

Security

Chapter 6

TABLE OF CONTENTS

This chapter highlights the steps one should take to ensure IP telephony traffic is secure against outsiders and unauthorized individuals.

Evaluate your Risks	1
IP Telephony - Specific Considerations	1
Network-Based Attacks	1
Phone Service Theft	1
Eavesdropping	1
Power Failures	1
SPIT	2
Other Threats	2
Network Security Basics	2
IP Telephony Security Basics	2
IP Telephony System Security	3
How to Mitigate IP Telephony Vulnerabilities	4
The Bottom Line	4

Anybody who's connected to the Internet or who owns a PDA/multi-function cell phone knows that they're at risk of getting viruses, worms, spam and other malicious threats. In addition to the potential damage these threats introduce in terms of lost data or corrupted files, there are now regulatory issues associated with ensuring protection. Healthcare has its own privacy regulations in the form of HIPAA (Health Insurance Portability and Accountability Act of 1996), and infringements can result in significant punishments and fines. The bottom line is that you have to protect your organization's devices and network. IP telephony is no different – the only difference is the form of the traffic: voice versus data. All traffic crossing a network can be stolen, manipulated or blocked if proper network security precautions are not put into place. This chapter will highlight the steps you should take to ensure your IP telephony traffic is secure against outsiders and unauthorized individuals.

Evaluate your Risks

The first step to determining the right network security strategy (VoIP or otherwise) is to determine the risks your particular organization faces. (Because of the increasingly complex network security threats and solutions out there, you may want to get a network security expert on board to help with the assessment.) For instance, a healthcare organization faces different regulatory requirements than a legal or accounting firm. An e-commerce organization has altogether different privacy and security requirements. Once you determine what your risks are, you'll be better able to determine the best multi-layer defense against attacks, eavesdropping, service theft and other evolving threats for the entire network, including the IP telephony system being utilized.

IP Telephony - Specific Considerations

Network-Based Attacks. IP telephony is susceptible to Denial of Service (DoS) attacks because these can cripple the network to the point that nothing, including voice calls, can get through. (It is generally recommended that every organization using IP telephony have backup telephone lines in the case of an out of control DoS attack or regional power failure.) Spam, spyware and phishing are other network attacks that are commonly used to commit identity theft and other fraud. Finally, viruses and bots can destroy data or devices or even hijack phones into a toll fraud scheme.

Phone Service Theft. A hacker could enter into an unprotected network and access the PBX to make endless international calls. There have been major cases cited in the news where toll fraud has cost companies millions of dollars. In many instances, the criminals have been caught and prosecuted, but not without major costs to the companies defrauded; and keep in mind, there are always those crimes that go undetected.

Eavesdropping. Without the proper security in place, a hacker could eavesdrop and possibly expose confidential information. A private conversation about financials could be recorded and played for anybody, which could lead to internal and external problems, including punishment from numerous regulatory agencies. Or a personal call from an employee to a florist with a credit card number could lead to credit card and even identity theft.

Power Failures. While outages affect data traffic, of course, there's a difference when it comes to telephony. People expect telephones to work even during an outage because homes often have a non-electronic phone that simply plugs into the telephone outlet. This expectation is generally brought into the workplace.

SPIT. Spam over Internet telephony is an alternative to telemarketing where one message can easily be sent to thousands of recipients with the click of a mouse. In other words, your employees' voice mail boxes can become as overloaded with spam as their e-mail would be without appropriate spam filters.

Other Threats. There are new threats created and discovered daily. One such attack is the spoofing of a phone number, which essentially allows a hacker to look like he or she is someone else, which is one of the easiest ways for this person to steal an unsuspecting person's identity. While individuals have learned not to trust e-mail, it is still generally believed that telephone communications can be trusted.

Network Security Basics

Network security will lead to a secure IP telephony system. Your organization has likely taken steps such as initiating the use of virtual private networks (VPNs) and installing firewall equipment, which protects the organization against intruders and threats mentioned earlier. Since voice is just another application on the network, the same precautions should be taken to secure the IP telephony equipment. Every form of security should be applied, including physical, human, network, and system security.

- **Physical security:** Buildings, equipment rooms, data servers, and wiring closets should be off-limits to anybody who is not authorized.
- **Human security via security policies:** Make sure your organization's informational assets are protected against inappropriate or unauthorized use by a renegade employee. Ensure hiring and system usage policies are in place to govern appropriate use. Establish and strictly enforce policies having to do with passwords and system usage.
- **Network security:** Again, create a multi-layered defense using firewalls, VPNs, and intrusion detection or prevention (IDS/IPS). Make sure wireless access points use the highest level of access control and encryption to prevent intruders from gaining access to your network and its resources.
- **System security:** Arm every desktop with anti-virus software to fight against spyware and other malware. Utilize host intrusion prevention systems to protect servers against attacks.

Another force to consider is segregating traffic via virtual LANs (VLANs). It is a method of logically grouping devices or departments onto their own LANs. Isolating LANs from one another provides an additional layer of security. It also reduces the impact of multicast or broadcast traffic since there are separate broadcast domains.

Finally, bandwidth management can be utilized to further guarantee bandwidth for business-critical, latency-sensitive traffic like VoIP traffic. Bandwidth management methods include assigning a certain priority to each type of traffic. VoIP packets should be assigned the highest priority to ensure voice traffic gets through.

IP Telephony Security Basics

When your network is secured, take it a step further and utilize best practices for deploying secure IP telephony.

- **Firewalls:** Make sure the firewalls you're using can handle the latency sensitive needs of IP telephony traffic.
- **Switched environment:** Use Ethernet switches (not hubs) to connect all your voice devices not only for better performance but also to limit the possibility of a hacker getting onto a call because in a

switched environment, the flow of traffic is between devices and nobody can tap in.

- **VLAN assignment:** Assign voice to a separate VLAN (or separate VLANs). This segregates traffic for improved performance and security.
- **Priority:** Prioritize voice traffic over data on these VLANs so that delay sensitive traffic gets through even during a network attack. Ensure your network switches can prioritize based on VLAN tags and support multiple queues.
- **VPN:** Use a VPN between sites, buildings, or departments to encrypt traffic. This is especially important when it comes to protecting confidential employee information, such as social security numbers. In addition, use software VPNs or VPN appliances for remote users to protect conversations from being tapped. Your system should also offer you the option of completely disallowing remote access for an even tighter security option.
- **Port lockdown:** Lock down IP telephony traffic on the physical switch ports so that only authorized MAC addresses can transmit over the port.
- **Media encryption:** Look for a solution that prevents eavesdropping by encrypting voice traffic. This way, even if someone taps a voice stream, they are unable to decode or understand the conversation. Not all IP telephony system vendors offer this but it is a necessity for IP telephony security.
- **Voice mail storage:** Make sure that your voice mail storage is itself secure to prevent unauthorized access of voice mail files.

IP Telephony System Security

Let's look now at the IP telephony system itself. While you can secure your network in all the right ways, you also need to choose a phone system that is secure itself. Consider moving away from a system that uses Microsoft Windows for call control because of the security considerations. With a constant stream of Windows security updates and patches, you're risking downtime and security breaches.

Another architectural consideration to keep in mind is ensuring your system is distributed, which will mean it has no single point of failure. A distributed system allows continued operation in the case of worms, viruses, or DoS attacks. An attack will not disable the entire system if intelligence is distributed amongst multiple devices.

Your chosen system should offer multiple levels for administrator permissions to limit control and ensure unauthorized individuals do not gain access. Once you've deployed, reserve full access for just a few key information technology employees. Ensure that a web-based management solution supports secure management using Secure Sockets Layer (SSL), which secures communications from the interface to the server.

According to the SANS (SysAdmin, Audit, Network, Security) Institute, a cooperative research and education organization, VoIP servers and phones are at significant security risk. The organization's 2006 annual update, SANS Top-20 Internet Security Attack Targets, indicates that there's been an increase in security scrutiny of IP telephony, especially on typical components such as the call proxy and media servers, as well as the phones themselves. Some products have been found to contain vulnerabilities that can either lead to a crash or a complete control over the server or device. "By gaining a control over the VoIP server and phones, an attacker could carry out phishing scams, eavesdropping, toll fraud or denial-of-service attacks."

How to Mitigate IP Telephony Vulnerabilities

SANS has determined and published a list of things enterprises must do to mitigate the IP telephony vulnerabilities mentioned in this chapter.

- Apply the vendor supplied patches for VoIP servers and phone software/firmware.
- Ensure that the operating system running the VoIP server is patched with the latest OS patch supplied by either the OS vendor or the VoIP product vendor.
- Scan VoIP servers and phones to detect open ports. Firewall all ports from the Internet that are not required for keeping up the VoIP infrastructure.
- Use a VoIP protocol aware firewall or Intrusion Prevention product to ensure that all UDP ports on VoIP phones are not open to the Internet for RTP/RTCP communications.
- Disable all the unnecessary services on phones and servers (telnet, HTTP etc.).
- Use VoIP “protocol fuzzing tools” such as OULU SIP PROTOS Suite against the VoIP components to ensure the VoIP protocol stack integrity.
- Additional caution should be taken at the product selection phase to ensure the VoIP product vendor supports OS patches as they are released. Many VoIP vendors will void support for unapproved patches and may take considerable time before approving them.
- Apply separate VLANs to your voice and data network as much as your converged network will allow. Ensure that VoIP DHCP and TFTP servers are separate from your data network.
- Change the default passwords on phones’ and proxies’ administrative login functions.

Source: SANS Top-20 Internet Security Attack Targets, 2006 Annual Update

The Bottom Line

IP telephony requires the same level of security as your data network requires. You need to ensure you’re receiving calls from trusted sources, you’re protecting your infrastructure from toll fraud, and you need to make sure your voice calls get through, even when parts of the network might be bogged down by DoS attacks, viruses, or worms. There are vendors that offer IP telephony solutions with additional layers of security. You don’t have to rely solely on network security devices in place. You can take it a step further and protect your IP telephony equipment so that voice communications and resources are as safe as possible from hackers and other criminals. The next chapter will discuss wireless IP telephony, including more on security, as well as QoS, reliability, and coverage areas.