Voice over IP Security Planning, Threats and Recommendations

Dan Sass

dsass@bellsouth.net

Abstract

Voice over IP (VoIP) communications is becoming increasingly critical to the corporate world. In fact, companies stand to gain significant cost savings and productivity enhancements by deploying Voice over IP. However, voice services also introduce a new level of vulnerability to the network.

Perhaps, Voice over IP should be viewed as an opportunity to develop new, more effective security policies, processes and infrastructure. These new policies and practices can have a positive impact on the security of the whole network not just voice communications.

Providing the appropriate level of security means organizations must first understand the threats. Then they must build a framework that includes security planning, policies and a secure infrastructure.

I. Introduction

Over the past several years, we have witnessed the growth of Voice over IP (VoIP) and the advancements in technology to provide circuit switched communications using the Internet and private IP networks. Voice over IP is gaining popularity as current economic pressures combined with large investments made in networking technology from the hay days of the Internet have many firms considering the advantages of combining their voice and data networks. By utilizing existing infrastructures, the migration of voice onto a common network with data raises hopes of increased efficiencies and reduced expenditures. (Werbach, 2005)

Initially, the roadblocks to adopting VoIP were filled with concern about whether the technology would work as well as traditional telephony does with ubiquitous availability. The issues that occurred echoes, delays, and dropped calls frustrated vendors and companies alike. Today we see many of these fundamental issues fade away as VoIP technology becomes more sophisticated, growing into a viable solution. (Werbach, 2005)

Just as the technical hurdles are being dealt with, a new fear has emerged as people realize combining two very dissimilar communication types also combined threats and introduced vulnerabilities never seen before in data or voice systems. The challenge of securing VoIP has become the central issue of discussion and a new barrier to embracing the technology. The ability to ensure the confidentiality, integrity, and availability of data and voice communications on a common network has important business impacts. (Collier, 2005) VoIP networks use servers, routers, switches, applications, unique protocols and many computing elements to support not only voice communications, but also collaboration.

It is easy to conclude traditional attacks, such as viruses, worms, denial of service, and exploitable vulnerabilities can use VoIP solutions to wreak havoc. Adding to the confusion, much of today's security technologies, such as firewalls and intrusion detection systems (IDS) are nearly

useless in detecting or stopping attacks based on protocol interaction foreign to traditional security measures.

Using IP as the foundation for call setup, management, communications, system management, and messaging introduces concerns for the security of the communication and its resilience to attacks usually saved for servers, e-mail systems, and workstations. The IP protocol has its own security flaws, but the addition of upper-layer protocols and specialized messaging structure offers hackers the opportunity to access data through a voice system or use known data network hacking techniques to manipulate the phone system. Toll fraud, redirected calls, free conferencing, voice mail exposure, and eavesdropping take on completely new meanings in a converged network. Convergence of data and voice, or better described as data network's acquisition of voice communications, will come of age very soon and find itself in all corners of the globe. IP-based networks are the standard worldwide and as IPv6 emerges, the number of uniquely assigned devices possible nearly exceeds imagining, adding to the possible variety of implementations.

II. Voice Over IP Security Planning

Security does not just happen; it develops from careful planning of policies and procedures that are consistently practiced. It is a balancing act between risk mitigation and resource allocation, so it needs to be tailored for each network. Additionally, educating users
on the importance of security, and providing the right incentives, are crucial to engaging people in appropriate practices and behavior. Typically this process begins with engaging stakeholders in setting policies to establish guidelines and expectations, as well as getting management support for both the policies and their enforcement. Next a framework is designed, encompassing processes and infrastructure to implement the policies. Security basically comes down to people, processes, and technology, in that order of importance (Whitman & Mattford, 2004).

For VoIP, policies developed for data networks must evolve to a more integrated, view that covers all information and communication resources including voice.
Voice cannot be treated as ‘just another’ type of traffic. Real-time, reliable delivery is crucial for voice applications.

Policy development creates an opportunity for stakeholders from different areas of responsibility to learn from each other and their vendors about how to identify and close security gaps that result from bringing together previously separate networks. For example, access devices will include phones as well as PCs and PDAs, remote access will occur via the public
switched telephone network (PSTN) as well as the Internet, and mobile workers will need access as well as workers in fixed locations. For many of these, new servers or servers in new locations of vulnerability will have to be protected. Previous policies may need to be modified or extended and new policies added to account for security threats and vulnerabilities that might not have been an issue in the distinct voice and data networks.

One of the most important considerations prior to defining policy is risk assessment. This is where systems, processes, and procedures are evaluated in terms of their importance to the Company and their vulnerabilities. Clearly, the more important a resource is, the more attention should be paid to its security. Remember that both policies and risks must be reviewed on a regular basis to keep up with changes in the enterprise environment.

With policies in mind, an infrastructure can be designed and deployed that encompasses all the important elements, from access to applications and infrastructure to management, using a multi-layered approach. Layers not only provide multiple boundaries where defensive mechanisms can be

deployed, but also define zones within which resources can be scrutinized both for mismatches in the levels of security provided and for sufficient capacity of the devices and mechanisms (Farnsworth, 2004).

The security architecture should be developed holistically rather than simply pasting together what worked in previously separate networks in order to uncover and address potential gaps (Rybczynski, 2002). Exactly what data flow and access should be allowed across various boundaries within the network perimeter may be as important as what crosses the perimeter itself. Remember that a majority of security threats still arise from poor mechanisms or practices. Each boundary needs to be carefully considered and drawn to provide.

Overall converged networks require security that expands traditional data security policies and procedures to protect the privacy of all network information, including IP telephony traffic. A holistic approach is also important because simple extension of traditional data security practices can erode the quality of IP Telephony voice if not engineered correctly. In general, there are many more security considerations within voice application layer controls that should be considered.

Finally, security planning must include disaster recovery, and consideration of business continuity, to ensure that applications and services will function properly in spite of incidents such as power failures or storms, or can be restored quickly following them. What converged communications typically adds to these requirements is a range of new and different types of devices such as IP phones, voice communication servers, and media gateways. Planning needs to consider both preventive and reactive measures for all types of applications and traffic. For example, if there are communication servers at multiple locations and one becomes unavailable, another should take over its tasks with no loss of functions or features.

If improperly planned and implemented, VoIP can pose significant operational risks. Therefore, firms should perform a comprehensive risk assessment before implementation to ensure the confidentiality, integrity and availability of voice communications using VoIP technology.

III. Voice Over IP Security Threats

The Voice over IP security alliance (VoIPSA) has developed The VoIP Security and Privacy Threat Taxonomy. (VOIPSA, 2005) The threats turn out to be similar to the conventional public switched telephone network (PSTN), but with added problems that come from running calls across the Internet.

Topping the industry body's (VOIPSA, 2005) list are more familiar issues such as privacy and eavesdropping, harassment by phone, premium rate abuse, and hijacking of service, all of which remain to be tackled by the industry. Businesses used to the PSTN might not, however, be as acquainted with other threats that will arrive with the technology. These include VoIP spam, caller-ID impersonation, and denial of service attacks, authentication and complex ID fraud.

As to denial of service attacks specifically, the report lists eight methods by which this can be initiated, which brings home the point that the VoIP world will have more in common with that of computing than that of the telephone networks people have become used to. And these are only the top-level security issues. Calls can also be "black holed", or terminated unexpectedly, rerouted, and degraded. As well as interfering with quality of service they will also make possible further security threats such as call impersonation (VOIPSA, 2005).

The opportunity for attacks against VoIP networks can be categorized as follows: (Radware,2005, p.7)

- *VoIP network operating system devices*, such as call managers, gateways and proxy servers, which could provide access to the launching of sophisticated attacks against entire VoIP networks, DoS and buffer overflows.
- *Configuration weaknesses in VoIP devices*, such exposed TCP and UDP ports in default configurations which, when compromised, can leave networks exposed to DoS, buffer overflows and password hacking.
- *IP infrastructure attacks*, such as any DDoS, SYN floods or other traffic surge attacks that exhaust network resources and could severely impact all VoIP communications. Additionally, VoIP protocols are vulnerable to any low-level attack, such as session hijacking, malicious IP fragmentation and spoofing, as well as IP protocol anomalies which can cause unpredictable behavior in IP services.
- *VoIP protocol implementation vulnerabilities*, such as DoS and buffer overflow attacks launched on functional protocol testing packets used for monitoring abnormal behavior on applications, operation systems and hardware devices. Readily available on the internet, these testing packets provide hackers with the tools necessary for crashing vulnerable implementations.
- *VoIP application level attacks*, such as DoS (spoofing identity can cause DoS in SIP-based VoIP networks), call hijacking (by spoofing SIP responses t hijack a call), resource exhaustion (by exhausting IP addresses in a VoIP network), eavesdropping (by sniffing network traffic and deciphering voice conversations), message integrity (man-in-the-middle attacks changing original communications between two parties) and toll.

IV. Voice Over IP Security Recommendations

A report from the U.S. National Institute of Standards and Technology (NIST) advises federal agencies to implement appropriate security measures when deploying voice over Internet Protocol (VoIP) telecommunications technologies. *Security Considerations for Voice Over IP Systems* (Special Publication 800-58) offers recommendations that agencies and other organizations can follow to reduce security risks and make the most VoIP benefits. (Kuhn, Walsh & Fries, 2005)

According to the NIST (Kuhn, Walsh & Fries, 2005) report, organizations can't assume that digital voice calls can be secured in the same manner as data communications. VoIP demands a higher level of performance than data networks and requires its own equipment, protocols, and software. At the same time, the report notes that the dynamic nature of VoIP network parameters creates potential security vulnerabilities. As a result, such networks need additional layers of defenses to protect voice calls. However, many of the security measures commonly used on data networks — such as encryption, firewalls, gateways, and Network Address Translation — can hinder the quality of voice service.

To integrate voice and data communications securely, NIST offers the following guidelines: (Kuhn, Walsh & Fries, 2005)

- **Ensure that the organization has examined and can manage and mitigate the risks to information, systems operations and continuity of essential operations when deploying VoIP systems.** When implementing VoIP, organizations need to manage risks to information, systems functions, and essential operations, the report advises. Considerations include technical knowledge and training, security practices, controls, policies, and system architectures. VoIP also has security, privacy, and confidentiality risks. Finally, as a developing technology, VoIP isn't as stable or as established as analog phone service.
- **Assess the level of concern about security and privacy. If warranted and practical, do not use soft phone applications, which utilize VoIP with a personal computer and client based software.** Where security and privacy are an issue, the NIST report recommends that organizations not provide voice service through personal computer systems that combine software with a voice headset. Security concerns such as worms, viruses, and Web browser vulnerabilities raise unacceptably high risks for most soft phone applications, the report notes.
- **Carefully review statutory requirements fro privacy and record retention with legal advisors.** The NIST report notes that U.S. laws regarding monitoring of voice calls and retention of call records may be different from those for conventional land-line networks. VoIP systems may also produce different types of call data than analog networks. The Privacy Act of 1974 governs privacy issues for U.S. government agencies such as retaining call records, which can be used to reconcile service billings and to detect fraud and abuse of services.
- **Develop appropriate network architecture.** NIST recommends that organizations keep voice and data networks separate, if possible. Access control and strong authentication should be used at the voice gateway. Organizations also need a way to carry voice traffic through firewalls, such as using application-level gateways or session border controllers. The report advises using Internet Protocol Security (IPsec) virtual private network or Secure Shell for remote management and auditing and using encryption at the router or gateway to lessen performance problems.
- **Deploy VoIP ready firewalls and other appropriate protection mechanisms. Organizations should enable, use and routinely test the security features of the VoIP system.** Digital voice networks need firewalls and other security technologies that are compatible with VoIP protocols to prevent system vulnerabilities such as packet sniffing.
- **Properly implement physical controls in a VoIP environment.** Organizations need to ensure that physical controls are in place to prevent access to VoIP network components. According to the report, such networks provide greater opportunities for users to listen in on phone conversations or monitor voice traffic than are available on analog networks.
- **Evaluate costs for additional power backup that may be required to ensure operation during power outages.** To prevent outages, organizations should have sufficient backup power systems at the VoIP network switch and desktop.
- **Consider the need to integrate mobile telephones with the VoIP system. If the need exists, use products implementing WiFi Protected Access (WPA) rather than Wired Equivalent Privacy (WEP).** The report recommends that organizations that plan to allow wireless access to their VoIP network make the WiFi Protected Access (WPA) security protocol part of their overall defenses. WPA offers significantly greater security than earlier wireless encryption

technologies. However, U.S. government standards mandate that federal agencies use strong encryption such as Secure Shell or IPsec to protect confidential information.

- **Give special consideration to emergency services communications (E-911) because the E-911 automatic location service is not always available with VoIP.** Organizations need to make sure their VoIP network can access emergency 911 services. Because VoIP is packet-switched like data, the area code of a telephone number may not indicate the actual location of the caller. A person calling for assistance from a number with a 704 area code could be located in Hawaii or Alaska, instead of North Carolina.

References

Bourque, L. (2005, April) VoIP Security Considerations for Enterprises. Retrieved October 13, 2005, from http://www.enterpriseitplanet.com/security/features/article.php/3497496

Collier, M. (2005, September). The Current State of VoIP Security. Retrieved October 27, 2005, from http://www.voip-magazine.com/content/view/511/0/

Cyber Security Industry Alliance (2005, May). Cyber Security for IP Telephony. Retrieved November 7, 2005 from https://www.csialliance.org/resources/pdfs/CSIA_VOIP_May_2005.pdf

Farnsworth, R.W. (2004, July). Enterprise Security – an Enabler of VoIP. Converge Network Digest. Retrieved Novemebr 3, 2005, from http://www.convergedigest.com/blueprint/ttp04/z4cisco1.asp?ID=141&ctgy=4

Garretson, C. (2005, July) VoIP security threats: Fact or fiction?, Network World. Retrieved October 28, 2005 from http://www.networkworld.com/news/2005/072505-voip-security.html

Jaikumar Vijayan (2002, October). VOIP: Don't overlook security. Computer World Retrived October 9, 2005, from http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html

Kuhn, D.R., Walsh, T.J., Fries S. (2005, January). National Institute of Standards, Security Considerations for Voice Over IP Systems. Retrieved October 15, 2005, from http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Morrissey, P. (2005, August). VoIP Security Keeping IP Voice Safe and Sound, Network Computing. Retrieved October 13, 2005, from http://www.networkcomputing.com/shared/article/printFullArticle.jhtml;jsessionid=U00U2ULREZXFMQSNDBCSKHSCJUMEKJVN?articleID=168600463

VOIPSA (Voice Over IP Security Alliance). 2005, October). VoIP Security and Privacy Threat Taxonomy. Retrieved November 3, 2005, from http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

Radware (2005, August). VoIP: Security Threats and Solutions. Retrieved November 3, 2005, from http://www.radware.com/content/document.asp?_v=about&document=6142

Rybczynski, T. (2002, December). Securing IP Telephony. Retrieved October 3, 2005 from http://www.tmcnet.com/it/1202/1202in.htm

Sicker, D.C., Lookabaugh, T. (2004, September). VoIP Security: Not an Afterthought. Queue, pp.56-64.

Werbach, K. (2005, September). Using VoIP to Compete. Harvard Business Review, pp. 140 – 147.

Whitman, M.E., Mattord, H.J. (2004). Management of Information Security.
Boston, MA: Thomson