



Dialing Up **New** Security Woes

By John Bumgarner
john@bumgarner.us

As consumers increasingly embrace the new Voice over Internet technology for their telephone service, a host of new security concerns are coming into focus and demanding attention.

Thanks to the convergence of data and voice networks, assaults waged against either can cripple both. Everything from eavesdropping to spam to denial-of-service attacks stand to be multiplied thanks to the mushrooming use of the Internet to provide telephone service. Security specialists must now come to grips with it all.

It all began, as is usually the case, with technological change ushered in as part of the ever-expanding digital revolution.

Until now, most consumers have been more or less content with the standard phone services that they have been receiving from their local Ma Bell. This traditional phone service is called PSTN (Public Switched Telephone Network), but is commonly referred to as POTS (Plain Old Telephone Service). It uses copper wires to carry analog voice data between two end points.

Newer digital technologies, such as Fiber Distribute Data Interface (FDDI), move telephone service to a new, higher level, providing voice, video and data much faster than traditional copper-based transmission methods. Boosted by the 1996 Telecom Act, this technological advance-

ment has fueled the move toward Voice over Internet Protocol (VoIP) technology, which is also referred to as Internet telephony, IP telephony, or Voice over the Internet (VOI).

By 2008, the U.S. consumer market for VoIP is projected to be \$5.8 billion, with 17.5 million residential subscribers and an unknown number of corporation users. Numerous organizations have already made the leap from fixed analog and digital to the newer technology.

Among large companies that have embraced VoIP technology early on are Bank of America, which plans to displace 180,000 hardware phones with VoIP systems in the near future, British Petroleum, which will replace 150,000 of its old-system phones, and Ford Motor Company, which is converting 50,000 phones.

As VoIP technology matures and additional access technologies such as broadband and wireless become more prevalent, more such conversions to VoIP, among businesses as well as consumers, are inevitable. The move will be fueled by several access technologies, including Voice over Digital Subscriber Line (DSL), Voice over Worldwide Interoperability of Microwave Access (WiMAX), Voice over Asynchronous Transfer Mode (ATM), Voice over Frame Relay (FR), and other media, such as satellite or Broadband over Power Lines (BPL).

VoIP Attack Points

As noted earlier, the migration to VoIP technology creates numerous new security risks. To reduce those risks, security personnel must understand some of the attack points within the VoIP architecture as a critical first step.

Among the primary attack points are the call controllers. These devices normally consist of a standard server, running an operating system such

as Microsoft Server 2003 and a vendor application that controls call functions. Some call controllers even use a back-end database such as Microsoft SQL Server.

VoIP telephones themselves can also be used as attack points, so understanding the various types is important to protecting them from attacks. There are two primary types of telephones. One type is hardware-based; the other is software-based.

Hardware-based VoIP telephones look like the standard phones that many organizations currently use, but they have advanced features, including Liquid Crystal Displays (LCD) and dynamic call features and functions. Some of the dynamic features allow Web-based content to be moved to the LCD screen. This content can range from stock quotes to news stories and even company announcements. Hardware-based telephones also include wireless handsets, which are available from various vendors.

A soft phone uses a client-side piece of software that turns any standard computer into an Internet Protocol (IP)-based phone. A soft phone can be either a standalone application running on an operating system or it can be integrated into applications such as Microsoft Outlook, several of which are expected to make such telephone software of their standard features. Several vendors have also even created soft phones for the Pocket PC platform and other similar devices.

VoIP Protocol Issues

Other attack points exist in the various protocols that a VoIP network can use. VoIP's primary transport mechanism is the Internet Protocol, but there are other underlying protocols that may have their own security risks that must be considered as well. Listed below are some of the various protocols that VoIP can use:

- ▲ H.323—defines a distributed architecture for creating multimedia applications, which includes VoIP. For additional information reference (<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.323>).
- ▲ Session Initiation Protocol (SIP)—defines a distributed architecture for creating multimedia applications, which include VoIP. For additional information reference IETF RFC 2543 (<http://www.ietf.org/rfc/rfc2543.txt>).
- ▲ Media Gateway Control Protocol (MGCP)—defines a centralized architecture for creating multimedia applications, which include VoIP. For additional information reference IETF RFC 3435 (<http://www.ietf.org/rfc/rfc3435.txt>).
- ▲ H.248/Megaco—defines a centralized architecture for creating multimedia applications, which includes VoIP. For additional information reference IETF RFC 2885 (<http://www.ietf.org/rfc/rfc2885.txt>) or (<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.248>).
- ▲ User Datagram Protocol (UDP)—is used to by the sending and receiving VoIP applications.
- ▲ Real-Time Transport Protocol (RTP)—defines a distributed architecture for creating multimedia applications, which includes VoIP. For additional information reference IETF RFC 2543 (<http://www.ietf.org/rfc/rfc2543.txt>).

Multiple vulnerabilities were identified in the Session Initiation Protocol in 2003. The vulnerabilities included unexpected system behavior; denial-of-service (DoS) and remote code execution. In 2004

various vulnerabilities were identified in H.323, which resulted in either a DoS attack or unauthorized arbitrary code execution against the devices affected. As VoIP deployments become common, additional vulnerabilities may be discovered within the protocols used to support the technology.

VoIP Security Issues

Once the attack points are understood, the security risks can be dealt with. Here it is useful to keep history in mind. While the convergence of data and voice networks may sound like a wonderful idea in the boardroom, most security professionals still remember watching a network crumble under the weight of a denial-of-service attack. In a converged network, such attacks can disrupt both data and phone services.

Knowing the types of attacks that can potentially affect VoIP networks is the first step in defending against them. Listed below are some of the most common attacks that may affect VoIP networks.


Denial-of-service

Many VoIP telephones are prone to the same types of denial-of-service attacks that have long plagued systems on traditional data networks. By transmitting specific types of IP traffic, such as fragmented User Datagram Protocol (UDP) packets, VoIP telephone service can be disrupted. Likewise, flooding the servers with fabricated call session setup requests can disrupt some of the servers that handle VoIP calls. Servers that offer Web services to end-users can be affected by overloading the system with HyperText Transfer Protocol (HTTP) requests.

Information Security Professionals
Earn your NSA certifications and continuing education credits!


*Learn the National Security Agency's methodologies
Identify and correct information security weaknesses
Receive NSA certification for both courses*

Training so good we teach the competition...

 All Security Horizon IAM students receive a **FREE** copy of our latest book, "Security Assessment: Case Studies for Implementing the NSA IAM"

Our NSA IEM is CVE® compatible!


*Learn from the course co-authors
Attend classes available nation-wide
Receive free licenses for SAINT® and NeWT™
Use commercial and freeware tools on multiple platforms*



Can't find a course near you? Contact us at info@securityhorizon.com to see about hosting a class!

"Security Horizon is an ISSA Membership Training Discount Partner"

Contact info@securityhorizon.com for more information
www.securityhorizon.com
719.488.4500 voice 719.268.1709 fax



Spoofing

VoIP calls have the potential to be hijacked by spoofing an SIP response, which allows an attacker to impersonate a valid user. This impersonation potentially allows the attacker to use the VoIP system to make free long distance calls. In order to accomplish this level of impersonation in a security-conscious environment, an attacker must be able to access the underlying protocols, packets stream, and even obtain a valid password or certificate to place the call.

Another spin on the traditional man-in-the-middle attack is when the attacker injects words into the target's established VoIP conversation. This form of attack is referred to as *voice spoofing*. The way voice spoofing works is that the attacker using a computer generates speech and injects the speech into the voice stream. Depending on the sophistication of the software used to generate the speech, it is possible to create perfect speech patterns that match the transmitter's voice.

Traditional phone systems have always been subject to third-party interception or eavesdropping. VoIP systems are no different, but the threat may be greater when encryption is not used to protect voice traffic.

Interception or Eavesdropping

Traditional phone systems have always been subject to third-party interception or eavesdropping. VoIP systems are no different, but the threat may be greater when encryption is not used to protect voice traffic.

One type of interception would require that an attacker have access to the IP stream that is carrying the voice traffic. In this scenario, a common packet sniffer called *tcpdump*¹ and a UNIX application called *Voice Over Misconfigured Internet Telephones* (Vomit). Armed with these simple, open-source tools, the employee could intercept Cisco VoIP telephone conversations and convert them into a standard wave (.wav) file that could be played in near real-time or stored for later listening.

Another type of interception requires an attacker to infect a computer that is using a "soft phone" with a Trojan. Depending on the attacker's objectives, the Trojan could be delivered in various ways. Regardless of delivery method, the objective of the attack is to obtain voice data that the client is sending. Once stolen, the information could be transferred off the client systems using traditional methods such as the File Transfer Protocol (FTP) or through a custom application using either the Transmission Control Protocol (TCP) or the User Datagram Protocol.

Simple Network Management Protocol

Many VoIP telephones support remote management through the Simple Network Management Protocol (SNMP). An attacker can potentially exploit a SNMP management interface that is protected with either a blank or weak password.

Once SNMP access is obtained, the attacker could render the phone inaccessible from the management station and block all outbound calls

from the device. This level of attack could force an organization to send someone to each phone's location to remedy the issues. Imagine if this level of attack occurred at Boeing, which will have 150,000 VoIP telephones. The level of effort to restore telephone service would be overwhelming for most support organizations.

Trivial File Transfer Protocol

Some vendors use the Trivial File Transfer Protocol (TFTP) to update software and firmware on the VoIP telephones. An attacker could potentially upload an unauthorized configuration file to the telephone if the TFTP session is not protected with an Access Control List (ACL). A successful attack could create the same problems as an SNMP-based attack.

VoIP SPAM

All of us have been victims of SPAM clogging our inboxes, but a new type has surfaced that targets IP telephony. VoIP SPAM has been dubbed spam over IP telephony (SPIT). The way SPIT normally works is a "spitter" would harvest telephone numbers from free VoIP services or those offering the service for a minimum charge. Enterprises using VoIP are semi-protected from SPIT because spitters must gain access to the internal network to obtain numbers. Currently SPIT is not a major issue for organizations because there are not enough users of the technology to justify the efforts voice spammers would have to exert. Over the next 3 years, however, SPIT will become an issue because more organizations and consumers will have adopted VoIP technology.

Viruses

Like SPAM, viruses have taken their toll on computer users worldwide, and it is likely that in the next three to five years VoIP will be affected by them, too. Viruses could be targeted at VoIP phones to disrupt service by resetting them, clearing their configuration or modifying the phones' LCD screens with either some text or a graphic. Meanwhile, call controllers can be affected by viruses, too, since most of the controllers run standard operating systems (e.g. Microsoft Server 2000) and backend databases (e.g. Microsoft SQL Server) that have been riddled with security holes. Spitters can use viruses to harvest VoIP account information from backend databases that have known vulnerabilities.

All the attacks listed here are technically possible today. The complexity of each attack depends on various parameters on each device targeted and the configurations of the network on which the devices reside.

Threat Mitigation Techniques

The security measures listed and explained below are the most effective methods to counter the security issues mentioned above that may affect your VoIP network.

1. **Encryption:** An important component of a secure VoIP infrastructure is encrypting the VoIP voice packets. Encryption protects against attacks such as spoofing and eavesdropping and will prevent an attacker from decoding voice packets with tools such as Vomit. Call-signaling information should also be encrypted because it would prevent an attacker from capturing endpoint registration and call-setup details. The minimum encryption level used to protect VoIP information should be 128-bit Advanced Encryption Standard (AES).
2. **Endpoint authentication:** This means requiring that all phones use some form of authentication to register with the call controller (e.g.


Cisco CallManager) and to receive authorization to initiate an off-site call. Integrated digital certificates would reduce the likelihood that an attacker could make a call using an unauthorized phone because a pre-approved certificate would be required to initiate the call request. Endpoint authentications protect against dangers such as spoofing, SNMP and TFTP attacks.

3. **Hardening call controllers:** This need is made critical by the fact that some well-known services, such as Microsoft Internet Information Server (IIS), have published security vulnerabilities that can lead to total system compromise. Providing this security measure involves conducting a comprehensive pre-installation security assessment through the use of tools such as Nessus (www.nessus.org) to discover open ports and identify known security issues. Any open ports not required should be turned off and any security issues identified should be corrected prior to placing the system into full operation. If the call controller logs information into a backend database, the tables and data stored in that database should be reviewed. Sensitive information identified in the database should be encrypted using a commercial product such as DbEncrypt. If the controller provides Web services such as unified messaging management to customers, an additional test should be conducted to detect common application security issues, such as SQL injections, cross-site scripting and cookie manipulation. Hardening call controllers protects against attacks such as denial-of-service and viruses.
4. **Using firewalls:** The goal here is to protect call controllers from security threats coming from the network. Firewalls can be used to restrict certain management functions to a subset of IP addresses. Firewalls should also be used to restrict unauthorized VoIP protocols from entering the Internet gateway and from the internal network. Firewalls protect against items such as denial-of-service, interception, SNMP and TFTP attacks.
5. **Using Intrusion Detection Systems (IDS):** Intrusion Detection Systems can protect the call controller from known security vulnerabilities. Both network-based and host-based should be used where applicable. IDSs can protect against items such as SNMP and TFTP attacks.
6. **Using anti-virus:** Anti-virus applications can protect call controllers from known security vulnerabilities associated with malicious code.
7. **Establishing strong SNMP strings:** This deters brute force attacks aimed at obtaining the SNMP strings used for management sessions.
8. **Establishing an Access Control List:** This list should be designed to protect SNMP and TFTP sessions for both telephones and call controllers from unauthorized IP addresses.
9. **Segment networks:** Break them into two distinct groups, data and voice. Segmenting the networks does not require two different physical networks, but logical ones using a Virtual Local Area Network (VLAN). This segmentation can prevent VoIP traffic from being disrupted by the next virus that penetrates your data network. Segmentation can also help protect unencrypted voice packets from being sniffed from the data network.
10. **Analyze call patterns:** This can identify unauthorized long-distance calls and calls that do not meet business requirements. This is one of the best measures to identify items like toll fraud.
11. **Have a patch management program:** This is an issue we are all familiar with in traditional networks, and a VoIP network is no

different. Patch management and change control programs should include not only call controllers, but also hardware phones and soft phones. A strong patch management program can protect VoIP networks from traditional attacks aimed at Web interfaces on call controllers or the telephones themselves.

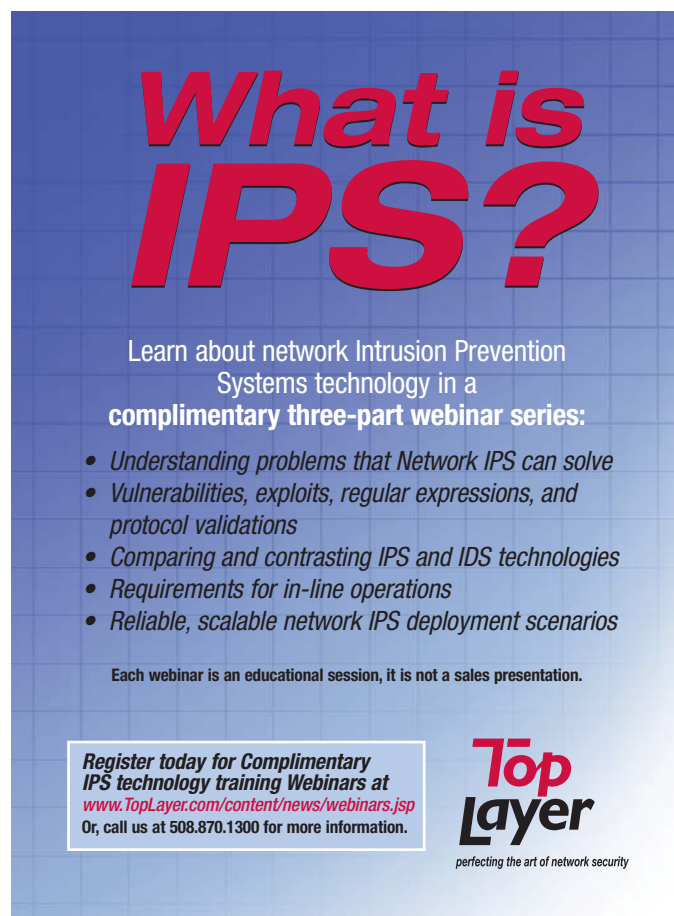
12. **Have a disaster recovery plan:** Items to consider include a means of handling emergency calls if your Internet connection is offline and a means of functioning at all if your call controller is offline for an extended period. A sound disaster recovery plan can help you recover from any of the attacks covered in this article and even those that were not discussed, such as power outages.

Conclusion

By all indications, as the VoIP market increases, so will the security issues that affect systems transmitting and receiving voice streams. With so many new devices going into use in so many areas of the home and workplace, attackers will be presented with a target-rich environment that they undoubtedly will work hard to exploit. The security measures outlined in this article will not make organizations bulletproof, but they will make organizations less vulnerable. 

John Bumgarner, MA, CISSP, GCIH, IAM, SSCP, is a senior security consultant. He also serves as the Research Director for Security Technology for the U.S. Cyber Consequences Unit, an independent agency funded by the Department of Homeland Security.

¹ <http://vomit.xtdnet.nl/>



What is IPS?

Learn about network Intrusion Prevention Systems technology in a complimentary three-part webinar series:

- Understanding problems that Network IPS can solve
- Vulnerabilities, exploits, regular expressions, and protocol validations
- Comparing and contrasting IPS and IDS technologies
- Requirements for in-line operations
- Reliable, scalable network IPS deployment scenarios

Each webinar is an educational session, it is not a sales presentation.

Register today for Complimentary IPS technology training Webinars at www.TopLayer.com/content/news/webinars.jsp Or, call us at 508.870.1300 for more information.

Top Layer
perfecting the art of network security