APPLICATION NOTE

ST-0118 July 28, 2005

Product: ShoreTel system **System version:** ShoreTel5 Release2

Network Security Best Practices for IP Telephony

Deploying IP telephony in a secure manner means following the best practices in secure network design, and in today's world, this demands more than placing a firewall between the LAN and the Internet. Enterprises must design their networks from the ground up with security in mind. Only with this solid footing can IP telephony be added to the network safely and securely.

Overview

The security threat is rising — in the form of worms, viruses, spam and other malicious software. At the same time, the penalties for security breaches are becoming increasingly severe — ranging from losing customers' trust to incurring financial and legal liabilities for failing to comply with privacy regulations and other laws.

This application note highlights some of the best practices in secure network design as well as unique considerations for securing IP telephony.

The first step in determining the right network security strategy is to understand the risks to the availability and privacy of your organization's information resources. After assessing the risks at hand, companies can put in place the strategies and best practices that will protect their sensitive information and protect their network systems.

Because network security is growing increasingly complex, more companies are relying on qualified security experts for guidance and consulting. If your organization does not have the relevant internal resources, you should consider bringing in consultants help to design a secure network.

Understanding the Risks

The first step in securing your IP telephony system is to understand the major risks facing networks and telecom systems today. Protecting your organization's IT infrastructure means constructing a multi-layer defense against network-based attacks, eavesdropping, service theft and evolving threats.

This main threats are summarized here:

- **Network-based Attacks.** An attacker may unleash a worm or denial-of-service (DoS) attack to interrupt network service. A DoS attack floods the network with so many additional requests that regular traffic is either slowed or completely interrupted. As with other IP applications, VoIP is susceptible to DoS attacks, including malformed requests, media attacks, and flood attacks.

  Blended threats like using spam to deliver worms are fast becoming the preferred method of spreading malicious code. Spyware and phishing are used to commit identity theft and other fraud.

- **Eavesdropping.** Hackers may eavesdrop on conversations which could lead to the exposure of confidential information. An unscrupulous employee could tap into the CFO's conversation and turn a private discussion about the company's financial earnings into a media file that can be replayed. Voice must be protected from unauthorized recording and replaying and other forms of electronic snooping over the network.

- **Service Thefts.** A phone system is subject to inappropriate uses and service thefts, such as hacking into the PBX to make hundreds of international calls. IT managers often overestimate the impact of service thefts, which is a risk well-known to telecom managers.

- **Rapidly Evolving Threats.** Attack vectors evolve rapidly. One new attack is to spoof the phone number of a legitimate caller on a caller ID display, which can be used for a variety of social engineering or identity theft scams.

  Your organization may be subject to SPIT, or spam over the Internet. Even cell phones are fair game for viruses, spam and embarrassing exposures of private information.

Network Security Best Practices

Secure IP telephony is predicated on strong network security. The majority of security measures to protect IP telephony are network-related, including virtual private networks (VPNs), firewalls and rate shaping, which are not specific to IP telephony.

IP telephony on the local network can be made very secure. Voice is essentially another application on the internal network, so the same precautions used to secure other applications can and should be used to secure voice.

IP telephony among corporate locations can also be made very secure. In a multi-site deployment, calls flow among locations over a private network, which could be a managed network, point-to-point connections, or IP connections using a WAN service provider with encrypted VPN tunnels between locations.

Taking a systematic approach to network security means organizations should consider physical security, human security, network security and systems security. Organizations should seek experienced security consultants to address these issues completely and cost effectively.

- **Physical Security.** Look at physical security as a series of concentric perimeters, with each layer more secure than the previous one. Your buildings, wiring closets and data centers must be adequately locked and secured — and accessible only by authorized personnel. No amount of network security helps if a thief breaks into a server room or walks off with the CEO's laptop.

  Security Policies. More than 80 percent of security breaches are the direct result of insiders, according to Gartner's report "Reduce the Risk of Data Leaks With Content-Filtering Tools." Whether accidental or intentional breaches, you must be prepared to protect the company's information assets against inappropriate or unauthorized use.

  Many IT managers and staff have unfettered access to all data by design. A renegade IT manager can pose a significant security threat

to information and voice systems alike. With the appropriate administrator permissions, an IT manager can view employees' salaries, view all e-mails sent and received, and breach other corporate trusts regardless of whether the voice conversations are secure.

Make sure that you have hiring policies and usage polices that govern appropriate use of corporate electronic resources. Users who write their passwords on yellow stickies and then paste them on their monitors may be an old joke among IT professionals, but it happens — frequently. Establish and enforce policies that require passwords to be a combination of numbers and letters and force password changes every 90 days.

- **Client and Server Security.** Protect desktops, laptops and servers with anti-virus software and keep the anti-virus signature files up to date. Desktop firewalls prevent spyware and other malicious software from being installed inadvertently or intentionally on employees' PCs and laptops. Host intrusion prevention systems protect servers and databases against buffer overflow attacks and other malicious activity.

- **Network Security.** Protecting the network perimeter means constructing a multi-layered defense of firewalls, VPNs and intrusion detection or prevention systems (IDS/IPS).

  Firewalls prohibit unauthorized traffic from entering or leaving a network, thus protecting the local network from external network attacks. A firewall sits behind the router that connects to the WAN and filters traffic, passing it onto a centralized switch in the data center. IT can create inbound and outbound rules on the firewall to control traffic and limit which types of TCP applications are permitted. Most firewalls include anti-virus protection and increasingly include IDS capabilities.

  IDS and IPS protect the network from worms, Trojans and DoS attacks. An IPS proactively blocks attacks as they occur, whereas an IDS detects the intrusion without taking action. An IPS should provide protection from application-level VoIP exploits.
  .
  VPN appliances should be used between corporate locations to encrypt communications using IPSec or SSL. Encryption ensures that site-to-site communications can not be snooped over private or public WAN connections.

  Wireless LANs are becoming pervasive, and whether or not your organization has a policy that forbids wireless, chances are that more than several tech-savvy employees have set up their own Wi-Fi hotspots. Make sure that wireless access points use Wi-Fi Protected Access 1.0 or 2.0 access control and encryption to prevent intruders from hopping onto your wireless network and launching attacks from within your trusted enterprise.

- **Traffic Segregation.** Isolating traffic using virtual LANs (VLANs) or routing is another way to protect network traffic. A VLAN is a logical grouping of devices on one or more physical LAN segments that are configured so they can communicate as if they were attached to the same wire. Using VLANs can also reduce broadcasts/multicasts, which improves performance.

For stronger security, companies may lock down physical switch ports, so that only specified MAC addresses may transmit over a particular port.

- **Bandwidth Management.** Bandwidth management methods, such as setting priorities for certain types of traffic, ensure that bandwidth is available for business-critical or delay-sensitive applications like IP telephony.

  Rate shaping carves out minimum and maximum amounts of bandwidth allotted to specific applications, ensuring that voice traffic can still get through even if the network is under attack.

  IEEE 802.1p or DiffServ can be used to implement quality of service (QoS), ensuring that delay-sensitive voice traffic gets higher priority than data. 802.1p provides QoS at Layer 2, allowing switches to reorder packets based on priority level. DiffServ enforces QoS at the IP layer.

  VLAN tagging can be used to provide a higher level of security between segments of an internal network. IEEE 802.1q establishes a standard method for tagging Ethernet frames with VLAN membership information.

IP Telephony System Architecture

While organizations can take many steps to secure their network infrastructure prior to deploying IP telephony, choosing a phone system that is inherently secure is a critical success factor. Security is inherent in the ShoreTel system because of its fundamental architecture, including an embedded platform, distributed intelligence, and network-independent call control.

- **Embedded Platform.** ShoreTel call control runs on Wind River VxWorks operating system, which is the leading embedded operating system in the market. This call control software runs on the ShoreGear voice switches, which are embedded devices with no moving parts other than a fan. All together, ShoreGear voice switches deliver five-nines of availability (99.999%).

  IT managers should be wary of systems that use Microsoft Windows for call control for obvious security reasons. Given the frequency of vulnerabilities discovered on Microsoft Windows platforms and the never-ending cycle of patching, relying on a Microsoft Windows-based IP telephony system creates a significant security risk.

  IT managers should also be wary of systems that rely on an embedded hard disk inside their call-control platforms, because the disk is the least reliable system element and will not deliver five-nines of availability.

- **Distributed Intelligence.** ShoreTel call control is completely distributed and has no single point of failure. Since there is no single device involved with the basic telephony, the system delivers levels of availability unmatched by even legacy PBX vendors. As with the Internet itself, its distributed nature makes it impossible to take down the entire network.

  If a WAN outage occurs, sites run independently. PSTN failover ensures that workers can still take calls and even retain features like four-digit dialing among offices in the event of a WAN outage. Outbound

calls, including 911 calls, can still be placed via trunk lines since each location has telephones, trunks, and the intelligence to make and take calls. In the unlikely event a ShoreGear voice switch fails, the other switches on the network automatically take on the call-processing load.

Approaches that centralize PBX intelligence into a server inherently impact system reliability and are more vulnerable to system-wide outages because of an attack.

- **Network-Independent Call Control.** ShoreTel call control is independent of many networking elements. With ShoreTel, if a router crashes or becomes congested because of data traffic from worms, viruses or DoS attacks, the system continues to operate since it is distributed and runs on embedded devices dedicated to telephony.

  IP telephony systems that are integrated with the router are inherently more vulnerable to network-based attacks. Worms, viruses and DoS attacks can simultaneously cripple voice and data communications when the router is compromised since it represents a single point of failure.

Secure Management

The ShoreTel system supports secure management sessions and multiple levels of administrator permissions. This way, organizations can limit control for internal administrators and ensure that only authorized outside partners are permitted to access and manage the ShoreTel system.

- **SSL Secure Management:** ShoreTel supports secure management. Sessions are encrypted using Secure Sockets Layer (SSL), which is the same protocol that is used to protect online banking sessions. SSL secures communications from the browser to and from the main ShoreWare server as well as between the main ShoreWare server and to all distributed ShoreWare servers. Please see the ShoreTel Application Note "Guidelines and Recommendations for Configuring SSL for Use with the ShoreTel System" to learn how to configure this functionality.

- **Multi-level System Management:** ShoreWare Director can be deployed with multiple levels of administration, which protects critical system components from accidental or malicious threats yet grants local access for day to day changes. Typically companies reserve complete system access for a few key IT professionals and grant responsibility for moves, adds and changes (MAC) for a site to local individuals. In addition, ShoreWare Director supports multiple simultaneous active sessions all with user ID and password protection.

- **Password Change:** To ensure tight user security, passwords for both the Call Manager and voice mail telephone user interface must be changed when a worker first logs in to the system.

IP Telephony Device Registration

The ShoreTel system is designed to ensure unauthorized IP end points cannot access system resources, while still providing plug-and-play deployment.

When an IP telephone is plugged into the network, it is automatically discovered by the ShoreTel system and granted minimal privileges.

The telephone has no feature privileges, is not able to make outbound calls, and cannot receive inbound calls. To become active with features, a user must login to the telephone with a valid user id and password configured by the administrator.

In ShoreTel6 Release1, when a SIP end point comes on the network, it is authenticated by the ShoreTel system with a user id and password. Rogue SIP devices do not receive service from the ShoreTel system.

Best Practices for Securing IP Telephony

Iron-clad IP telephony security is built on top of strong network security. Here are best practices for securing IP telephony in the WAN, the campus and local networks, and for remote users working from home or the road.

Best practices for deploying secure IP telephony over the WAN include:

- **Use a VPN Between Sites.** When interconnecting multiple locations, organizations may use managed networks, point-to-point communications or an IP service provider. Whatever WAN connection you choose, use VPN tunnels between locations to encrypt communications.
- **Use Firewalls.** Use a firewall to protect your internal network from the threats coming in from the WAN and public Internet. Make sure the firewall has the performance to handle the real-time needs of VoIP traffic. Specifically, the firewall must be able to handle a large number of small packets without introducing a lot of latency. ShoreTel has done interoperability testing and has certified Juniper/NetScreen and SonicWall firewalls.

Best practices for secure IP telephony in the local network include:

- **Use Ethernet Switches.** Use Ethernet switches for your all voice devices, including IP phones, SoftPhones, ShoreGear voice switches and ShoreWare servers to reduce the possibility of snooping into the voice traffic. In a switched environment, traffic flows between the two devices and cannot be observed by non-malicious users. Do not use Ethernet hubs, as it is easy to observe traffic on this shared resource.
- **Put Voice in Separate VLANs.** Organizations can set up separate VLANs for voice traffic, which eliminates broadcast domains and segregates traffic for improved performance and security. Using VLANs can limit the number of ports for which voice traffic is destined, adding to security. With ShoreTel, VLANs IDs can be set automatically using DHCP, which saves time.
- **Prioritize Voice Over Data (LAN) -** The VLAN can be used to prioritize voice over data on the local area network, which can allow the voice traffic to get through even when data traffic is intense— including some network attacks. Check your network switches to ensure they can prioritize based on VLAN (or DiffServ) tags and that they support multiple queues.
- **Prioritize Voice Over Data (LAN/WAN) –** DiffServ should be used to prioritize voice over data on the LAN and the WAN to ensure the voice traffic gets through even when data traffic is intense—including some network attacks. Check your WAN access devices to ensure they can prioritize based on DiffServ and that they support multiple queues.

- **Rate Limiting –** Critical network elements like routers and switches should use rate limiting to make sure a single traffic flow cannot consume the entire resource, such as CPU, memory, or bandwidth, in the face of a DoS attack.

- **Port Lockdown –** For stronger security, companies can lock down VoIP traffic on physical switch ports so that only devices with specified MAC addresses may transmit over the specified port. This process is labor-intensive but it can mitigate local threats.

- **Prevent Eavesdropping.** A malicious employee or intruder who has penetrated your network can use snooping tools to capture a session before the call is initiated and play back the communications later. Attackers can fake the MAC address of a client, pretending to be a legitimate device, and gain access to the network. With port mirroring, all the traffic on one switch port is simultaneously sent to a network analyzer connected to another port. An intruder can use then snoop the network traffic.

  Media stream encryption — a new feature in ShoreTel6 Release1 — is the ultimate protection against electronic eavesdropping and replay attacks. Even if someone successfully taps the media stream, they cannot decode and understand the conversation.

Best practices for deploying secure IP telephony on campus networks, on building floors and in workgroups include:

- **Use VPNs Between Buildings.** Use a VPN between buildings on a campus or floors in a building. Because the traffic is encrypted, the information inside the VPN tunnel is protected from eavesdropping.

- **Use VPNs for Departments.** Deploy VPNs between key departments, such as human resources, finance, executives or legal, whose conversations are often company confidential.

- **Use Encryption for Important Individuals.** Use the media stream encryption feature in ShoreTel6 Release1 to protect communications for extremely important users like generals or CEOs. Media stream encryption is more cost effective and simpler to deploy than VPNs.

Best practices for deploying secure IP telephony to remote workers include:

- **Use Software VPNs for Soft Phones.** Employees working from home or on the road connect to the corporate network over untrusted connections, be it cable or DSL from home or from a Wi-Fi hotspot at the hotel or coffee shop. Remote workers using the ShoreTel IP SoftPhone should use a software-based VPN.

- **Use VPN Appliances for IP phones.** Remote workers using IP phones should use a hardware-based VPN to protect their conversations. ShoreTel has tested and certified SonicWall and Juniper/Netscreen solutions.

Telephony Class of Service Protects Against Service Thefts

The IP telephony system itself should protect companies against service thefts such as toll fraud and feature abuse. That protection is built right into the ShoreTel system.

With ShoreTel, anything that costs your organization money or can lead to feature abuse can be controlled through class of service. This includes the ability to restrict calling (i.e., long distance and international), overhead paging, trunk-to-trunk transfers, and transferring and forwarding to external numbers. ShoreTel gives administrators complete control over telephony, call and voice mail feature permissions.

Users are placed into user groups which in turn are assigned telephony, call, and voice mail permissions. The following telephony permissions can be controlled:

- Maximum Number of Calls
- Maximum Parties in Make Me Conference
- Allow Call Pickup
- Allow Trunk-to-Trunk Transfer
- Allow Overhead and Group Paging
- Allow Make Hunt Group Busy
- Allow Extension Reassignment
- Allow PSTN Failover
- Show Caller ID Name and Number on Monitored Extensions
- Allow Customization of IP Phone Buttons
- Show Extensions with Different Prefixes in Directory
- Allow Collaboration Features
- Allow Recording of Own Calls
- Allow Directed Intercom / Paging
- Allow Barge In
- Allow Record Other's Calls
- Allow Monitor Other's Calls
- Allow Call Handling Changes
- Allow External Call Forwarding and Find Me Destinations

The following call permissions can be controlled:

- Internal Only
- Local Only
- National Long Distance
- International Long Distance
- Wildcards allow complete customization of outbound calling

The following voice mail permissions can be controlled:

- Maximum Incoming Messages
- Incoming Message Length
- Outgoing Message Length
- Allow Access to Broadcast Distribution List
- Allow Access to System Distribution Lists
- Allow Message Notification
- Allow Message Notification to External Number

In addition, the ShoreTel system can change class of service permissions by time of day, which is important for vertical markets like manufacturing and education that need more restrictive permissions during off hours. For instance, in manufacturing it is common to allow long

distance during the day when the supervisor is present but restrict long distance in the evenings and weekends when cleaning personnel are in the building.

The ShoreTel system also supports authorization codes and associated reporting. This allows users with the proper authorization to place outbound calls from restricted telephones.

Preparing for the Future of IP Telephony Security

Organizations are embracing IP telephony at unprecedented rates, and IP telephony will continue to replace more elements of the traditional telephone network. When pure IP calls are available among different corporations through SIP trunking, security issues become paramount. Security is also critical for residential IP telephony services in which calls traverse the public Internet. Concerns about listening in on calls, DoS attacks and even VoIP spam must be anticipated.

A secure IP telephony deployment is contingent on a secure network infrastructure. ShoreTel delivers strong security by design by protecting the conversation content and guarding against service thefts. Only with a robust network design can the ShoreTel system be deployed in safely and securely.

More Information

The following books provide good guidelines on network security:

- *Voice Over IP*, by Uyless Black
- *Hacking Exposed: Network Security Secrets & Solutions*, by Stuart McClure
- *Secrets and Lies: Digital Security in a Networked World*, by Bruce Schneier

Since VoIP and network security are changing and evolving rapidly, the trade press and industry organizations are an excellence source of learning.

- SANS
- Computer Security Institute
- "Fortifying Network Access Control," *Network Computing*
- "Is VoIP Secure? You Make the Call," *Information Security Magazine*

Glossary

Denial of service (DoS) attack — An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a denial of service attack interrupts network service for some period. VoIP is susceptible to several types of DoS attacks, including malformed requests, media, flood attacks and load-based attacks. These DoS attacks include:

- **Malformed Request DoS** — Carefully crafted protocol requests can be used to exploit a known vulnerability resulting in a partial or complete loss of service.
- **DoS on Media** — VoIP media is carried within Real Time Protocol (RTP) packets and is vulnerable to any attack that congests the network or slows the ability of a phone or gateway to process packets in real time. An attacker who has access to the network where media is present can inject large numbers of media packets or high quality of service packets, which will contend with legitimate media packets.
- **Load-based DoS Attacks** — Flooding a target with legitimate requests can easily overwhelm a system. Even without an actual VoIP request, a DoS attack such as TCP SYN Flood can prevent a device from being able to accept calls for long periods of time.

Intrusion Detection System (IDS) — Software that detects an attack on a network or computer. IDS monitor traffic for signatures of known attacks or look for derivations of normal routines as an indication of an attack.

Intrusion Prevention System (IPS) — Software that prevents an attack on a network or computer. An IPS stops the attack from damaging or retrieving data, whereas an intrusion detection system passively monitors threats.

Firewall — A firewall allows or blocks traffic into and out of a private network, keeping it secure from intruders. To effectively support VoIP, look for a firewall that can perform deep packet inspection and transformation of embedded IP addresses and port information.

SPAM — E-mail that is not requested. Spam is used to advertise products or to broadcast some political or social commentary.

SPIT — Spam over Internet telephony (SPIT) is unsolicited bulk messages broadcast over VoIP to phones connected to the Internet. It is a small but growing program. IP telephony makes an effective channel for commercial voice mail messages because the sender can send messages in bulk instead of dialing each number separately. Unscrupulous marketers can use spambots to harvest VoIP addresses or may hack into a computer used to route VoIP calls.

Secure Sockets Layer (SSL) — The leading security protocol on the Internet, SSL is widely used to validate the identity of a Web site and to create an encrypted connection for sending credit card and other personal data.

Trojan Horse — A program that appears legitimate, but performs some illicit activity when it is run. A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer.

Virtual LAN (VLAN) — A group of devices on one or more LANs that are configured so that they

can communicate as if they were attached to the same wire, when actually located on different LAN segments.

Virtual Private Network (VPN) — Enterprises use VPNs to secure communications over site-to-site connections to branch offices and to allow mobile users to dial up to their company networks. Communications are encrypted using IPSec or SSL.

Worm — A destructive program that replicates itself throughout disk and memory, using up the computer's resources and eventually taking the system down.