

What Is IP Telephony Security and Why Do You Need It?

In last few decades, communication systems have evolved, and one such major evolution is in the field of telecommunications in which increasingly, there has been adoption of Internet Protocol-based communications or in other words, Internet Protocol Telephony. Internet Protocol Telephony (IP Telephony) leverages the power of a converged network that is, a network where data and voice can co-exist, thereby helping organizations to reduce the Total Cost of Ownership (TCO) and increase the Return On Investment (ROI).

IP Telephony is a real-time technology that virtually encompasses an organization's communication channels and dependent lines of business and processes. This fact makes it vulnerable and susceptible to attacks and exploits. It is unfortunate, but true that there are many threats to your IP Telephony network's safety and security. If you feel intimidated by the mere idea of securing your IP Telephony network, don't worry. In this chapter, you will learn about the rationale behind securing your IP Telephony networks and get an insight to the various types of threats to modern-day telephony (IP Telephony networks). By the end of this chapter, you will know about the tools that can be used to exploit and attack an IP Telephony network, and how you can address the various business challenges posed against IP Telephony Security in the best possible manner. This chapter is intended to provide you an introduction to the world of IP Telephony Security.

This chapter covers the following topics:

- Defining IP Telephony Security
- Understanding various threats to IP Telephony
- An insight to VoIP security tools
- Understanding business challenges and Cisco IP Telephony Security responses

Defining IP Telephony Security

What is IP Telephony Security and why do you need it? How can you secure your IP Telephony network?

The following sections answer these questions and more.

What Is IP Telephony?

IP Telephony has been prevalent since the 1990s and seen as the future of communications, enabling various business verticals to transport multimedia over the IP network. The major reason behind the prevalence of IP-based communications is the key benefits such as cost-savings, rich media service, mobility, portability, ease of integration with other applications, and rich features. With the ever-increasing awareness and adoption of IP Telephony, IP-based communication networks are now gaining popularity, and businesses continue to leverage VoIP platforms to handle all their communication traffic, whether it is voice calls, Instant Messaging, or voicemail. As IP Telephony technology matures, new voice services and applications will be offered and therefore resulting in yet broader acceptance and implementation of IP-based communication networks.

IP Telephony is slowly becoming an integral part of the modern day organization's day-to-day operations. However, the benefits of IP Telephony do not come without cost. The openness of modern day IP-based communications introduces new ethical, financial, and business continuity demands to protect networks and enterprises from internal and external threats and attacks.

What Is IP Telephony Security?

IP Telephony and other pertinent services are real time in nature and a vital focal point for an organization adopting it, security of the same becomes of paramount importance. Moreover, because of IP Telephony's inherent nature (which acts both in its favor and against it) it depends on the underlying network (OSI Layers 1 through 7) for its successful operation and functioning. In essence, IP Telephony networks are built on top of underlying network infrastructure and share the strengths and weaknesses of the data networks. This implies that IP Telephony networks are susceptible to attacks as much as its basic foundation: the data networks. To make matters worse, Voice over IP has its own set of security requirements, which can be exploited if left exposed.

IP Telephony Security by definition is "Securing the 'IP Telephony components' on top of a 'Secure data network infrastructure' to provide a resilient, stable and scalable IP Telephony network."

Cisco IP Telephony operates at a system level by interacting with many different components: Call Control, IP Phones, voicemail, gateways, other IP Telephony applications, and underlying network infrastructure.

IP Telephony Security includes (and is not limited to) securing Call Control, Voice Messaging, Voice/Video calls, Network Infrastructure (LAN/WAN), Wireless, Perimeter

network defenses, and so on. In short, IP Telephony Security is securing—a conversation from an IP endpoint (IP Phone) to another endpoint or an end device (IP Phone, gateway, application server, and so on).

Figure 1-1 gives a 10,000 feet view to how a Cisco IP Telephony network is built and leverages underlying network infrastructure for converged communications.

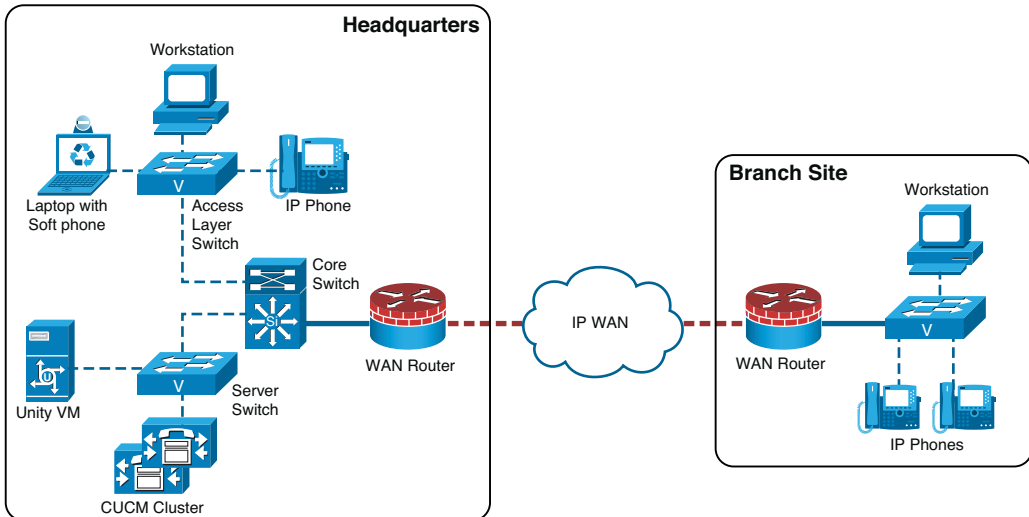


Figure 1-1 IP Telephony Network Built on Top of a Data Network

Securing data networks is the first and foremost step taken by almost all organizations. However, they tend to ignore the IP Telephony Security aspect because of lack of confidence to secure a relatively new technology. Although, this is a major loophole in overall organizational security, it is an opportunity for the hackers and attackers to exploit the vulnerabilities.

The most prominent question is, “Why would anyone attach a VoIP/IP Telephony network?” The answer is, “To benefit financially via information and identity theft, toll fraud, and espionage and to disrupt service.”

Because of the converged nature of VoIP/IP Telephony (that is, to leverage the underlying data network for voice applications), the same types of attacks that plague the data networks can also impact the IP Telephony environment as well. Thus, the content of VoIP network is vulnerable to being attacked, hacked, altered, re-routed, or intercepted. An attack on the IP Telephony system could eventually compromise the entire IP network, leading to a business’s inability to communicate via either voice or data. In addition to external threats, internal threats also need to be prohibited. Appropriate security policies need to be implemented to ensure that employees cannot abuse or misuse the IP Telephony network.

Consequently, developing a culture of security is not limited to physical, application, or network security measures; it also extends to an organization’s core values and ethics.

The concepts of security controls, processes, and framework for IP Telephony and developing a culture of security awareness are discussed in-depth in Chapter 2, “Cisco IP Telephony Security Building Blocks,” Chapter 3, “What Can You Secure and How Can You Secure It?” and Chapter 4, “Cisco IP Telephony Security Framework.” Moreover, the basics pertinent to IP Telephony network and application security as well as detailed configuration examples along with best practices for safeguarding are discussed in following chapters.

The Cisco approach to securing IP Telephony is a ‘multilayer security’ implementation to ensure protection of the critical IP Telephony components. Security mitigation techniques are available starting from the network periphery to IP Telephony devices.

What Is the Rationale Behind Securing an IP Telephony Network?

Before embarking on our journey on the road to secure Cisco IP Telephony networks, it is imperative that you understand the rationale behind securing the IP Telephony networks.

The first and foremost question that may arise in your mind is, “Why should I even bother securing my IP Telephony network? It has been running fine, and I do not want to break something which is working by applying security.” It is a common misconception that applying security to an IP Telephony network will break it! The reality being that, a non secure IP Telephony network is open to attacks and is prone to breakdowns.

Now, let’s consider some IP Telephony Security breach incidents that have occurred in the past and understand the overall impact. As illustrated in Figure 1-2, there have been incidents in which unsecured or poorly secured VoIP/IP Telephony networks were exploited and the consequences were disastrous.

VoIP Telecom Billing Fraud shakes telecom industry...

Miami: The federal government arrested Edwin Andrew Pena, 23, owner of Fortes Telecom Inc. and Miami Tech & Consulting Inc., for hacking into other providers' networks, routing his customer's calls onto those platforms, then billing those companies and pocketing the proceeds. He reaped more than \$1 million.

Source –

<http://nolastname.articlealley.com/voip-telecom-billing-fraud-shakes-telecom-industry-67797.html>

Small business gets \$120,000 phone bill after hackers attack VoIP phone!

Sydney: A small business landed with a \$120,000 phone bill after criminals hacked into its internet phone system and used it to make 11,000 international calls in just 46 hours.

Source –

<http://news.hitb.org/node/29587>

Figure 1-2 IP Telephony Networks Attacked

These cases are public examples of attacks on IP Telephony networks.

As you can see, attacks on the IP Telephony network may result in monetary and reputation loss. Interruption of communication service equates to dollar loss, and a business that was hacked is most likely to lose consumers and will not be expecting new customers for a while. It is the overall business value of security everybody overlooks until they become a victim of an attack. Besides, attacks can adversely impact the organization's business continuity. Overall, the consequences can be devastating.

You should secure your IP Telephony networks for the following reasons:

- **Secure IP Telephony infrastructure:** Securing what is an asset to an organization's daily life operations, without which the organization's communications will crumble. This in turn has a domino effect as; the organization can experience disrupted communications with peers, amongst employees, with customers, and so on.
- **Secure the conversation:** Ensure that your conversation is private and protected from eavesdropping or hacking of voice calls. Securing voice or video calls can help evade any chances of confidential information (being conveyed over an IP Telephony system) being eavesdropped, leading to Intellectual Capital theft, for example, eavesdropping of a conversation between a CEO and a CIO of a financial institution could otherwise reveal a lot of confidential information if it weren't secure.
- **Business continuity:** Ensures that the business continuity is maintained and the chances of disruption and losses are minimized. If voice and video conversations are secure, it helps ensure the business continuity and minimize disruption leading to monetary and credibility losses.
- **Business value:** Protect your company's privacy and intellectual property by protecting your IP Telephony communications. Lost business and trade-secret information, for example, pursuant to a man-in-the-middle (MITM) attack, could be worth a million dollars to your company.

Keeping your voice communications safe from the same threats that can impact your data network is essential. In a world plagued with attackers and hackers, IP Telephony Security is an even more critical issue than ever before.

A secure voice network is the foundation of a successful organization.

What Can You Do to Safeguard Your IP Telephony Network?

Before taking any action to safeguard an IP Telephony network, it is imperative for organizations and businesses to understand the key security threats to their IP Telephony network and the proactive solutions they can adopt to mitigate these threats. The key lies in recognizing the problem before finding the solution.

Not all threats are present in all organizations. A commercial organization may be concerned primarily with toll fraud, whereas a government agency may need to prevent disclosure of sensitive information because of privacy or integrity concerns. Thus,

organizations must evaluate what is the right level of security for them; what is the cost versus risk trade-off for them, and so on.

No single solution protects a network from a variety of threats. You need multiple layers of security. If one fails, others still stand. Therefore, you need to understand how to secure a Cisco IP Telephony network using a layered approach. Throughout this book, you discover ways to apply security measures in a step-by-step and layered approach, that is, leveraging defense-in-depth with—physical security, network security, application security, and endpoint security to secure your Cisco IP Telephony network.

In the next section, you will explore and understand the various types of attacks or hacks that can be launched against an IP Telephony network. Moreover, in next few chapters you will explore the step-by-step approach to develop an IP Telephony Security plan and understand how you can implement end-to-end security by developing an IP Telephony Security framework, evaluating cost versus risk, and understanding the level of security required for your organization.

IP Telephony Security Threats

Advances and trends in Information Technology have always outpaced the corresponding realistic yet necessary security requirements. These security requirements are often tackled only after these technologies have been widely deployed.

IP Telephony is no different. As IP Telephony adoption increases, so will its exposure to current and emerging security threats. Both “phreakers” (voice) and “hackers” (data) lurk around all the time, trying to find vulnerabilities and security slacks to do what they do the best—disrupt the IP Telephony network.

The following section gives you an insight to how hackers can attack an IP Telephony network.

How Do Hackers Attack an IP Telephony Network?

It is worthwhile to know about the ways a hacker can break into your IP Telephony network so that you know how to deter an attack. A hacker may use the following sequence of events to break into your IP Telephony network:

- **Foot printing:** Gather information about the target organization.
- **Scanning:** Search for an active or open target.
- **Enumeration:** Extract information from target(s) found during the scanning phase.
- **Exploit:** Eavesdrop, hijack streams, install backdoors, and debilitate an IP Telephony network.
- **Cover tracks:** Evade any detection by making a legible user accountable.

Let’s go through these steps in detail to understand what happens behind the scenes and how a hacker can possibly breach your network defenses.

Foot Printing

A hacker typically starts with finding as much information as possible through the Internet by:

- Looking into WHOIS records
- Performing Internet searches
- Probing blog posts and boards where employees leave any information pertinent to their organization structure, phone numbers, extensions, and so on
- Researching the organization's websites for contact details

These searches give the hacker enough ammunition to launch the next wave of attack, which is scanning.

Scanning

The hacker will now try to scan for any active targets (live hosts) that can be compromised, by leveraging:

- Host discovery via ping sweeps
- SNMP sweeps
- TCP ping scans
- Port scans

The most common tools used for scanning are Nessus, Nmap, hping, snmpwalk, and so on.

Enumeration

During this stage, the hacker tries to extract usernames and passwords from hosts who were identified to be reachable and live on the victim's network using the following:

- SIP option, registration, and invite (automated or manual)
- Enumerate TFTP server
- SNMP enumeration

The most common VoIP security tools used for enumeration are SIPVicious, Nastysip, and Nmap to name a few.

Exploit

During this phase, the hacker or attacker exploits the IP Telephony network and compromises its integrity. The following attacks or hacks can be used to extract invaluable and confidential information:

- Eavesdropping
- DoS/DDoS attack
- Call redirection and hijacking
- Toll fraud
- Flooding attack
- Call pattern tracking
- Signaling and media manipulation
- Registration removal and rejection

This phase is the most devastating for the IP Telephony network and is a “Gold Mine” phase for the hacker/attacker. On one hand, calls can be eavesdropped, blocked, and manipulated, and on the other hand, calls can be hijacked and redirected. The IP Telephony platform now is vulnerable to toll fraud, registration rejection, flooding, and DoS attacks.

Covering Tracks

This is the last phase in which the hackers tries to cover their tracks to ambush the integrity of an IP Telephony network. Essentially, the hackers or attackers attempts to cover the detection of their presence by erasing any logs, using IP spoofing tools, using ARP spoofing tools, and by imitating valid user credentials, so the victim is someone innocent (a legal employee or member of organization). Moreover, Trojans and backdoor programs are usually installed on victim machines to allow for easy entry the next time an intrusion is attempted.

Equipped with the knowledge on how your IP Telephony network can be compromised by an insider or an outside attacker or hacker, let's now go over some of the key security threats and their mitigation techniques.

What Are IP Telephony Security Threats and Countermeasures?

It is a war out there between Cisco IP Telephony administrators and phreakers or hackers. To be successful, you must know your enemy as well as your own strengths and weaknesses. As you know by now that IP Telephony networks share the same weaknesses as their underlying foundation data networks, it is time to explore the cause that phreakers or hackers can leverage to take advantage of any weakness in your IP Telephony network. To truly know the threats, you must consider both external and internal threats. Internal security threats are perceived by the employees or from within the secure zone, and the external security threats originate from public network(s) or nonsecure zone.

The next section highlights the main threats targeting the IP Telephony system.

Let's understand what each one of these threats is all about and how you can counter them, as explained in the next section, following which you'll be introduced to various commercial and free tools available that can be used to exploit and attack an IP Telephony network.

Threats

This section highlights the various threats that can adversely distress your IP Telephony network:

- **Eavesdropping:** Refers to loss of private or confidential information because of sniffing, scanning, and interception (tapping) of voice calls. If calls can be sniffed, conversations can be replayed or eavesdropped; there is a monumental risk associated with non-secure IP Telephony systems and ample opportunity for phreakers and hackers. While hacking calls, a hacker, for example, could acquire access to financial material. Because of the open nature of IP networks and especially the low trust level in the Internet, privacy is a commonly raised concern when comparing IP Telephony solutions against traditional telephony solutions. Free and paid tools are available on the Internet that can be used to sniff or passively scan the voice traffic.
- **Manipulation:** Integrity of information means that information remains unaltered by unauthorized users. In the context of IP Telephony, this refers to the loss of integrity of voice communications (alteration of voice or video traffic) by hijacking calls and injecting or altering the contents of voice packets (man-in-the-middle attack). If voice call signaling or media messages can be intercepted, they can be modified, and the recipient (listener) can be made to listen to what the attacker or hacker wants and not what the original party (speaker) conveyed.
- **Impersonation:** Identity spoofing is not limited to humans (for instance, the person behind a telephone) but can also extend to devices, such as Cisco CallManager, a voice gateway, or an IP Phone. Impersonation in the form of frame-tagging (VLAN-hopping) and MAC or IP address spoofing gives attackers the ability to impersonate a VoIP phone.
- **Denial-of-service (DoS):** This refers to the prevention of access to voice network services by bombarding voice servers, proxy servers, or voice gateways with malicious or malformed voice packets. This leaves users deprived of the services or resources they would normally expect to have. For example, voicemail, IM, and SMS (notification) services in IP Telephony systems can be the targets of message flooding attacks. These attacks cause loss of functionality.
- **Toll fraud:** Refers to when an individual or an organization devises method(s) to gain unauthorized or unsolicited access to IP Telephony resources to gain the ability to dial long-distance calls. When access is gained, it can lead to large telephone bills, accumulating in a period of days or even hours.

- **SPIT and Vhishing:** Spam over Internet Telephony (SPIT) is equivalent to unnecessary e-mail (SPAM). A dedicated hacker can release a flurry of calls to a targeted IP Telephony system and a particular IP Phone. This can cause that IP Phone to be overloaded (unable to take any calls) and the IP Telephony system to be busy for that endpoint. Now, imagine this attack scaled to multiple IP Phones. Not only can it leave the IP Phones unusable (because per line capability for taking calls will be well overshot), it will also busy out the PSTN channels and the IP PBX's capacity to handle calls. If SPIT were not enough, hackers can also ploy Vhishing to lure IP Telephony users into yielding personal information such as credit card number, bank accounts, Social Security numbers, and so on under the guise of needing this information for a legitimate reason.

Countermeasures

At a high level, following suggestions can help prevent loss of integrity, privacy, and threats arising out of impersonation, DoS attacks, toll-fraud, and so on.

- Be up to date on new and changing threats.
- Follow best practices for VoIP network security (as mentioned throughout this book).
- Implement tools to monitor and report of IP Telephony use.
- Follow a layered security approach instead of only a network or an application security approach.
- Implement an IP Telephony Security policy for your organization.

To overcome the concern of loss of privacy, DoS attacks, hijacking of media, signaling streams, and so on, it is highly recommended to use the defense-in-depth (also known as layered security) approach (as detailed throughout this book) because there is no single system or way to stop or evade privacy threats. Cisco IP Telephony applications, endpoints, and Cisco network gear empowers you to leverage the built-in security features. These features and associated leading practice recommendations on planning, designing, deployment of secure IP Telephony networks are described and discussed in detail in following chapters.

You will learn more about the end-to-end security methodology for IP Telephony and layered security approach throughout this book. As we explore the world of Cisco IP Telephony Security, you will discover the best practices and ways to secure your Cisco IP Telephony network.

An Insight to VoIP Security Tools

This section gives you insight to various VoIP security tools. These tools are meant to test an IP Telephony network's resilience and susceptibility against attacks. However, they can be used by hackers and phreakers to attack an IP Telephony network. These

tools can be used to launch attacks against VoIP systems, such as hijacking media and signaling streams (MITM attack), sniffing RTP traffic (eavesdropping), rebooting phones (DoS attack), flooding phones with calls (DoS attack), and reassigning the devices (impersonation) unlawfully to other users.

There are many VoIP security tools available on the Internet, some free, whereas other are commercial tools. As discussed earlier, on one hand these tools can be used to compromise integrity of an IP Telephony network, and on the other hand, they can be used to assess the security posture of an IP Telephony network, find any security gaps, and fill them.

The following section gives you an insight to various VoIP security and penetration tools available which can be used in favor of or against your IP Telephony network's security.

IP Telephony Security/Penetration Tools

Now, that you know about the possible ways a hacker could possibly compromise your IP Telephony network as well as the threats which lurk around your IP Telephony network, it is time to go over different VoIP security tools that can be used effectively for and against your IP Telephony network.

Following is the list in which the VoIP security tools can be broadly categorized:

- Sniffing tools
- Scanning and enumeration tools
- Flooding/DoS tools
- Signaling and media manipulation tools

Sniffing Tools

Sniffing tools are some of the most popular tools available to promiscuously sniff the data off your IP Telephony network:

- **Cain & Abel:** It can reconstruct RTP media calls. This tool has features such as APR (ARP Poisoning Routing), which enables attackers to sniff on switched LANs and perform MITM attacks.
- **UCSniff:** An assessment tool that enables users to rapidly test for the threat of unauthorized VoIP eavesdropping. UCSniff supports SIP and SCCP signaling. It supports G.729, G.723, G.726, G.722, G.711 u-law, G.711 a-law voice codecs, and H.264 Video codecs. It can reconstruct the voice conversation and has features such as MITM (ARP Poisoning mode).
- **VOMIT:** Can convert a Cisco IP Phone dialogue into a wave file that can be played with any ordinary sound player. It however works only with G.711 codecs.

- **VoIPong:** Detects VoIP calls on a pipeline (only G.711 codec) and can dump actual conversation into wave files. It supports SIP, H.323, SCCP, RTP, and RTCP protocols.
- **VoIP Hopper:** A GPLv3 licensed security tool that rapidly runs a VLAN Hop into the Voice VLAN on specific Ethernet switches. VoIP Hopper does this by mimicking the behavior of an IP Phone.
- **Wireshark:** One of the most famous network traffic analyzer, which can capture RTP and VoIP signaling traffic (SIP, SCCP, H.323, MGCP, and so on). It can reconstruct the voice conversation and play it back as a .wav file.

Scanning and Enumeration Tools

Scanning and enumeration tools can not only be used by an attacker to scan for active and live targets for IP, ports, services, and so on, they can also to gain valuable information about your IP Telephony network.

- **Nessus:** One of the most famous vulnerability scanners that supports credentialed or un-credentialed port scanning and network-based vulnerability scanning leading to vulnerability analysis. It can be used to scan for outdated services, vulnerability, and security exploits.
- **Nmap:** An open source utility for network exploration or security auditing. It supports Advance techniques for mapping networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP and UDP), OS detection, version detection, ping sweeps, and so on.
- **SIPVicious:** A set of tools used to audit or attack SIP-based IP Telephony systems. It has a SIP scanner, a SIP phone extension range finder, and an online password cracker for SIP PBX and provides the ability to manage sessions and generate reports.

Flooding/DoS Tools

The information or session flooding and DoS attack tools present a new attack vector to bring down a functional and healthy IP Telephony system. Thus, you should be aware of the various tools available, which hackers bring into play to carry out their dirty work, so that you can take preventive measures:

- **Scapy:** Forges or decodes packets of a wide number of protocols and send them on the wire, capture them, and match requests and replies. It can send invalid frames, combine techniques (for example, VLAN hopping plus ARP cache poisoning) and perform VoIP decoding.
- **RTP Flooder:** Creates RTP packets that can flood a phone or proxy thereby leaving the target unusable for the legal user.

- **UDP Flooder:** Used to send numerous UDP packets at a pre-selected speed. It uses a specific port to attack and also uses some imaginary source address.
- **Nastysip:** A simple Linux-program that generates bogus SIP-messages and can send them to any peer.

Signaling and Media-Manipulation Tools

These tools help an attacker or hacker to manipulate the information and have the listener listen to what the attacker or hacker wants and not what the original party conveyed. Moreover, these tools can be used to hijack calls:

- **RTP Injector:** An attack tool that can be used to inject random audio into established RTP connections. The tool can identify active conversations and can enumerate the media codec in use, allowing for the injection of an arbitrary audio file that is automatically transcoded into the necessary format required.
- **Fuzzy Packet:** Used to manipulate messages through the injection, capturing, receiving, or sending of packets generated over a network. It can fuzz RTP and includes built-in ARP poisoning option.
- **H225regreject:** Enables you to disconnect H.323 calls. It can watch a network to figure out whether a call is happening. When it finds a call, it can send a Registration Reject packet, which will effectively end the call.
- **SIP-Kill:** Simple yet effective, this tool can sniff for SIP-INVITEs and tear down the call.

Business Challenges and Cisco IP Telephony Security Responses

Where there is security, there are challenges ranging from ethical concerns to technical or procedural complexity for the application of security. It is not unusual to face a multitude of challenges when you prepare to secure your IP Telephony network.

There are quite a few questions, which unfold during conception phase, while developing an approach to IP Telephony Security. The majority of these revolve around various technical, solution, and business goals.

Common Business Challenges Associated with IP Telephony Security

Let us look at some of the major business challenges, which are likely to be encountered while preparing for planning, executing, and optimizing IP Telephony Security:

- **Solution challenge:** The major challenge is to identify the customer security risks and vulnerability, how to develop a security policy around it, and how to maintain stability and robustness of the IP Telephony solution.

- **Ethical challenge:** Every IP Telephony user has a responsibility to promote ethical use of the IP Telephony system and any relevant information. However, what is the remediation when people overlook ethics?
- **Technical challenge:** How to implement IP Telephony Security and develop similar standard(s) applicable to corporate users dispersed over multiple region or locations.
- **Environmental challenge:** How to deploy IP Telephony Security around a network which is not all Cisco equipment (inter-operating with other vendors), which can be difficult or sometimes, impossible.

Cisco IP Telephony Security Responses

There's no "silver bullet" to address all these issues. However, Cisco IP Telephony offers the following best practice recommendations and solutions to address these issues:

- **Solution challenge:** This can be addressed by understanding the needs of the organization or business, through security risk assessment, working on a detailed security plan with internal and external customers or stakeholders, followed by a phased deployment approach to implement just the right level of security. (You learn more about an IP Telephony Security policy development approach and determining the right level of IP Telephony Security required in Chapter 4).
- **Ethical challenge:** Although there is no black-and-white procedure to tackle this challenge, IP Telephony Security policy can help clear out many grey areas. As an IP Telephony Security policy is driven by the corporate security policy, it should lay down specifics of the level of access, ease of access, information access review or audit, and so on. Moreover, employees' awareness of the corporate security policies helps reduce the likelihood of insider threats.
- **Technical challenge:** This can be addressed via the Cisco leading practices to deploy and secure IP Telephony technologies across the globe. Cisco Advance Services (AS) teams have deployed IP Telephony Security solutions for many organizations worldwide in different market segments ranging from finance to manufacturing to government to pharmaceuticals.
- **Environmental challenge:** This can be addressed by keeping the IP Telephony Security solution based on industry standards. The Cisco IP Telephony Security implementation conforms to the industry wide standards (for example SSL and AES) and can be leveraged by third-party vendors and products for secure integration with Cisco IP Telephony network.

Summary

Just as you wouldn't leave your doors unlocked and your precious belongings in the open, you do not want to leave your IP Telephony network open to attacks from within and outside the organization either. In This chapter, we tried to unfold the meaning of IP Telephony Security and understand the logic behind securing an IP Telephony network.

This chapter looked at some of the basic yet important logical measures you can take to ensure the security of your IP Telephony network, and the rationale behind why you should secure your Cisco IP Telephony network. You learned about the security threats that lurk around your IP Telephony network, the detrimental effects of leaving an IP Telephony network unsecured, how attackers or hackers can attack an IP Telephony network, and the ways in which various security tools can be used or abused.

This book is primarily focused on understanding the Cisco IP Telephony network security principles, features, and protocols that can help you in the successful implementation of comprehensive end-to-end Cisco IP Telephony Security. As you go through the various chapters of this book, you will learn about ways by which you can secure your Cisco IP Telephony network. This will ultimately result in you gaining a deep level of understanding of IP Telephony network security-related issues and their resolution. At this point, you have a brief understanding of IP Telephony network security and its importance to your organization.

In following chapters, you learn in depth how you can go about securing your Cisco IP Telephony network in a holistic manner and build a concrete understanding on Cisco IP Telephony Security fundamentals.