

VoIP: The Evolving Solution and the Evolving Threat

Copyright© 2004 Internet Security Systems, Inc. All rights reserved worldwide

 **INTERNET | SECURITY | SYSTEMS®**
Ahead of the threat.

Introduction

Voice over Internet Protocol (VoIP) is an evolving telephony solution that brings voice and data traffic together on the same IP-based network. As a result, VoIP is becoming an increasingly appealing alternative for more enterprises seeking to gain cost efficiencies and enhanced features.

Enterprises wishing to exploit the advantages of switching voice calls to the IP network must understand that maintaining security of those packets is an integral part of the overall VoIP deployment. Focusing on quality of service and throughput is certainly important, but ensuring the integrity of voice transmissions and guarding against malicious activities and access is crucial to the success of the evolving solution.

VoIP – The Evolving Solution

VoIP / IPT Defined

Voice over Internet Protocol and Internet Protocol Telephony (IPT) are two evolving solutions that are switching phone transmissions from analog to digital. Compiling and transporting a voice conversation digitally offers organizations many new benefits, saving them money and introducing new and more advanced features.

- Voice over Internet Protocol calls originate in analog form but are later digitized and separated into digital packets (via a “vocoder”) for transport over Internet Protocol (IP)
- Internet Phone Telephony is a technology in which calls originate in digital form (vocoder function is housed in either an IP Phone or a PC-Based IP Phone) for transport over Internet Protocol.

For the purposes of this whitepaper, VoIP and IPT are used interchangeably and together are referred to as VoIP.

These two technologies have been around for several years. Their recent popularity is due to their role in defining and driving the concept of a “converged network”.

The Converged Network

“Converged networks” — bringing disparate applications onto a unified framework — have already found their way to a number of organizations. The idea behind converging related but distinctly deployed applications or services is driven by cost efficiencies and process improvements. By porting voice transmission responsibilities to the IP-based data network, organizations can begin to achieve significant cost improvements by utilizing the efficient switching, routing and transport capabilities inherent in an IP-based data network for the purpose of routing and terminating voice transmissions.

The IP-based structure of the data network also allows for more feature-rich communication applications at a lower cost of deployment. Organizations that utilize, rely on and deploy a significant amount of telecommunications infrastructure, such as call centers, large inside sales and telemarketing operations, can significantly enhance their customer relationship execution by introducing more IP-based, feature-rich communications services.

VoIP / IPT Deployments

Dedicated VoIP over local area networks (LAN) / wide area networks (WAN)

A dedicated VoIP over a LAN / WAN configuration may also be described as enterprise-dedicated VoIP. These deployments represent the use of VoIP within the network definition of a single enterprise — transmitting voice traffic over dedicated facilities between offices. The “dedicated” label implies that the traffic does not connect with an outside service provider framework such as the public switched telephone network (PSTN) or that of an Internet service provider (ISP). This label and construct does not imply that this structure is free from attack.

Open VoIP and the PSTN

Open VoIP and the PSTN refers to deployments where voice calls either originate or terminate in traditional analog form and at switch to the PSTN for a portion of the call. In this case, the analog portion of the calls would take place outside of the enterprise. The term “open” implies that at some point the call travels over an uncontrolled — from the enterprise’s perspective — or unsecured network.

Open VoIP and an ISP

Open VoIP and an ISP deployment involves a minimum of two stages in the IP portion of call handling, where calls originate or terminate on the enterprise’s IP network and at some point are handled by the IP network of an ISP. These calls may also be analog and travel over the PSTN at some point, depending on the technology at the originating or terminating point. Again, “open” refers to the fact that at some point, the call is outside the control and oversight of the enterprise.

VoIP: The Evolving Threat

Why VoIP is Vulnerable

Deployment Focus

VoIP networks exist and operate in a state of high vulnerability simply due to the nature of how and under what metrics they are initially deployed. Organizations deploying VoIP today initiate the process with a primary or sole focus on throughput and quality of service. Security issues are often secondary if considered at all. Service quality is and always will be an important component of voice transmission in both analog and digital forms. However, organizations must realize that voice in a digital packet form is highly susceptible to the same — or possibly greater — number of attacks as the core data network.

VoIP is Data

VoIP is data and is transmitted in digital packet form. This means that the voice transmissions can be now attacked, hacked, intercepted, manipulated, re-routed and degraded just as any data packet on the data network can. Viruses, worms, trojan horses, denial of service attacks and hijacking are all possibilities on the VoIP network.

Immature VoIP-Oriented Operating Systems

VoIP is a nascent market and early-adopted technology, and the underlying operating systems that deploy and support VoIP processing can be viewed similarly, which means that these operating systems and applications are as vulnerable as data network-based operating systems were in the early stages of their development and deployment.

Operating systems and supporting applications are also often installed using their default configuration, which has little or no security structure, therefore ensuring that the system or application is vulnerable from the moment it becomes operational.

Where VoIP is Vulnerable

VoIP deployments generally make use of at least three tangible components and operate over various signaling and transport protocols. The components and protocols play a vital role in the management and transmission of the data packets, and also represent weak points and opportunities for malicious activities.

The End Points/Customer Premise Equipment

The IP Phone is a new desktop phone configured and equipped specifically for IP-based voice calls. Vulnerabilities in the underlying operating system and supporting software dedicated to the specific unit introduce risks.

The PC-Based IP Phone, a software application that provides IP phone capabilities via the user's PC, is susceptible to attack as a result of its relation to the underlying operating system and installed applications on the PC. In addition, the PC resides on the data segment of the portioned network, which may allow for crossover attacks originated in the VoIP segment and vice versa.

The Central Administration/Call Processing and Management Application

The central administration/call processing and management application acts as the "switch" for IP-based voice traffic. This application often is installed and runs on a dedicated server or PC and is subject to the same security issues as any server or PC in the network or enterprise. The central administration/call processing and management application is the most vital link in the VoIP architecture but is seen as the "single point of failure" and therefore may be the most common target of attack.

The Voice Mail System/Server

The voice mail system/server is the storage, retrieval and "auto-attendant" mechanism for IP-based voice mail. The voice mail server would be a likely target for "prank-oriented" attacks — such as altering messages — in addition to standard attacks such as eavesdropping, spamming and others.

The Protocols

VoIP utilizes several protocols for establishing, maintaining, transporting and terminating the voice calls represented by digitized voice packets. The call or session management protocols (Session Initiation Protocol or SIP and H.323) are responsible for establishing, maintaining and terminating the call and are susceptible to common attacks such as attempts to overflow one of the central administration/call processing and management application's buffer, which the attacker uses to establish "root access." The call transport protocols, such as Real-Time Transfer Protocol (RTP), will undoubtedly present vulnerabilities themselves due to the fact that they are relatively new and evolving and have yet to receive a great deal of "real world hardening."

How VoIP Can Be Exploited

As illustrated earlier, VoIP has inherent weaknesses and is vulnerable at multiple points in the framework. VoIP must be secured in order to ensure the availability of the voice system, protect the content value of voice conversations and protect the integrity of the overall communications system.

Due to its default construction and deployment, VoIP is susceptible to a number of easily anticipated and defined attacks. A few of these are defined and assessed below:

Primary Types of Attacks

Service Disruption or “Denial of Service” (DoS) — DoS attacks are generally the most simple and thus most common type of attack faced by data networks. For VoIP, the attack would simply bombard the call processing/managing application with an inordinate amount of simultaneous requests that it cannot process, causing the application to essentially shut down and deny service to authorized and intended users. Calls in process would be abruptly terminated and any attempt to originate a call would be unsuccessful.

Primary risks of successful denial of service attacks include loss of revenue due to lost sales call volume, negative customer experience resulting from lost support calls and productivity lost as communications with remote offices drop off.

Toll Fraud/Service Theft — Toll fraud or service theft will likely be the most common attack or exploit that will be seen, at least in the early stages of VoIP deployment. The attack would simply take the form of an unauthorized user gaining access to the VoIP network by mimicking an authorized user or seizing control of an IP Phone and initiating outbound long distance calls. This is one of the most common forms of fraud or “hacking” in the PSTN environment, particularly for expensive, international toll calls.

Risks include increased expenses and decreased productivity as billing issues must be investigated and resolved.

Eavesdropping — VoIP services measurement and troubleshooting software make eavesdropping on a packetized voice call possible. Hackers can take the data and convert it into a WAV audio file.

Lost revenue, and disclosure and compliance issues are among the risks of successful VoIP eavesdropping.

Phishing — “Phishing,” an attempt to obtain information from someone by posing as a legitimate party, is becoming more and more prominent over e-mail, but the same tactics can be used over VoIP if an unauthorized user begins calling individuals in the organization and initiating requests sensitive information using a legitimate name and phone extension.

For example, someone receives a call from an extension in human resources wanting to make sure records are up-to-date and asks to verify their name, Social Security number and date of birth. Once obtained, this information is a simple launching pad for identity theft. This exercise could also be used to obtain sensitive customer information as well.

Primary business risks include legal exposure from the release of employee and/or customer information.

Other Types of Attacks

Call Re-Direction: Sends all outgoing or incoming calls to an incorrect destination via unauthorized access to the call processor/manager

Information Theft: Data, including names and phone extensions, obtained via unauthorized access to voice mail servers or to the call processor/manager

Call Integrity Compromise: Altering or corrupting call content or modifying packet sequencing, thus degrading quality

Internet Security Systems and VoIP Security

Proventia® Enterprise Security Platform

The Proventia Enterprise Security Platform (ESP) from Internet Security Systems (ISS) is founded on the concept of preemptive protection and is easily and directly extendable to the security requirements for enterprise VoIP deployments. Proventia ESP leverages the industry-leading security products and services from ISS within a framework that allows enterprises to identify vulnerabilities, prioritize the required protection, provide the necessary patching and ultimately report and benchmark on the overall security process.

The preemptive approach to security becomes more even relevant with VoIP deployments, since there is potential for new attack, and so few have been launched. Proventia ESP shields vulnerabilities from attack, ensuring voice system availability and sustained operations and productivity.

X-Force® Research

Internet Security Systems (ISS) is uniquely positioned in the security industry thanks to its X-Force security intelligence team, a group of 100 dedicated security engineers responsible for investigating, cataloging and providing guidance relative to evolving cyber threats and application vulnerabilities. The X-Force has compiled the industry's largest proprietary security knowledge database and leverages this database in their role as an independent and unbiased advisor for the organizations they support.

The research conducted by the X-Force underpins and serves as the key differentiator for all of ISS' security offerings. The X-Force has a dedicated research team focused on VoIP-related security issues, including vulnerabilities, attacks and protocols, and the results of this research and discovery are already embedded in the appliances and applications deployed by ISS today.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS**Australia and New Zealand**

Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific

Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa

Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

About Internet Security Systems, Inc.

Internet Security Systems, Inc. (ISS) is the trusted expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers worldwide. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call **800-776-2362**.

Copyright© 2004 Internet Security Systems, Inc. All rights reserved worldwide

Internet Security Systems is a trademark, and the Internet Security Systems logo, X-Force and Proventia are registered trademarks of Internet Security Systems, Inc. All other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

MC-VOIPWP-1204