

Top Five Ways VoIP Security is Different

By Bogdan Materna, CTO and VP Engineering, VoIPshield Systems

For service providers and enterprises to successfully deploy VoIP, it is important to understand that while some VoIP security requirements are similar to those in data networks, several areas are specific to VoIP. Let's examine these differences:

1. VoIP is Real-Time: First and foremost, VoIP is a real-time service and requires security infrastructure to provide automated, real-time response to security threats in order to preserve very high availability demanded by telephony users. The types of attacks that are common in the data security realm and render email and computer networks unusable for several hours, are not acceptable when it comes to IP communication.

2. New Hardware and Components: VoIP infrastructures includes a wide range of components and applications such as telephone handsets, conferencing units, mobile units, call processors/call managers, gateways, routers, firewalls, and protocols that allow for new forms and types of security attacks. Since VoIP communications are carried in the form of packetized voice there is potential for such malicious activities as call eavesdropping, malicious replay or identity theft.

3. New Types of Threats and New Technologies: VoIP services are offered with many features such call ID, call forward, voice mail and three-way calling , which open up service providers to a number of new threats such as toll fraud, service theft, voice spam (SPIT), and identity theft. The introduction of new technologies such as advanced wireless technologies and concepts such as VoIP over Wi-Fi, Wi-Max and IMS create other security concerns. Presently, VoIP wireless networks do not provide strong encryption and authentication and they are much more accessible to potential attackers. While wireline networks require a physical access to the wires, wireless technology allows remote attackers to tap into the VoIP networks without any physical access to the network.

4. Delay, Packet Loss, and Jitter: Data security is based on deployment of a number of security devices and applications to protect and observe networks such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN), authentication services, anti-virus software and gateways. Paradoxically, VoIP is highly sensitive to delay, packet loss and jitter, making these security measures inadequate. For example, current firewalls/NAT will delay or block call setups, encryption engines will introduce additional jitter and in-line IDS/IPS devices will add delay to inspected packets. Another challenge of using data security devices for VoIP security is that there's a lack of coordination between security devices making it ineffective in protecting VoIP services from sophisticated, system level attacks and internal threats.

5. Gateways: For the foreseeable future PSTN and VoIP networks will coexist and require media gateways that provide internetworking between carrier IP networks and TDM-based PSTN networks. This could enable cross-network security attacks impacting mission-critical PSTN networks.

Conclusion

The real-time nature of VoIP, stringent QoS and availability requirements impose new demands on the security infrastructure and processes. Existing data security technologies fall short in addressing the unique needs of VoIP deployments. Security applications and devices must seamlessly support VoIP protocols without impacting QoS parameters such as packet delay, loss and jitter. The infrastructure used to secure VoIP must be able to support automated detection and response to security threats in order to support PSTN-like availability requirements. Without recognizing the differences between VoIP and data security, PSTN-level service cannot become a reality.

About the Author

Bogdan Materna is the CTO and VP of Engineering at VoIPshield Systems (www.voipshield.com) a provider of VoIP security software. He can be reached at bmaterna@voipshield.com or (613) 224-4443.