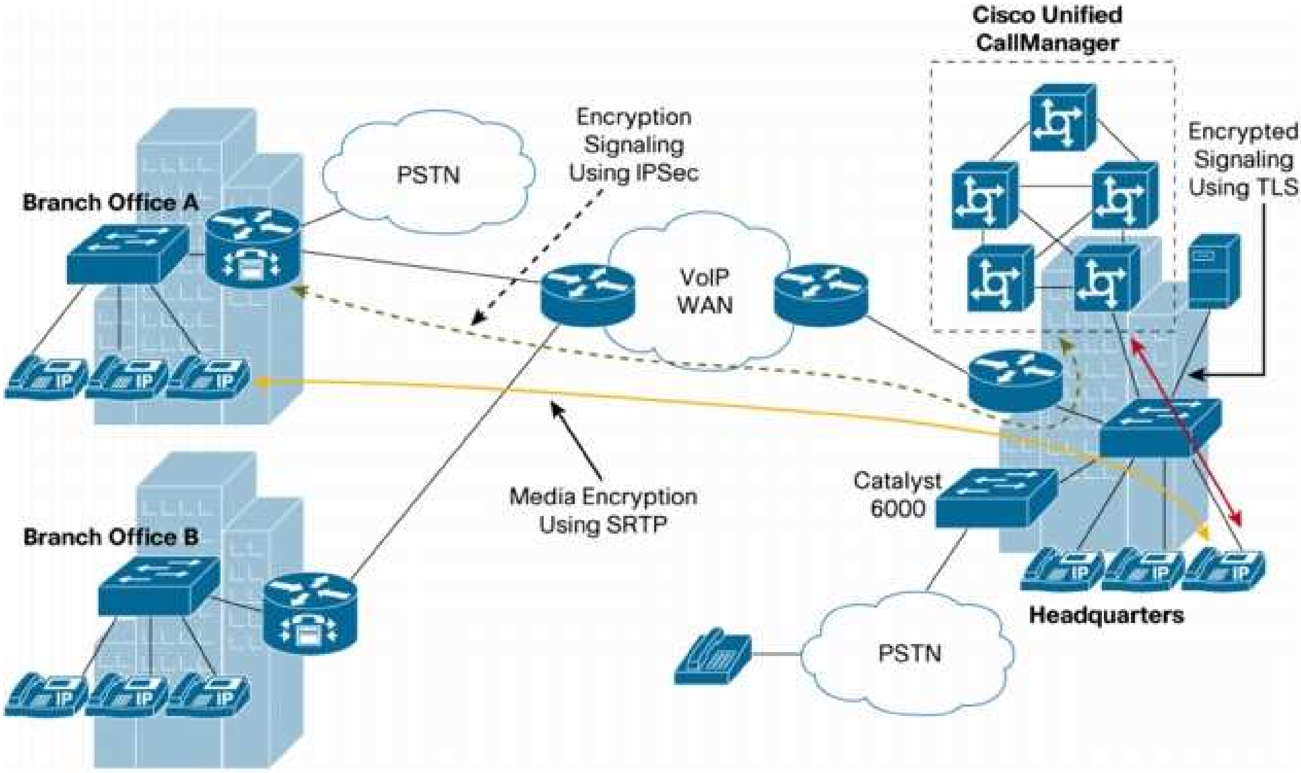


Figure 3: Example of encryptions in Cisco Call Manager

Similarly, voice gateways such as Cisco Integrated Service Routers (3800, 2800, and 1800) support both media and signaling encryption. Media encryption using Secure Real-Time Transport Protocol (SRTP) delivers protection by encrypting the voice conversation, rendering it unintelligible to internal or external eavesdroppers who have gained access to the voice domain. .

Media encryption on Cisco routers works together with Cisco Unified CallManager software and the media encryption feature on Cisco Unified IP phones to secure both gateway-to-gateway calls and IP phone-to-gateway calls. This enables secure analog phone calls or secure calls between an IP phone and the gateway, depending on the gateway interface type the media is terminated on. Voice encryption keys derived by Cisco Unified CallManager are securely sent by encrypted signaling path to Cisco Unified IP phones through the use of Transport Layer Security (TLS) and to gateways over IP Security (IPSec) protected links.

Media encryption features on Cisco routers are available beginning with Cisco IOS® Software release 12.3(11)T2 and with an upgrade to the Advanced Enterprise Services and Advanced IP Services IOS Software Feature Sets. The features are enabled on digital signal processing modules (DSPs) available on the PVDM2, EVM-HD, NM-HD-, AIM-VOICE and NM-HDV2 voice gateway network modules.



Cisco Unified CallManager
Encrypted Signaling Using TLS
Encryption Signaling Using IPSec
PSTN
Branch Office A
VoIP WAN
IP
Media Encryption Using SRTP
Catalyst 6000
Branch Office B
Headquarters
PSTN

Figure 4: Media Authentication and Encryption in Cisco ISR Routers

For more information, Please refer to “Secure Voice on Cisco Multiservice and Integrated Services Routers,” in “Cisco 3800 Series Integrated Services Routers” (http://www.cisco.com/en/US/products/ps5855/products_data_sheet0900aecd8016c784.html)

In addition to the above two solutions, IPSec is a widely available protocol on Cisco devices and can be used to provide layer 3 encryption services in a number of IP Telephony environments.

Encryption enhances help to defense several attacks in Table 1, including:

V4: Eavesdropping and sniffing (with the supports of sRTP and TLS for protecting the content privacy)

V5: Spoofing (through identity mechanisms inherent to the encryption protocols)

V8: Theft of Service (through strong identity of endpoints)

V9: Main the Middle Attacks (TLS and sRTP have built in mechanisms for protecting against MITM attacks)

7. Protections against application-focused threats

Attacks aimed at exploiting weakness in the security of various applications are among the threats that can potentially impact IP Telephony environments. Cisco provides built-in solutions as well as best practices for securing various applications in IP Communications environments.

For example, secure solutions for Cisco voice mail are introduced in the chapter, "Configuring Voice Mail Ports for Security," of the "Cisco CallManager Security Guide, Release 4.1(3)," (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803fe699.html).

Here is a quote from the above document which outlines some of the salient features of the security built into Cisco voicemail applications.

"Voice Mail Security Overview:

When you configure security for Cisco CallManager voice mail ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

When the device security mode equals authenticated or encrypted, the Cisco Unity TSP connects to Cisco CallManager through the Cisco CallManager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Cisco CallManager through the Cisco CallManager SCCP port. ……"

Another example of where Cisco provides enhancements to protect applications is the use of HTTPS for secure administration in the call manager. For further details, please see the related HTTPS sections in the chapter, "Introduction," of the "Cisco CallManager Administration Guide, Release 4.1(3),"

(http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed648.html)

In addition to building security within various applications, Cisco also provides products which are focused on preventing various abuses of application-layer protocols. The Application security services available on the Cisco Adaptive Security Appliance (ASA) 5500 series provide advanced application inspection and control for dynamic and reliable protection of networked business applications. These services include control of bandwidth-intensive peer-to-peer services (P2P) such as Kazaa and Instant Messaging (IM), Web URL access controls, protection and integrity validation of core business applications like database services, and numerous application-specific protections for Voice over IP (IP Telephony) and multimedia services. For more information, please see Cisco ASA 5500 Series Adaptive Security Appliances

(http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html).

Cisco Security Agent (CSA) helps reduce operational costs by identifying, preventing, and eliminating known and unknown security threats in desktops and servers. In a converged environment where there is significant reliance on the reliability of various telephony servers, this is a very important service that organizations must consider in the context of protecting the servers and PCs running softphones. The Cisco Security Agent consolidates many security functions in a single agent, providing:

- Operating-system integrity assurance

- Host intrusion prevention

- Spyware/adware protection

- Protection against buffer overflow attacks

- Distributed firewall capabilities

- Malicious mobile code protection

- Application inventory

Cisco Security Agent provides intrusion detection and prevention for the Cisco Unified CallManager, and is bundled as a standalone security agent for use with servers in the Cisco Unified CallManager voice cluster. The agent provides Windows and Linux security that is based on a tested security rules set (policy), which has rigorous levels of host intrusion detection and prevention. The agent controls system operations by using a policy that allows or denies specific system actions before system resources are accessed. CSA is also recommended to be installed on personal computers running softphones. For more information, please refer to:

Installing Cisco Security Agent for Cisco CallManager
(http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a0080242186.html)

Cisco Security Agent - Technical Support & Documentation
(http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html)

Deploying Cisco Security Agent to Windows Desktops
(http://www.cisco.com/web/about/ciscoitatwork/case_studies/security_dl1.html)

Note that several attacks in Table 1 are addressed by the solutions outlined in this section, including:

V2: Application related security issues (through the use of features incorporated in the Cisco Security Agent, Cisco Adaptive Security Appliance, and Cisco CallManager).

V3: OS related security issues (through the use of features incorporated in Cisco Security Agent)

8. OS Hardening and Protection

Cisco provides a number of enhancements for hardening and protecting various operating systems that are introduced into the IP Communications environment. This includes hardening of the IP phone OS and hardening the OS running on CallManagers. In addition to the hardening, Cisco also provides for the use of the Cisco security agent software which can protect against various types of threats targeted at operating system weaknesses. Cisco also has a product line of network Intrusion Prevention Systems (IPS) which can detect and ward off OS-focused attacks. In general, there are five types of enhancements that Cisco utilizes to safeguard against attacks exploiting OS weaknesses:

- Hardening of the OSs themselves to ensure that minimal opportunities for exploitation exist

- Using behavior-based host protection software (CSA)

- Use of network intrusion detection systems

- Best practices guides for IP telephony administrators outlining some of the practices (such as patching) which can keep OS vulnerabilities to a minimum

- Networking protections limiting access to the IP telephony servers and end points (such as through VACLS on switches and ACLS on router)

8.1 Hardened Server OS:

Cisco provides guidelines for hardening the Windows OSs on which its various telephony servers run. While the specifics of hardening vary from server to server, for the Cisco CallManager, a hardened Win2K OS or Linux appliance is shipped by default and can also be downloaded from the Cisco website as needed.

8.2 Patching and Anti-virus Software:

Cisco also recommends tested and supported Anti-virus software from McAffe, Symantec and TrendMicro to further augment the security of the OS on which its servers run. Please see following link for more information:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_bulletin0900aecd800f8572.html

Cisco wraps Important, Moderate, and Low-Security patches, as classified by Microsoft or a third-party vendor into an operating system support patch, along with any Critical patches that were posted individually. Cisco tests, then posts, the support patch on the third Tuesday of each month. Any support patches that are obsolete due to a more current patch on cisco.com will be removed. The support patches and associated README files can be found on cisco.com at:

http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des

8.3 Hardened IP Phone OS:

Cisco provides guidelines on how to harden IP phones running in its IP Communications environment. The use of these techniques, however, depends on the specific needs of each environment. Some of the possible settings changes that can be done to harden Cisco IP Phones are listed below:

- Disabling the Gratuitous ARP Setting: By default, Cisco Unified IP Phones accept Gratuitous ARP packets. Gratuitous ARP packets, which devices use, announce the presence of the device on the network. However, attackers can use these packets to spoof a valid network device. For example, an attacker could send out a packet that claims to be the default router. If you choose to do so, you can disable Gratuitous ARP in the Phone Configuration window of Cisco Unified CallManager Administration.

- Disabling Web Access Setting: Disabling the web server functionality for the phone blocks access to the phone internal web pages, which provide statistics and configuration information. Features, such as Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling the web server also affects any serviceability application, such as CiscoWorks, that relies on web access.

To determine whether the web services are disabled, the phone parses a parameter in the configuration file that indicates whether the services are disabled or enabled. If the web services are disabled, the phone does not open the HTTP port 80 for monitoring purposes and blocks access to the phone internal web pages.

- Disabling the PC Voice VLAN Access Setting: By default, Cisco Unified IP Phones forward all packets that are received on the switch port (the one that faces the upstream switch) to the PC port. If you choose to disable the PC Voice VLAN Access setting in the Phone Configuration window of Cisco Unified CallManager Administration, packets that are received from the PC port that use voice VLAN functionality will drop. Various Cisco Unified IP Phone models use this functionality differently.

- Cisco Unified IP Phone 7940 and 7960 drop any packets that are tagged with the voice VLAN, in or out of the PC port.
- Cisco Unified IP Phone 7970 drops any packet that contains an 802.1Q tag on any VLAN, in or out of the PC port.
- Cisco Unified IP Phone 7912 cannot perform this functionality.

- Disabling the Setting Access Setting: By default, pressing the Settings button on a Cisco Unified IP Phone provides access to a variety of information, including phone configuration information. Disabling the Setting Access setting in the Phone Configuration window of Cisco Unified CallManager Administration prohibits access to all options that normally display when you press the Settings button on the phone; for example, the Contrast, Ring Type, Network Configuration, Model Information, and Status settings.

The preceding settings do not display on the phone if you disable the setting in Cisco Unified CallManager Administration. If you disable this setting, the phone user cannot save the settings that are associated with the Volume button; for example, the user cannot save the volume.

Disabling this setting automatically saves the current Contrast, Ring Type, Network Configuration, Model Information, Status, and Volume settings that exist on the phone. To change these phone settings, you must enable the Setting Access setting in Cisco Unified CallManager Administration.

- Disabling the PC Port Setting: By default, Cisco Unified CallManager enables the PC port on all Cisco Unified IP Phones that have a PC port. If you choose to do so, you can disable the PC Port setting in the Phone Configuration window of Cisco Unified CallManager Administration. Disabling the PC port proves useful for lobby or conference room phones.

More details on how to make the above changes can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sec_vir/ae/sec502/secu_ph.htm

8.4 Cisco Security Agent:

A discussion of CSA has already taken place earlier in this paper. For more information, please refer to: Cisco Security Agent - Technical Support & Documentation (http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html)

Note that several attacks in Table 1 are addressed by the solutions outlined in this section, including:

V3: OS related security issues (through the use of features incorporated in CSA and CTA as well as through other OS hardening and protection measures)

9. Access Control in IP Telephony

Cisco has firewalling solutions which serve as application level gateways (ALGs) in IP Communications environments. These ALGs are able to undertake stateful inspection of IP Communications protocols. This requires the ALG to track signaling traffic and use the information gathered to build state information for allowing voice traffic to traverse the ALG.

The ALG functionality exists for the SIP, SCCP, H323 and MGCP signaling protocols. ASA Firewall, and the Firewall Service Module support this functionality. Please see the link below for further information on how ALG functionality works for various voice protocols in the PIX firewall:

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_1/conf_gd/inspect.htm

In addition to the basic access control functionality, in which media streams are allowed through an ALG based on the signaling taking place for it, Cisco voice gateways also provide additional access control features. Examples of these features include access control mechanisms based on:

- Call rate

- Time-based call blocking

- System-based admission control

- Telephone-number-based access control

These gateways can also interoperate with the 3rd parties (such as Radius servers) for better access control. For more information, please see

Call Admission Control for H.323 IP Telephony Gateways (http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800e0d4b.html)

IP Telephony Call Admission Control (http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800da467.shtml)

With reference to the threats listed in Table 1, the most notable threat addressed by the above solutions are:

V6: Unauthorized components or users (with the help of access control schemes)

V7: Unauthorized access to system data (with the help of access control schemes)

V10: DoS and DDoS (with the help of access control schemes)

10. Denial of Service Protection in IP Telephony

ACLs on the networking layer can be used to prevent inbound data packets used in DoS attacks from entering the voice VLAN. Separate ACLs are set up for inbound and outbound traffic, enabling organizations 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.

Access control lists are an important part of the toolset a network administrator has at his/her disposal to monitor and control access into an IP Communications network. However, ACLs can become a limiting factor in the performance of networking devices if they are not configured in the most optimal manner such that the most likely matches occurring towards the beginning of a search for a match through a large ACL. Judicious use of the locations where ACLs are deployed can also ensure that ACLs are only brought into use when there is a real need for traffic to be inspected against them (for example at the edge of a network versus its core). Cisco provides a number of enhancements in its networking software to ensure that the processing of ACLs does not become a bottleneck in the processing of the packets. These enhancements include those done in software as well as in hardware for processing ACLs. ACLs can also provide challenges in terms of management. Cisco provides various management tools for taking care of this issue. These management tools can provide visual elements for creating and maintaining ACLs.

Cisco switches provide for identity enhancements on the 2nd layer, in which a port does not turn on for data traffic 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.

Cisco routers and switches support several types of IP and MAC anti-spoofing features. Theses range from Radius based ACLs, to uRPF Strict mode, DHCP Snooping, and IP SourceGuard. Each of these Cisco innovations validates the source address of the packet and in two of these cases also checks the MAC address of the sender. This insures devices connect to the network within the scope of the administrative security policy and minimizes the impact of violated computers spewing out spoofed packets. Please see the following link for more information on how to setup URPF. The other features have previously been discussed in this document. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm

Cisco Voice Gateways serving as Application level gateways can provide intelligent access control by inspecting the rate of call establishment occurring in the signaling traffic passing through them. Through configuration of this feature, based on an established rate of call establishment in a given IP Telephony environment, DOS attacks resulting in higher call rates can be recognized and managed.

In addition to all the above tools and techniques, careful network design can go a long way towards thwarting DOS attacks. Separation of voice and data traffic at the 2nd layer through VLANs and PVLANs and the use of designs which limit access to various portions of a network on a need only basis are examples of such design elements.

With reference to the threats listed in Table 1, the most notable threat addressed by the above solutions are:

V5: Spoofing (through unicast RPF)

V6: unauthorized components or users (with the help of ACLs)

V7: unauthorized access (with the help of ACLs)

V10: DoS and DDoS (through the techniques listed above)

11. Additional Notes

Note 1: Multimedia Internet KEYing (MIKEY) is one proposed approach to providing key distribution and management (RFC 3820) for SRTP. It has a mandatory requirement to implement the MIKEY-RSA mechanism which requires both endpoints to have a means to access each other's public keys. However there doesn't exist a standard mechanism to obtain such keys especially across administrative domains (such as between enterprises) and this can be further complicated by trust chains that don't involve a mutually-trusted certificate authority.

Cisco uses Security Descriptions, draft-ietf-mmusic-sdescriptions, to exchange SRTP keys for MGCP-controlled endpoints and a very similar mechanism to distribute keys between SCCP-controlled endpoints.

Note 2: It is worth mentioning that IP Communications may be deployed in a number of disparate environments. In some scenarios, the IP PBX is a replacement for a legacy PBX and nothing more, which means the IP PBX shares the exact same connectivity to the PSTN as the legacy PBX. In the future, it's expected these IP PBX islands will be interconnected directly without going through the PSTN, but this has yet to be been done in large scale. In other scenarios, an IP PBX may be connected to potentially hostile networks such as other organization's IP PBXs, the Internet, or places where organizations cannot control the end systems, end users, or the network. All these varying scenarios require varying levels of security control.

It is conceivable that some deployments, such as an IP Tandem setup, described below, may remove the susceptibility to most of the security issues cited in this document.

Note 3: Quantifying Threats: Threats need to be quantified and qualified to be real in a given environment. Perceived Threats need to undergo a complete analysis in order for them to become useable as part of a mitigation strategy. What follows is one model of quantifying the threat.

Potential Attack Vector: If one can logically walk through on paper that a threat might exist, it is considered a potential attack vector. In other words, the attack vector is a possibility, but its existence has not yet been proven. It is latent. It is a *potential problem* which typically means it has never been demonstrated in controlled conditions in a lab. This also means that the potential attack vector is not an exploited attack vector.

Feasible Attack Vector: If one has tested the avenue of attack in a lab to demonstrate that it can be done, then it is classified as a feasible attack vector. Feasible attack vectors can be exploited – if the conditions are conducive for exploitation. Hence, just because an attack vector is feasible, it does not mean that it is an attack vector that can be exploited. Exploitability means that a miscreant can successfully use it and not break the first two core principles of the miscreants (don't get caught and don't work too hard).

Exploitable Attack Vector: An attack vector that could be used by a miscreant, criminal, BOTNET, Worm, or any other condition that would intentionally, collaterally, or unintentionally disrupt the system. Exploitable attack vectors can be done from off net or after a first stage attack (i.e. like breaking into a device). Both need to be explained, since a first stage attack is a dependency for the exploitability of the attack vector.

Active Exploit: An attack vector used by the miscreant community to attack, penetrate, violate, etc. systems.

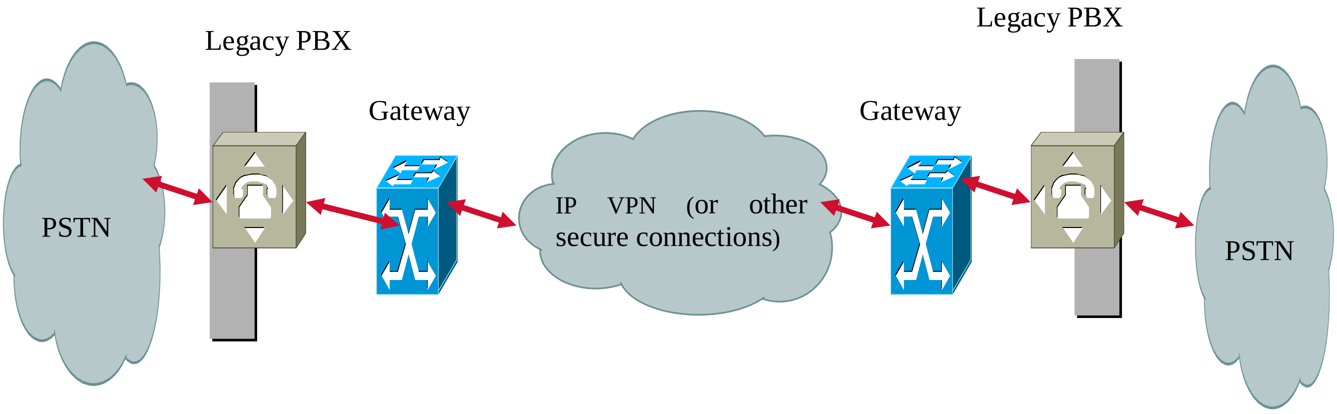


Figure 5: An IP Telephony Tandem Setup

Note 4: ALGs and SBCs share a significant shortcoming -- that they be aware of the signaling protocol and allow "good packets" while blocking 'bad packets". As SIP is still evolving, it is difficult for either an SBC or an ALG to stay abreast of the SIP's changes. Thus, both products require frequent updating and any lags in such updating by vendors or by customers will result in interoperability issues, including failed calls, between endpoints that have implemented new SIP features.

13. Resources

Cisco white paper, Security for IP Communications: Integrated Across the Network (http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_audience_business_benefit09186a008033a411.html)

Cisco White Paper, CallManager Express Security Guide to Best Practices (http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html#wp40225)

Cisco White Paper, “Security in SIP-Based Networks”, briefly describe DoS and how to deal with DoS. For more information, please refer to the link (http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml)

Cisco IP Telephony Solution Reference Network Design (SRND) for Call Manager 4.0 and 4.1

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00805fdb7b.html

Cisco IP Telephony Solution Reference Network Design (SRND) for Cisco CallManager 5.0 (http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_chapter09186a008063742b.html)

Cisco Unity Security Guide (With Microsoft Exchange), Release 4.x, (http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_administration_guide_chapter09186a0080442f6a.html)

14. Authors

Feng Cao and Saadat Malik are the primary authors of this document with substantial contributions from others including Dan Wing, Troy Sherman, Barry Greene, Bob Bell and Kevin Flynn towards its contents.