IP Telephony Security—A Double-edged Sword?

WHITE PAPER

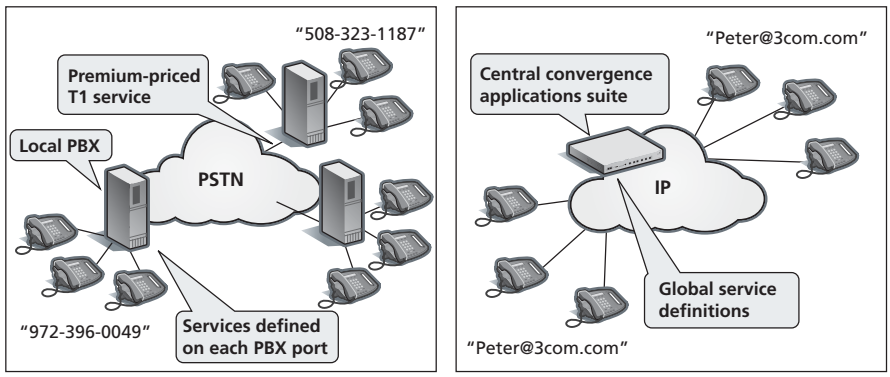
CONTENTS

Why IP Telephony—Now?

In the last five years, advances in networking technologies have enabled convergence of telephony as an application on IP networks. Enterprises have taken advantage of IP telephony for a variety of business-critical benefits:

- Cost savings due to toll bypass and bandwidth consolidation
- Simplified voice network engineering
- Reduced legacy PBX equipment requirements
- Consolidation of wiring infrastructures for voice and data via Ethernet
- Consolidation of directory and other infrastructure data for voice and data
- Natural mobility by leveraging inherent IP network capabilities such as DHCP and DNS, IP based wireless enterprise networking and remote access through the Internet
- Appearances on multiple phones to simplify lives of users who work from different locations including office, conference rooms, remote locations, and home
- Client devices such as IP phones that are more user-friendly, feature-rich, and standards-based than their TDM equivalents
- Availability of new applications and services resulting from increased speed-to-market product development
- Integration with applications due to web-friendly interfaces supported by IP telephony protocols such as SIP

Figure 1. Convergence transforms telephony.



- Smart network, dumb devices
- Locally-delivered features
- Scale via hardware investment
- Some of the bandwidth, all of the time
- Location-specific addressing
- Rigid 10-digit numbering plan
- Voice only
- Conferencing - hardware dependent

- Smart devices, dumb network
- Globally-delivered features
- Scale independent of hardware
- All of the bandwidth, some of the time
- Location-independent addressing
- Flexible, mnemonic numbering plan
- Voice, video, real-time collaboration
- Conferencing via software

A Double-edged Sword?

Most of the benefits of IP telephony are due to architecture-enabled transformation of telephony. Such transformation is enabled by implementing telephony and other convergence applications in location independent application servers. These servers can be deployed anywhere on the IP network as long as performance requirements are satisfied and connectivity exists between the servers and their clients (other applications and end-user devices).

Because IP telephony is implemented using client-server architecture based on the well-known, well-publicized, and open Internet Protocol, it is subject to the same security vulnerabilities of any IP network-based client server system. The problem with standards is that they're open: open to third parties, open to university researchers, open to systems manufacturers, and of course, open to unintended consequences—like hacker attacks, viruses and toll fraud.

Despite this exposure to unintended consequences suffered by exposed IP telephony systems, proprietary systems that don't rely on open standards are considered even less secure. Open systems such as IP or Session Initiation Protocol (SIP) leverage the power of collective security. Viruses, worms, and system vulnerabilities can be minimized or even avoided by the rapid dissemination of information through industry associations like the Computer Emergency Readiness Team (**www.cert.org**) at the Software Engineering Institute.

Fortunately, the benefits of standards-based IP telephony outweigh the cost of unintended consequences. To help enterprises blunt the double-edged sword of IP telephony implementations, this white paper offers the following information:

- Components of IP telephony systems that are vulnerable to security threats
- Possible security threats in an IP network
- Impacts of the security threat on IP telephony systems
- Solutions optimized to cost-effectively protect each of the vulnerable components of the IP telephony system

Enterprises can reduce the cost of security exposures and the uncertainty resulting from lack of knowledge on the subject. Well-armed, they can protect and defend themselves.

Vulnerabilities in IP Telephony

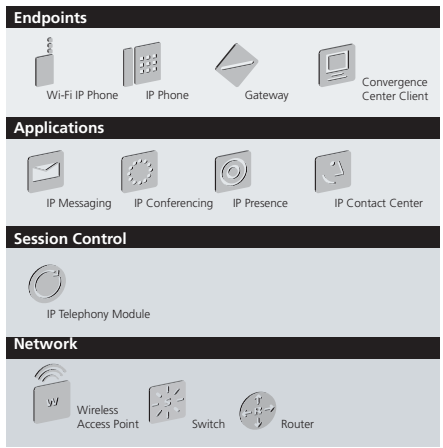
Today, enjoying the benefits of using any combination of modern computers, software, and networks is not without its challenges. There are several attacks that impact client server systems, including IP telephony services within an IP network. The following list of five threats are particularly significant:

- Distributed Denial of Service (DDoS)
- Eavesdropping
- Toll fraud
- Spam
- Virus

Threats and best practice responses can be identified based on four broad layers of functionality within IP telephony architecture—network, session control, applications, and endpoints. (See Figure 2.)

- **Endpoints**—phones, clients, and gateways are vulnerable to distributed denial of service attacks as hosts that enable viruses, toll fraud, and eavesdropping.
- **Applications**—like endpoints, software products running on computers can be victims or hosts in distributed denial of service and virus attacks or as spam targets.
- **Session Control**—IP telephony systems have centralized software services to coordinate network resources for the interaction of applications and endpoints.
- **Network**—wireless access points, switches, and routers are vulnerable to packet floods caused by viruses and distributed denial of service attacks.

FIGURE 2. Security risks categorized by four infrastructure layers



Distributed Denial of Service

The 3Com® Convergence Applications Suite runs on a specially tuned, reduced 3Com Linux operating system where non-essential services are turned off.

The 3Com switch portfolio can automatically recognize 3Com IP phones and insert them into the IP telephony VLAN.

3Com solutions support traffic shaping and packet prioritization for audio quality. The 3Com VCX™ IP Telephony Module supports 3Com Voice Boundary Routing, assuring high availability and low-cost backups and failovers.

Overview

Distributed Denial of Service (DDoS) attacks are designed to flood a target computer, network, or network link with an overwhelming number of spurious service requests or malformed packets, preventing the reasonable handling of legitimate packets and service requests. Hundreds or thousands of computers contribute a tiny portion of their processing power to this distributed assault, making detection of the resulting mayhem difficult. In aggregate, they form a considerable threat.

These attacks use a network of unsuspecting agents (computers) to deposit simple agent programs that listen for attack commands on innocuous Internet Relay Chat services, leveraging identified operating system vulnerabilities. Handlers recruit and control these networks of agents. On command from the client, they unleash them onto the target.

Common attacks involve:

- exploiting mechanisms such as the Internet Control Message Protocol (ICMP) which is used for router-to-host communications and is intended as a method for providing feedback to the host about communications environments
- transmitting a volume of connection requests to the target from phony IP addresses that are never acknowledged in order to overflow the connection management buffer
- delivering User Datagram Packets (UDP) to random ports on the agent with forged source; the target naively and unnecessarily processes the packets, discovers that there is no application waiting for the UDP, and then sends a response packet to the target
- broadcasting forged ICMP echo packets to subnets with the target forged as the packet source; the hosts on the subnets respond to the target with ICMP echo packets and overwhelm the target host, network, or network link with bogus packets to cause the denial of service

Impact

Clients such as PC based soft-clients and IP phones, as well as telephony and convergence applications servers using operating systems or other foundation software platforms with well known vulnerabilities are affected by DDoS. DDoS attacks cripple client and server computing systems by causing them to perform unproductive tasks and denying them any resources to perform their intended functions. Left unchecked, such attacks can render telephony systems inoperable. In addition, they can cause enormous amounts of unproductive traffic within the network, denying any bandwidth, routing, or switching resources for transport of telephony control and media traffic such as voice or video.

Solution

Protocol tuning in endpoints, applications, and session control:
Software engineers need to establish buffer limits on attempts at malformed packet assembly and session initiation requests. A favorite technique of DDoS attacks is to consume server resources through flooding the server with service requests or malformed packets which consumes processor cycles and leaves no capacity for legitimate applications.

Support for IEEE 802.1Q:
Modern network switches today support IEEE 802.1Q virtual LAN (VLAN) services to segment IP telephony traffic from other network applications and sources. This degree of internal isolation makes it more difficult for compromised PCs or applications to affect IP telephony VLAN-attached endpoint devices.

Support for seamless service continuity:
To maintain quality telephony service for the enterprise and optimize security precautions, communications networks should include fast failover session control services that will quickly backup modules elsewhere in the enterprise network if needed.

Preventing attack damage:
A new product category, the intrusion prevention system, is a powerful combination of control software and silicon that performs very fast and very deep packet inspection. Vulnerabilities in protocols such as SIP and H.323, traffic signatures of attacks, and even packet anomalies can be detected and halted in milliseconds before the protected applications and systems are affected. The Digital Vaccine® service closes the gap between vulnerability reporting and network inoculation.

Operational Practices

Best practices in enterprise security combine products and business practices.

For example:

- Implementing a policy of not exposing IP telephony session control servers to the Internet
- Use of telephony protocol cognizant firewalls (such as SIP-capable firewalls) to isolate an enterprise IP telephony system from the Internet

- Deployment of VPN routers or proxy servers to traverse firewalls and balance security with user convenience and cost
- Deployment of IP telephony VLANs for IP phones, gateways, applications, and session control servers to minimize cross-application performance risks
- Use of an intrusion prevention system to complement the LAN switching fabric by responding to packet anomalies, protecting known vulnerabilities, and recognizing performance signatures of attacks

Eavesdropping

Overview

Eavesdropping is not a new or special attribute of IP telephony. Years ago, it was common for users to share a party line and listen, often inadvertently, to their neighbors' conversations. As recently as 1995, analog radio scanners enabled listening to police and emergency networks to hear about the burglary down the street or car-chase at the south end of town. Analog cell phones were so open that anyone could eavesdrop on cellular conversations, including significant political or business discussions.

At first glance, aspects of IP implementations would appear to make eavesdropping particularly easy. In IP telephony networks, packets are routinely duplicated for audit purposes or packet assembly function. Thus, audio signals that are transported as packets can be stored for later retrieval and recombination into cohesive speech. Associating such speech packets with a conversation, however, requires retrieval of telephony call or session details which occurred asynchronously and perhaps through a different network path compared to the speech packets, and correlating them with the reassembled speech packets. Therefore, while it is technically feasible in IP telephony networks to eavesdrop, in practice it is quite hard.

Impact

The endpoints and the session control layers are most likely the targets of eavesdropping attacks—one of the endpoints, the gateway, the IP phone, or the PC client is probably the only component directly in the path of the audio stream. The network layer transports all the packets of the corporation, so finding specific IP telephony packets of interest may be difficult.

The session control layer is a point of attack since it knows which endpoints are communicating with each other at any moment in time. It could provide the interloper with enough information to induce the network to yield those specific packets or authorize duplicate packet streams to a third IP endpoint.

Solution

Encryption is commonly thought to be the most effective tool against eavesdropping, but it is not without a significant cost in processor time, inconvenience, and interoperability. Some of these issues can be alleviated with standards-based encryption systems.

In IP telephony, the packet stream is most often delivered as Real-Time Protocol (RTP). Secure RTP (SRTP)—a current Internet Engineering Task Force (IETF) draft—provides a security profile for RTP specifically addressing IP telephony applications that adds confidentiality, message authentication, and packet replay protection to the packet,

SRTP is intended to secure only RTP and the Real-Time Control Protocol (RTCP) streams, not to provide a full network security architecture. SRTP uses the RTP/RTCP header information, along with the Advanced Encryption Standard (AES) algorithm, to derive a keystream algebraically applied to the RTP/RTCP payload. SRTP calls for the Hash-based Message Authentication Code (HMAC) - SHA1 algorithm to be used for packet authentication.

There are additional component interactions that can strengthen privacy protection. The session establishment dialog, commonly using Session Initiation Protocol (SIP), is also standardized within a privacy implementation as SIPS and defined in IETF RFC 3261. Within SIPS, call control messages are transmitted within a Transport Layer Security (TLS) encrypted session, at least through the hostile IP environments where prudent policy might indicate the advantage of strong privacy protection in session initiation dialogs.

Easier and less costly protection can be achieved with a modern Ethernet switch feature called automatic virtual LAN segmentation (implemented as IEEE 802.1Q). This technique logically restricts access and packet flow to well-defined and well-understood endpoints. Devices on the IP telephony VLAN are segmented separately from devices on another VLAN and their two traffic flows

do not mix. Performance impacts and issues in one VLAN do not impact the other VLAN. Endpoints receive only those packets to which they are entitled.

The latest generation of wireless LAN environments assure over-the-air privacy using IEEE 802.11i. The standard enables strong privacy, message integrity, and authentication service. Furthermore, rapid setup of virtual LAN tunnels to maintain addressing and RTP flow integrity let wireless switches deliver call hand-offs from access point to access point or from subnet to subnet. This functionality enables IP telephony deployments over a wireless LAN campus to deliver performance that is consistent with user expectations set by public cellular network service.

3Com wireless switching solutions enable cross-domain mobility for IP telephony over Wi-Fi environments.

In addition, wireless switch management capabilities help detect, neutralize, and manage rogue or interfering access points that users may encounter.

Operational Practices

Using network features like VLAN segmentation to protect against infiltration of the logical segment makes the eavesdropper's task more difficult.

Implementing 802.11i authentication services and wireless switching within Wi-Fi environments are essential to successful IP telephony mobility within the enterprise.

Generally, encryption is required only where the risk of eavesdropping exceeds the cost of providing privacy service. A useful guideline is the availability of encrypted e-mail within the enterprise. Contents of e-mails are often far more critical and private than content shared in a phone conversation. Therefore, one can expect an enterprise to encrypt e-mail before being concerned about lack of encryption in IP telephony.

Toll Fraud

Overview

Toll fraud is long distance service theft with a long history of practice and profitability. Although the attractiveness of stealing long distance (LD) minutes has been diminished by falling LD rates in Canada, the United States, and most European countries, international dialing is a choice target even today.

Fraud happens as a result of:

a. "social engineering"—employees or auto attendants unwittingly transfer callers to outside lines or to premium 900-style information services

b. voice mailbox theft—the message "hello" pause "yes" pause "I accept the charge" is recorded on the mail box, allowing third-party pay calls to be sent to the mail box to get permission

c. calling-card number theft—video capture of dialers or line bridging of public pay phones to obtain dialed digits for unauthorized use and resale

d. reconfiguration of PBXs—hacking through the maintenance modem, resulting in the ability to configure unauthorized extensions to forward to trunks for long distance theft

Impact

Endpoints and applications are most often targets of toll fraud because they enable features for call forwarding and social engineering. Applications, and in particular voice mail, are also targets for toll fraud perpetrators.

Solution

Features for avoiding toll fraud are readily available in typical IP-PBX and PBX products.

Operational Practices

A critical best practice that can be implemented to avoid toll fraud is training receptionists and call center employees in social engineering avoidance. Training should include information about the cost of toll fraud, the techniques used to perpetrate the fraud, steps to avoid the fraud, and processes for reporting incidences should they occur.

Another practice is to shutdown all unassigned voicemail boxes and take steps to educate users in password selection—avoid simple, easily stolen passwords such as the default password or 1-1-1-1. Periodic password rotation procedures and aging mechanisms do increase the number of calls into IT help desks, but also increase security.

Most IP PBXs do not have maintenance ports for remote modem dialup. IP-PBX support professionals often choose to use their browsers with VPN enterprise network access for remote support service or for access to the management system dialog. Therefore, methods for accessing the PBX maintenance ports deserve examination.

Spam

Overview

Spam—unsolicited e-mail—was recently regulated in the United States by the CANSPAM Act of 2003. Most spam is commericial advertising, often for dubious products. However, as every user can attest, spam is a problem of epidemic proportions on the Internet. Because e-mail accounts can receive ten times more spam than legitimate e-mail, major Internet Service Providers such as AOL, MSN, Earthlink, and Yahoo! have implemented strategies and technologies to reduce the volume of junk mail arriving in their users' inboxes. Market estimates indicate that between 38% and 80% of all e-mail in North America, more than 11 billion pieces of e-mail, is spam.

Users are spending significant time, money, and IT resources dealing with spam-related issues. Spam comsumes bandwidth and storage space. It also acts as a launching pad for virus attacks on enterprise networks. And, though instances have not yet been reported, an IP telephony version of spam called spit can deliver unsolicited advertising as voice mail or interrupt conversations with injections of nuisance or nonsense words.

Impact

Spam most directly affects the applications layer. Some applications such as voice mail as e-mail or read-me services integrate with e-mail services, making them particularly vulnerable to spam.

Solution

The Simple Mail Transport Protocol (SMTP) feature should be disabled when read-me e-mail service is not required or enabled as an appropriate feature. All other applications should send, but not receive e-mail. And to reduce the incidence and productivity impacts of spam, enterprise e-mail servers can include anti-spam enhancements or modules such as spam-assassin or the 3Com® Email Firewall appliance.

Operational Practices

E-mail management practices can minimize spam production, distribution, and its effect on IP telephony systems and user services. Effective best practices ensure that authentication services require server accounts and passwords for sending messages from the SMTP server and receiving them from the POP3 or IMAP4 servers.

Analytical services can remove messages written in common spam techniques—such as using all capital letters, including forbidden terms—and delete known harmful attachments or extensions. Spam can also be combated by the use of black lists that deny mail from domains of known spammers.

Virus

Overview

Viruses are resource-consuming software programs that deliver no real value to the computer owner. Some are harmless or nuisances, while others can harm networks, applications, operating systems, and data. Examples include:

- lengthy e-mails warning of viruses and recommending precautions that don't work or will cause PC problems, minor or serious
- programs that send themselves to all addressees in an e-mail address book
- spyware that transmits every keystroke or participate as agents in Distributed Denial of Service attacks

Impact

Viruses plague all layers. They clog the network with unnecessary and useless packets and messages, and they exploit weaknesses in the operating systems of session control applications that lead to network instability. Viruses also act as launching pads for DDoS attacks.

Solution

The most obvious solution for avoiding viruses and their potentially devastating impact is to avoid IP telephony products based on operating systems with well known vulnerabilities.

Microsoft Windows operating systems may have the most publicized vulnerabilities due to their popularity, large community of independent software developers (ISV), and comprehensive Microsoft documentation. Even in cases where a well-known vulnerability has been effectively solved by Microsoft, many Windows installations continue to be vulnerable due to the complexity of Windows installation. Windows places special burdens on installation. IT staff must ensure that the

The 3Com TippingPoint Intrusion Prevention System (IPS) delivers wire-speed deep packet inspection along with a Digital Vaccine service that can quickly adapt to new virus threats.

The 3Com Email Firewall strips away unproductive spam and viruses before they contaminate corporate e-mail servers.

dozens of available security patches are installed correctly and up-to-date. Therefore, Windows platforms are often the favorite target of the nefarious virus development community.

Windows platforms may be unavoidable in the enterprise desktop environment, but should be critically evaluated for use in the server farm and for mission-sensitive applications.

Depending on the market segment served, operating systems may be tightly coupled to the IP telephony system hardware; such is the case with the 3Com NBX® IP Telephony Module for small businesses and medium enterprises. Using the VxWorks real-time operating system derived from a UNIX distribution, NBX systems have been successfully deployed in over 19,000 environments without a single case of virus attack. A tight coupling of the platform and the application can also assure a high degree of security with the added benefit of simplifying and accelerating installation and maintenance.

In the larger enterprise market, the 3Com VCX™ IP Telephony Module features substantial security enhancements to the Linux operating system such as built-in firewall packet filtering and severe restrictions on available or used platform ports. The VCX solution gives customers the use of industry-standard processors and industrial-grade high-performance applications. And 3Com Voice Boundary Routing[1] can help assure seamless backup and failover of VCX IP telephony modules so that phone users are protected from service disruption.

Preventing attack damage:
As already described, the intrusion prevention system can prevent virus attacks that exploit vulnerabilities in protocols such as SIP and H.323, traffic signatures of attacks, and even packet anomalies. The IPS proactively detects attacks and prevents them at the network level in milliseconds before the protected applications and systems are affected. The Digital Vaccine service closes the gap between vulnerability reporting and network inoculation. This automatic inoculation methodology reduces reliance on the manual application of complex patches and virus definitions to server and client systems, mandated by software platform and operating systems vendors.

Operational Practices

Despite their prolific attributes, viruses in enterprise networks can be controlled through vigorous hygiene procedures that remove or quarantine known infectious objects on incoming e-mail.

Commercial anti-virus programs from companies like Symantec or McAfee can be deployed on user desktops. These applications provide control of common viruses through active, background tasks such as file and process inspection. Most often these products provide subscription services available as individual or enterprise-wide licenses. The products periodically can check for updates that are automatically downloaded and deployed on the computer.

Summary

As one of many applications that rely on IP networks, IP telephony implementations are vulnerable to several well-known security threats. The following table indicates five threats that may affect IP telephony system components.

	DDoS	EAVESDROPPING	TOLL FRAUD	SPAM	VIRUS
Endpoints (clients)	✓	✓	✓		✓
Applications (servers)	✓	✓	✓	✓	✓
Session Control (servers)	✓	✓			✓
Network (infrastructure)	✓			✓	✓

To protect the integrity of its brand, infrastructure, business processes, operations, and IP telephony infrastructure—and the trust of employees, partners, and customers—organizations must be responsive to changing threats. They must track adoption of periodic security audits, participate in industry collaborative efforts such as the federally-funded Carnegie-Mellon University Software Engineering Institute's CERT (**www.cert.org**), and implement security awareness initiatives within their user community. IT professionals should also become familiar with collaborative projects such as the non-profit VoIP Security Alliance (**www.voipsa.org**) which is dedicated to sharing research, knowledge, tools, and best practices.

[1] See the 3Com white paper Voice Boundary Routing: The Case for IP Telephony in Branch Networks, 2004 at http://www.3com.com/voip/whitepapers.html

3Com has been a major contributor to the convergence industry since 1998 when the 3Com NBX solution liberated users of business telephone systems from the tyranny of complexity. In 1999, the company developed an architecture for a distributed softswitch for AT&T and brought the first commercially-deployed carrier softswitch to market. The 3Com VCX platform (2003) and the 3Com Convergence Applications Suite (2004) indicate the company's continuing focus on transforming business through innovation.

As a founding member of the VoIP Security Alliance and with over 16,000 patents (plus more than 500 pending), operations in over 45 countries around the globe, a market-leading portfolio, and over 19,000 systems deployed worldwide, 3Com is changing the way business speaks.

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

503152-001 04/05