



# VoIP Security Primer

## Protecting VoIP Users From a New Breed of Threats

Voice-over-Internet Protocol or VoIP is quickly becoming the telephone service of choice for companies and consumers alike. With dramatic cost savings over traditional phone systems and possibilities for new applications, Internet-based telephone equipment is now leading sales. It is estimated that by 2009 VoIP will represent over 90 percent of all enterprise phone systems worldwide. But for all the benefits of VoIP, users are at serious risk with this new technology. As telephone service providers and enterprises are making the move to VoIP, security has quickly emerged as a major concern that needs to be addressed before it can be a mass-market reality. Without proper VoIP security architectures, customers lose trust in the availability and integrity of the service.

VoIP-specific security attacks and vulnerabilities are emerging and there's no question that attacks will increase in frequency and severity as VoIP becomes mainstream. Recently, Cisco issued two alerts related to vulnerabilities in Call Manager. Fortunately, this time, these flaws were discovered before they could be exploited.

IP-based telephone communications are exposed to all of the existing vulnerabilities of data networks plus a whole new series of threats specific to VoIP technology:

- **Service Disruption:** These include Denial of Service (DoS) attacks and viruses which can seriously impact the quality of VoIP services or make them unavailable. DoS attacks are designed to overload the network with in an effort to disrupt services. IP-specific viruses clog the network and exploit weaknesses in operating systems and programs. When the SQL Slammer worm hit a major U.S.-based brokerage firm, brokers' IP-based phones were knocked out, leaving them unable to execute any trading activity. This type of service outage, which may be come increasingly common, had major financial and business consequences for this firm.
- **Spam over Internet Protocol (SPIT):** Spammers are increasingly creative as they are trying to find new ways to get around anti-spam technologies. It is expected that one of spammer's next targets will be VoIP-based voicemail boxes, which has the potential to quickly overwhelm the telephone services.
- **Privacy Violations:** By moving telephone services to the Internet, a whole new set of privacy issues are introduced. The most common privacy threats are call eavesdropping, insertion and disruption, as well as masquerading, impersonation, registration hijacking, and replay. Free tools already exist on the Internet that allows someone connected to a VoIP network to 'sniff' phone calls and then an attacker can listen, copy, alter, and replay confidential phone conversations. The possibilities for new scams, identity theft, or even threats to national security could result from such privacy violations.
- **Service Theft:** With the deployment of VoIP come new possibilities for criminals to defraud service providers by committing acts such as toll fraud, subscription fraud and non-payment. Call tracking tools can be used to capture authentication credentials and subsequently spoof legitimate users to place calls at the subscriber's expense.

### Global adoption of VoIP

Major North American service providers including AT&T, Bell Canada, Comcast and Verizon are now offering VoIP services

IP phone company Vonage has launched services in the U.S., U.K and Canada and currently adds approximately 40,000 new subscribers each month

Despite the understanding of the need to secure VoIP deployments, there's a lack of technology that addresses the unique nature of telephony networks. Currently available security solutions are merely an extension of existing data security products, and fail to address the complexity and reliability needs of VoIP networks. While many of the lessons learned from the data security world are valuable to consider when deploying VoIP, it is important to remember that VoIP security is unique and demands much more than a one-size fits all approach.

## VoIP Can Be Secured

- **Deploy Secure VoIP:** In designing and deploying VoIP networks, security cannot be an afterthought. It is essential to include a proactive security strategy from the onset of VoIP deployment to keep costs manageable. With the right technologies and security strategies in place, even the smallest organizations can deploy secure VoIP.
- **Take a Proactive, Systems-Level Approach:** To successfully secure VoIP networks, a proactive security strategy is required to ensure that risks can be identified and eliminated before the network is impacted. The complexity of VoIP networks demands a systems-level approach, which enables organizations to secure all parts of the network. A firewall-type approach where only the "door" to the network is secured leaves many "windows" for intruders to penetrate the network and brings the risk of serious financial and business consequences.
- **Choose VoIP-specific Security Technologies:** In the rush to fill the need for VoIP security solutions, many data security vendors have adapted existing data solutions or created add-ons to their existing products. Telecommunications networks are very different than data networks, so organizations should look for solutions that are specifically designed to secure telephony networks and built to address VoIP security issues.
- **Listen to the Experts:** Regulatory and other invested organizations are rushing forward with solutions to address the need for VoIP security. In January 2005, the U.S. NIST (National Institute of Standards and Technology) issued a strategic report on VoIP security, which urged organizations to proceed with caution, and outlined nine specific recommendations for deployment. And VoIP technology and security product vendors have formed VoIPSA (VoIP Security Alliance), with the organization's first act being a warning as to the potential for security attacks.

### VoIP Security Resources

NIST Report: <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

VoIP Security Alliance (VoIPSA): [www.voipsa.org](http://www.voipsa.org)

VoIPshield Systems [www.voipshield.com/resources](http://www.voipshield.com/resources)

For anyone looking to make the move to VoIP, security should be the number one priority. But security concerns should not prevent organizations from taking full advantage of the business benefits of VoIP. By taking a proactive approach to VoIP security from the early stages of deployment, everyone can protect their next-generation voice networks in a holistic, cost-effective manner.