Global Knowledge™

Written and provided by

Expert Reference Series of White Papers

Enterprise VoIP Security: Potential Threats and Best Practices

Enterprise VoIP Security: Potential Threats and Best Practices

Prepared for Global Knowledge by Technology Marketing Corporation

Table of Contents

Introduction

Voice over Internet Protocol (VoIP) is reaching critical mass. With most major telecommunications carriers currently in the process of readying VoIP services for mass deployment, it's clear that IP telephony is finally headed for prime time. However, the promise of mass VoIP consumption also increases the risk for widespread security violations, spawning a new sense of urgency to develop secure VoIP solutions now before hackers wreak havoc on corporate voice networks.

Until now, VoIP security hasn't been a particularly significant subject, since most IP deployments were small in scale and relatively contained. But as VoIP usage becomes widespread, enterprise users will become subject to many of the same security risks that have affected data networks.

This report will strive to highlight some of the potential security problems associated with VoIP and address what measures can be taken to secure enterprise VoIP deployments.

A Word on VoIP

VoIP is a process of digitizing and sending voice telephone signals over the Internet or other data network. Enterprises of all sizes can benefit from this technology, but they must do some basic research to figure out if VoIP is right for them. Which vendor should I call? Would I rather deploy and manage my telecommunications in-house, or does it make sense to outsource to a hosted services provider? How much will this cost, and how much money can I save in the long run?

The first thing most people realize about VoIP technology is that it can save their business money by reducing or eliminating the toll charges for long-distance and even local calling. However VoIP is much more than simply a plan to lower a company's phone bill. There are many so-called "soft" benefits enabled by VoIP, such as increased worker productivity, the ability to collaborate among multiple branch offices, and lower operational expenditures as a result of simplified management schemes.

The first thing many people think about VoIP is that this technology is primarily a cost-saver. For many enterprises, that is enough of a reason to consider VoIP. Of course the cost element has many aspects to it that merit consideration. Tremendous cost savings come in the form of lower telephone bills. By converting voice into packets and transporting these packets over an IP network, corporations are able to avoid the Public Switched Telephone Network (PSTN) and the tolls associated with that.

In the case of an enterprise with multiple branch offices, this is especially true. By using the company's data network, enterprises can eliminate all costs associated with calling between branches. Furthermore, they can have all locations served off of a single IP PBX, thus enabling extension dialing between far-flung locations. By simply dialing a coworker's extension, you can speak to a distant colleague as if they were in the very next cubicle. VoIP enables seamless call transferring to experts across a connected enterprise, be they in the same building, across town, or across the globe.

If the data network reaches a remote location, so too do the telephony applications that are enjoyed by employees at the main corporate location. Applications such as conferencing, voice mail, unified communications, click to dial—all of these new productivity-enhancing services are enabled across the enterprise. But managing the system is simplified due to the elimination of the need to look after multiple networks.

VoIP reduces the cost and complexity associated with moves, adds, and changes. Many enterprise VoIP solutions allow administrators to manage the system via a web-based browser interface and enable managers to enact changes to an employees phone settings and voice mail settings (for example) remotely, and without the need to call the phone system's manufacturer to send a representative to make those moves, adds and changes.

Potential Security Risks

Denial of Service/Distributed Denial of Service (DoS/DDoS)

There are a number of common security breaches that can affect an enterprise's VoIP deployment. Among these, one of the most widely talked about is a denial of service (DoS) attack or a distributed denial of service attack (DDoS).

A denial of service attack is defined as an assault on a network or computing system designed to cause a loss of service. Hackers can overload the resources of a system under attack or simply consume all the available bandwidth by flooding the network with malicious traffic. Problems can stem from the central network under attack to branches and subsequently wider geographic areas, as routers get overloaded and cease to function properly.

A distributed denial of service attack occurs when hackers take control of enterprise or personal computers connected to the Internet (through a broadband connection such as DSL, cable modem, or T1 lines in the case of an enterprise). These computers can be commandeered by viruses or Trojan horse programs that allow the attackers to remotely control the machine. With a large number of compromised PCs now being used to flood a network with malicious packets, even the largest enterprises and service providers can fall prey to DDoS attacks.

Imagine what these types of attacks can do to voice traffic, which is extremely time and delay sensitive.

In January 2005, Cisco Systems was forced to issue a warning to its customers after it was discovered that a flaw in the Cisco IOS software could potentially open the door to a hacker intent on flooding a company's routers with malformed packets. This would cause the device to reload repeatedly, resulting in a DoS attack, and rendering the router useless.

Other examples abound. According to an article that appeared in *Network World*, Carnival Cruises learned the hard way that their IP telephony system was vulnerable to attack.

"[We] got hit by the Nimda virus last year," says Tom McCormick, senior technical analyst with the Miami cruise line. "It was a demo box and it wasn't patched to protect against the latest viruses."

Since the system was being used for evaluation, Carnival's business was not affected by the crash, but the event did serve as a wake-up call. Carnival learned from the experience and went on to deploy IP telephony in their network.

Enterprises rely on their phone systems. For many companies the phone system is the lifeblood of their business. It's safe to say that a DoS/DDoS attack can cause an enterprise tremendous loss of revenue, not to mention untold amounts of grief, when the security breach results in loss of communication.

Other VoIP Security Threats

Aside from DoS/DDoS, there are a number of other significant concerns in a VoIP environment.

Call Interception

Unauthorized monitoring of voice packets or Real-time Transport Protocol (RTP). The threat of eavesdropping is very real, especially from within your own network. According to Robert Moskowitz, writing in *Secure Enterprise* magazine, ". . . like other IP servers, SIP servers and proxies may be vulnerable to attacks, such as registration hijacking, impersonation, exploitation (acting as a wiretap), and DoS. A compromised server could trick two phones into acting as if each is using a codec that the other lacks, providing an instant wiretap by turning the server into a codec converter."

Signal Protocol Tampering

In the same category as call interception, a malicious user could monitor and capture the packets that set up the call. By doing this, they can manipulate fields in the data stream and make VoIP calls without using a VoIP phone. Or, they could make expensive calls (e.g., international) and make the IP-PBX believe it originated from another user.

Presence Theft

Impersonation of a legitimate user sending or receiving data. A hacker can gain control of an IP phone and redirect traffic to someplace other than the intended party. If a caller is unaware of the redirection, he/she may be willing to give up personal information such as social security numbers, credit card information, and other personal details to the hacker.

Toll Fraud

The ability of a malicious user or intruder to place fraudulent calls. This threat is self-explanatory. By inserting a rogue phone or commandeering a legitimate phone surreptitiously, an attacker can make calls anywhere in the world, racking up expensive charges, or perhaps can even use the phone's identity in order to make purchases and online transactions.

Call Handling OS

The call handling software of many IP-PBX systems relies on operating systems, or operating system components, that may not be secure. For example, the use of Microsoft IIS as a web-based configuration tool for the IP-PBX may introduce significant vulnerabilities in your VoIP environment. Once compromised, this could be an avenue into other connected systems and information stores.

SPIT

Spam over Internet Telephony, or SPIT as it's referred to, may seem more like an inconvenience than a bona fide security threat, but as with a denial of service attack, the potential introduction of waves of unwanted traffic can be harmful to an enterprise's business practices. Just imagine having to spend 20 minutes every morning wading through unwanted voicemail advertising the latest miracle fat-burning or impotence drugs, or having to listen to scions of Nigerian royal families promise you millions in exchange for some bank account information. In much the same way that e-mail spam is today growing from a nuisance to a full-fledged productivity drain, so too can SPIT tax your company's resources, by drawing focus away from your core business objectives.

Impact of Hackers

According to security vendor Symantec Corp. in its most recent semi-annual Internet Security Threat Report, hackers continued adding billions to the cost of doing business on the Internet, despite security efforts to prevent malicious attacks.

"Attackers are launching increasingly sophisticated attacks in an effort to compromise the integrity of corporate and personal information," said Arthur Wong, vice president of Symantec Security Response and Managed Security Services.

Key findings of the report include:

- Rise in threats to confidential information
- Steady increase in phishing attacks
- Increase in attacks against web applications
- Rise in number of windows virus/worm variants
- Increase in severe, easy-to-exploit, remotely exploitable vulnerabilities

According to a report from Deloitte identifying the top 10 trends for the technology, media, and telecom sectors, ". . . viruses, worms, and other malware will multiply and spread to connected mobile devices, frustrating the public and costing companies billions in lost data and downtime."

All in all, the prognosis is not good. And yet all may not be lost. Increased awareness of security threats and breaches will reveal tremendous opportunities for vendors of security products.

VoIP Security Best Practices

To minimize the security risks in a VoIP environment, the following best practices are recommended.

Virtual LANs

Keeping voice and data on separate VLANs is a good idea for increasing performance and security. What's more, the best practice for securing a voice VLAN is to control the traffic between the voice and data VLAN using filtering and/or firewalls. This can prevent DoS attacks and spoofing as well as providing general filtering that limits malicious footprinting.

A recent report from the National Institutes of Standards and Technology (NIST), entitled Security Considerations for Voice Over IP Systems, supports this. The report recommends that users separate voice and data on logically different networks if feasible. Different subnets with separate address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection.

Encryption

Wherever possible and practical, you should implement encryption through VPNs or any method available to you. On one hand, encryption potentially can delay voice packets and adversely affect the performance of VoIP on your network—especially with multiple encryption points. On the other hand, if a network is operating efficiently, the overhead of the encryption should have little impact on the performance of the VoIP system.

Again, NIST supports the idea of encrypting VoIP traffic for added security. The report suggests that users take advantage of encryption at the router or other gateway, not at the individual endpoints, to provide for IPsec tunneling. Since not all VoIP endpoints are powerful enough to perform adequate encryption, placing this functionality at a central point ensures that all VoIP traffic originating at the enterprise network has been encrypted.

Direct Firewall Support

If VoIP traffic will be traversing a firewall, make sure your firewall is capable of direct support for SIP or H.323. If you have to "open" a port to allow these protocols through, then your firewall does not adequately support VoIP.

Reverse Proxies

Segment your VoIP traffic from your data traffic and consider using a multimedia gateway or reverse proxy. These devices offer greater security and are designed to handle VoIP traffic more efficiently than a traditional firewall.

Secure OS of Call-Handling Software

Use a commercial scanning tool to "probe" the call servers in your VoIP system. If any critical or high-level vulnerability arises, contact your vendor to have them corrected as soon as possible. Care should be taken to allow only necessary services to run and to limit the number of listening ports that could be attacked. This might warrant placing core VoIP devices in a "safe zone" behind a firewall or a router with access filters.

Routine Monitoring

Managed services are a good idea for firms without the resources to keep an eye on their networks. It also makes sense when your VoIP system becomes mission critical. You should establish daily, weekly, and quarterly milestones of activities to watch for.

Sound Security Practices

If already in place, a good data security program—strong passwords, anti-virus protection, reliable backup, and so forth—gives firms an advantage when implementing VoIP and should be maintained rigorously at all times thereafter.

Summary

It's clear that IP telephony is finally headed for prime time. However, the promise of mass VoIP consumption also increases the risk for widespread security violations. As VoIP usage increases, enterprises will become subject to many of the same security risks that heretofore have affected data networks.

There are any number of security risks that can adversely affect an enterprise: from denial of service attacks to unauthorized monitoring of calls; from impersonation of legitimate users to the ability of a malicious user to place fraudulent and damagingly expensive calls. And the community of hackers is constantly striving to stay ahead of the technology curve to wreak its madness.

However, increased awareness of security risks, a growing wealth of experience, and a mandate to maintain high levels of security in an ever-more connected world bodes well for future deployments of VoIP.

Solutions exist that allow enterprises to secure their networks for both voice and data. Every day brings a wealth of new information on how, when, and why to deploy methods to prevent attackers from gaining access to your critical enterprise information and from disrupting your business.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

Implementing Voice over IP
Fundamentals of Voice over IP
Advanced Deployment of Voice over IP
CVOICE – Cisco Voice over IP
Network Security I: Policy, Administration, and Firewalls
Network Security II: Integration and Implementation

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About Technology Marketing Corporation

Technology Marketing Corporation (TMC) publishes two magazines: *Customer Inter@ction Solutions*, and *Internet Telephony*, and the online publications, *TMCnet.com, Planet PDA Magazine, WiFi Revolution, SIPMagazine, Speech-World, WiFi Telephony Magazine, VoIP Developer, WiMAX Magazine,Alternative Power,* and *BiometriTech.*TMC is also the first publisher to test new products in its own on-site laboratories, TMC Labs. TMC also produces The VoIPDeveloper Conference, Speech-World Conference, IPContact Center Summit, and The Global Call Center Outsourcing Summit. TMCnet.com publishes more than 25 topical online newsletters. For more information about TMC, visit its web site at www.tmcnet.com.

Glossary

Codec – Coder/Decoder. A technique for compressing information to a fewer number of bits for more efficient transmission and storage (coding), and subsequently recovering the original data (decoding). Normally the term codec applies only to compression of human-perceived signals such as speech, audio, images, or video; and it usually refers to lossy compression.

CTI – Computer telephony integration.

Delay – The amount of time it takes for a signal to transfer or for the time that is required to establish a communication path or circuit.

DoS – Denial of service.

DDoS – Distributed denial of service.

Firewall – A data-filtering device that is installed between a computer server or data communication device and a public network (e.g. the Internet). A firewall continuously looks for data patterns that indicate unauthorized use or unwanted communications to the server. Firewalls vary in the amount of buffering and filtering they are capable of providing.

G.711 – A standard analog to digital coding system (coded) that converts analog audio signals into pulse code modulated (PCM) 64 kbps digital signals. The G.711 is an International Telecommunications Union (ITU) standard for audio codecs. The G.711 standard allows for different weighting processes of digital bits using mu-law and A-law coding. The G.711 standard was approved in 1965.

G.723 – An International Telecommunication Union (ITU) standard for audio codecs that provides for compressed digital audio over standard analog telephone lines.

G.729 – A low bit rate speech coder that was developed in 1995. It has low delay due to a small frame size of 10 msec and look ahead of 5 msec. It has a relatively high voice quality level for the low 8 kbps data transmission rate. There are two versions of G.729: G.729 and G.729 A.

H.323 – H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that may not provide a guaranteed Quality of Service (QoS). H.323 specifies techniques for compressing and transmitting real-time voice, video, and data between a pair of videoconferencing workstations. It also describes signaling protocols for managing audio and video streams, as well as procedures for breaking data into packets and synchronizing transmissions across communications channels.

ILEC – Incumbent local exchange carrier. A telephone carrier (service provider) that was operating a local telephone system prior to the divestiture of the AT&T bell system.

IP Centrex – The providing of Centrex services to customers via Internet protocol (IP) connections. IP Centrex allows customer to have and use features that are typically associated with a private branch exchange (PBX) without the purchase of PBX switching systems. These features include 3- or 4-digit dialing, intercom features, distinctive line ringing for inside and outside lines, voice mail waiting indication, and others.

IP PBX – A private local telephone system that uses Internet protocol (IP) to provide telephone service within a building or group of buildings in a small geographic area. IPBX systems are often local area network (LAN) systems that interconnect IP telephones. IPBX systems use an IP telephone server to provide for call processing functions and to control gateways access that allows the IPBX to communicate with the public switched telephone network and other IPBX's that are part of its network. IPBX systems can provide advanced call processing features such as speed dialing, call transfer, and voice mail along with integrating computer telephony applications. Some of the IPBX standards include H.323, MGCP, MEGACO, and SIP. IP PBX represents the evolution of enterprise telephony from circuit to packet. Traditional PBX systems are voice-based, whereas their successor is designed for converged applications. IP PBX supports both voice and data, and potentially a richer feature set. Current IP PBX offerings vary in their range of features and network configurations, but offer clear advantages over TDM-based PBX, mainly in terms of reduced Opex (operating expenses).

IP Phone – Internet protocol phone. A device (a telephone set) that converts audio signals and telephony control signals into Internet protocol packets. These stand alone devices plug into (connect to) data networks (such as the Ethernet) and operate like traditional telephone sets. Some IP Telephones create a dial tone that allows the user to know that IP telephone service is available.

ISP – Internet service provider.

Jitter – (1-general) Jitter is a small, rapid variation in arrival time of a substantially periodic pulse waveform resulting typically from fluctuations in the wave speed (or delay time) in the transmission medium such as wire, cable or optical fiber. When the received pulse waveform is displayed on an oscilloscope screen, individual pulses appear to jitter or jump back and forth along the time axis. (2-packet) The short-term variation of transmission delay time for data packets that usually results from varying time delays in transmission due to different paths or routing processes used in a packet communication network. (3-IP Telephony) The variance of interpacket arrival times.

LAN – Local-area network.

Latency – The amount of time delay between the initiation of a service request for data transmission or when data is initially received for retransmission to the time when the data transmission service request is granted or when the retransmission of data begins.

Malware – Software program developed for the purpose of causing harm to a computer system, similar to a virus or Trojan horse.

NIST – National Institutes of Standards and Technology.

PBX – Private Branch eXchange. A private telephone network used within an enterprise.

Phishing – The act of attempting to fraudulently acquire sensitive information, such as passwords and financial details, by masquerading as a trustworthy person or business in a seemingly official electronic notification or message (e-mail, IM).

PSAP – Public safety answering point. An agency that receives and processes emergency calls. The PSAP usually receives the calling number identification information that can be used to determine the location of the caller.

PSTN – Public switched telephone networks. Communication systems that are available for public to allow users to interconnect communication devices. Public telephone networks within countries and regions are standard integrated systems of transmission and switching facilities, signaling processors, and associated operations support systems that allow communication devices to communicate with each other when they operate.

QoS – Quality of service. One or more measurements of desired performance and priorities of a communications system. QoS measures may include service availability, maximum bit error rate (BER), minimum committed bit rate (CBR) and other measurements that are used to ensure quality communications service.

RTP – Real-time transport protocol.

SIP – SIP is an application layer protocol that uses text format messages to setup, manage, and terminate multimedia communication sessions. SIP is a simplified version of the ITU H.323 packet multimedia system. SIP is defined in RFC 2543.

SMB – Small and medium businesses.

SOHO – Small office, home office.

SPIT – Spam over Internet telephony.

UPS – A battery backup system designed to provide continuous power in the event of a commercial power failure or fluctuation. A UPS system is particularly important for network servers, bridges, and gateways.

VoIP – A process of sending voice telephone signals over the Internet or other data network. If the telephone signal is in analog form (voice or fax), the signal is first converted to a digital form. Packet routing information is then added to the digital voice signal so it can be routed through the Internet or data network.

WAN – Wide-area network.