Multi-layered Security Solutions for VoIP Protection
INTRODUCTION

The Benefits of VoIP

Voice over Internet Protocol (Voice over IP or VoIP) allows users to make phone calls over the Internet, or any other IP network, using the packet switched network as a transmission medium rather than the traditional circuit transmissions of the Public Switched Telephone Network (PSTN). As the technology has become more reliable in recent years, companies have been moving to VoIP for a number of reasons. Consolidation of voice and data on one network reduces costs and results in a lower network total cost of ownership (TCO). Operating expense savings include lower long distance charges, reduced support costs and savings via workforce virtualization. Companies also use the migration to VoIP as an opportunity to replace aging telephony equipment with feature-rich technology like teleconferencing and collaboration/multimedia applications. VoIP supports increased mobility, since remote workers have the same access to voice features as corporate office employees.

Research organization Gartner Inc. recently reported that spending by US companies and public-sector organizations on VoIP systems is on track to grow to $903 million in 2005 (up from the $686 million in 2004). By 2007, Gartner expects 97 percent of new phone systems installed in North America to be VoIP or hybrids.

Planning and Implementing VoIP Security

While it is true that Voice over IP can provide savings over traditional telephony solutions, there are security risks associated with this technology that need to be addressed. Risks include denial of service (DoS), service theft, unauthorized call monitoring, call routing manipulation, identity theft and impersonation, among others. Not only does VoIP inherit all data network security risks, but it introduces new vectors for threats related to the emerging and untested technology and protocols associated with VoIP. These new threat vectors in turn increase the risk to the data network.

Companies may spend $100,000 or more on network upgrades required to support a VoIP implementation, yet they may overlook VoIP security during their network assessment. Many enterprises assume that their existing security policies are adequate. And in many cases, executives do not include security managers in the decision-making process (either for purchase or deployment of VoIP).

The technology behind VoIP is a complex collection of protocols, applications and appliances that all require attention when planning a new implementation or conducting risk assessments of existing technology. An ideal VoIP security solution provides multi-layered, preemptive protection from threats affecting both traditional data-driven network traffic and the underlying infrastructure, devices and protocols that support VoIP data transmissions, all without interrupting Quality of Service.

ISSUES ASSOCIATED WITH VoIP SECURITY

The biggest threats associated with VoIP are service disruption or degradation (DoS) and remote compromise that can lead to unfettered access to an enterprise's critical systems and the confidential information stored on those systems. Attack prevention and the preservation of Quality of Service are the key requirements for a VoIP protection system.

Quality of Service (QoS)

VoIP requires higher standards of Quality of Service and availability than are accepted on worldwide data networks. The degree of latency that may be acceptable for data traffic cannot be tolerated for voice transmissions. Any threat that disrupts service, even slightly, or compromises call integrity could result in a service outage. Executives contemplating or undergoing the switch to VoIP need to consider how an outage might impact their business. A prime example of VoIP risk is a business call center undergoing a denial of service attack. The “lines” would be flooded; no calls could get through. The cost of network cleanup and recovery may be substantial, but that pales in comparison to the cost of lost business opportunities while the network is down. Fortune magazine data shows that Fortune 1000 companies earn revenues per minute ranging from $9,000 to $258 million, with an average of $62,000 per minute. Such financial losses from VoIP network downtime are unrecoverable.

Integrated VoIP technology assures Quality of Service through multiple devices including routers, VoIP-specific servers, the virtual private networks (VPNs) across which the traffic might travel, and third party products. Security solutions protecting the VoIP network should honor QoS and protect against Denial of Service in order to assure the network’s quality and reliability.

Exploitation of Vulnerabilities

A security concern regarding VoIP technology is that all vulnerabilities inherent in IP networks will also affect VoIP on the converged network, presenting new risks to an enterprise’s voice services. Vulnerabilities in the network infrastructure can affect the security and availability of the VoIP network. For example, products from certain switch and router makers have fatal flaws that could let hackers craft Denial of Service attacks to disrupt enterprise networks. VoIP systems are also vulnerable due to weaknesses in the operating systems on which the VoIP servers are running.

In addition to these operating system and data network security risks, VoIP specific threats increase an organization’s risk as the voice and data networks converge. Further security measures are needed to manage this added risk.


INTERNET SECURITY SYSTEMS
Ahead of the threat.
SECURITY BEST PRACTICES FOR VOIP PROTECTION

Potentially, every component of a VoIP system may be vulnerable. These include the protocols, IP infrastructure (routers, switches), IP/PBXs (private branch exchanges), VoIP-specific servers, and individual phones or “soft phones” (a PC with a headset). Careful network design and deployment of the VoIP network coupled with the implementation of specific security technologies will ensure quality, reliability and security for VoIP traffic.

Protection Technologies

While standard network security policies and procedures such as encryption, access control and logical separation of the voice network do provide some protection for VoIP, these measures alone will not provide adequate attack prevention, given the potential for unauthorized access or attacks that easily bypass traditional security mechanisms.

Further, protocol-specific vulnerabilities and flaws within the VoIP applications themselves may leave VoIP systems vulnerable to attack in the absence of a vendor-supplied patch. According to a Forrester Research study, “It is up to companies to provide the added security measures required for IP [Telephony]: Don’t assume that vendors will respond to each and every risk that appears with patches for installed products.”

Encryption for VoIP traffic offers some protection from eavesdropping and other call compromises. But it must be backed up with strong protections not only at the gateway but at the network and host as well.

A multi-layered security solution must provide attack prevention for the following: TCP/UDP based attacks, operating system vulnerability attacks, protocol flaws, device configuration flaws and VoIP application flaws. A robust solution should allow for deep packet inspection of the packet payload to recognize known attacks, anomalies or suspected attacks based on known vulnerabilities.

MINIMAL STEPS FOR SECURING VOIP NETWORKS:

- Separate voice and data on different logical networks (VLANs)
- Separate DHCP servers
- Use strong authentication and access control on the voice gateway system
- Incorporate “VoIP-aware” application layer gateways (ALGs) and firewalls
- Use IPsec or SSH for remote management

### Vulnerable VoIP Components

<table>
<thead>
<tr>
<th>Vulnerable VoIP Components</th>
<th>Threats against VoIP infrastructure</th>
<th>VoIP Protection Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols (IP, H.323, SIP, SCCP)</td>
<td>DoS</td>
<td>NIPS</td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td>DoS</td>
<td>HIPS</td>
</tr>
<tr>
<td>(Routers, Switches, Firewalls)</td>
<td>Remote Compromise</td>
<td>Firewall</td>
</tr>
<tr>
<td>Underlying OS (Windows, Linux, AIX)</td>
<td>Worms</td>
<td></td>
</tr>
<tr>
<td>IP PBX / Management Server</td>
<td>Viruses</td>
<td></td>
</tr>
<tr>
<td>IP Phones</td>
<td>DoS</td>
<td></td>
</tr>
<tr>
<td>Soft Phones</td>
<td>Remote Compromise</td>
<td></td>
</tr>
</tbody>
</table>

**Further details about VoIP vulnerability exploitation can be found in the ISS white paper, “VoIP: The Evolving Solution and the Evolving Threat.”**

INTERNET SECURITY SYSTEMS’ (ISS) MULTI-LAYERED VOIP SECURITY SOLUTION
The ISS Proventia® intrusion prevention solution is an essential element of a multi-layered VoIP security solution providing intrusion prevention at the gateway, on the network and at the host. Proventia products block threats that can bypass even a VoIP-aware firewall, and provide added protection to VLANs and VPNs dedicated to voice traffic.

ISS’ method of analyzing VoIP traffic differentiates its Voice over IP protection from other methods on the market. ISS’ Proventia products parse and analyze the underlying VoIP family of protocols, including SIP, MGCP, H.323, SCCP and many others.

Because Proventia intrusion prevention technology recognizes and parses these VoIP protocols, it is able to properly identify VoIP traffic and analyze the payload for known or suspected attacks. Proventia can recognize traffic that does not fit or follow the rules of the protocol and can alert administrators to anomalous traffic or block it outright. The use of protocol analysis techniques also means that when variant attacks are released, Proventia will still block them without needing a pattern matching signature update.

By parsing and analyzing VoIP protocols and providing preemptive vulnerability protection via ISS’ Virtual Patch™ technology, which preemptively protects vulnerable systems without a vendor-supplied patch, Proventia security products identify and protect an enterprise’s VoIP systems against known and unknown threats—before they impact the network.

The combination of ISS’ Internet Scanner® vulnerability assessment solutions and Proventia’s Virtual Patch technology, powered by X-Force® security intelligence, make vulnerability management on the voice network easy to maintain.

CONCLUSION
Many companies are migrating to IP telephony without fully investigating or understanding the security risks involved. VoIP is subject to all the risks and vulnerabilities that affect Internet data networks. In addition, there are several VoIP-specific vulnerabilities related to VoIP protocols and specific components of VoIP technology. Since VoIP has a lower tolerance for service disruption or degradation than would be acceptable on a data network, careful security planning is essential for maintaining availability and quality on a VoIP network.

Enterprises must put in place a VoIP security solution that preserves Quality of Service by protecting against service disruption and provides protection against attacks that exploit VoIP-specific flaws and vulnerabilities and attacks against supporting operating systems and devices. A multi-layered security solution that includes intrusion prevention and preemptive shielding of vulnerabilities is essential to keep the voice network secure.

VoIP vendors and standards bodies have the opportunity to make telephone communication more secure than even traditional PSTN, however, security is traditionally not a priority when new emerging technology is being developed. Even as vendors make security improvements over time, it is important for an enterprise to implement a complete, multi-layered security solution from a VoIP-aware security vendor to ensure its combined voice and data network is fully protected.