



February 2006

# Understanding Voice-Over-IP (VoIP) Security

By Bogdan Materna, CTO and VP Engineering, VoIPshield Systems

The emergence of Voice-Over-IP (VoIP) technology is creating a major discontinuity in telecommunications. The promise of reduced hardware and operations costs coupled with a promise of new value-added services makes VoIP and then subsequently IP TV, videoconferencing, IP Multimedia Subsystem (IMS) and presence services a compelling solution for enterprises and service providers. But at the same time, VoIP introduces a set of new problems for the network operators and services providers. Current voice services provide high voice quality, very high reliability (99,999%), carry critical services such as E911, enable federal agencies with ability for lawful intercept while offering an extremely high level of security operating on well established PSTN networks.

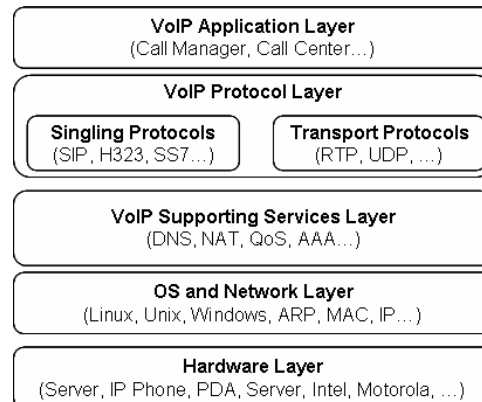
Enterprises, carriers and cable companies have publicly committed to VoIP deployments. However, there are several issues that need to be addressed if there is to be widespread acceptance and adoption of VoIP. Currently, the security of VoIP networks is considered as a one of the prime concerns and barriers that could significantly delay deployment of VoIP networks. This article examines unique nature of VoIP security requirements and specific VoIP security threats.

Comprehensive security architecture for VoIP networks is proposed and discussed in the context of practical VoIP security problems. A references section is included at the end of the article.

## ***VoIP Security Requires A Different Approach***

VoIP is not just another application running on the top of the IP infrastructure. VoIP is a complex service, as shown above, with its own business models and set of features offered to the end-user, similar to existing

PSTN and PBX offerings. Over the years, service providers and PBX vendors have established their respective brands as being synonymous with high levels of reliability, quality and security and need to preserve these attributes in their VoIP offerings. The VoIP reliability requirements are very stringent and approaching 99.999% (5 minutes of downtime a year). Clearly, this level of reliability calls for automated, real time response to the security threats and attacks. The types of attacks that are common in the data security realm and may render email or the computer network unusable for several hours are not acceptable when it comes to IP communication.



VoIP characteristics such high sensitivity to Quality of Service (QoS) parameters, real-time nature of the service, a wide range of infrastructure devices, protocols and applications, and interaction with the existing phone networks require different techniques and methodologies that will support PSTN like security and reliability.

VoIP QoS sensitivity to packet delay, packet loss, and packet jitter makes most the existing security solutions inadequate. Existing firewalls cannot efficiently handle

## - Understanding Voice-Over-IP (VoIP) Security -

new VoIP protocols such as standard based SIP and a wide range of vendor proprietary protocols such as Cisco Skinny or Nortel Unistim since they rely on dynamic port ranges and do not support Network Address Translation (NAT) very well. A new generation of the firewalls called Session Border Controllers (SBC) is addressing most of these problems.

Most of the firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and similar security devices rely on deep packet inspection techniques that introduce delays and jitter to the VoIP packet streams thus impacting overall QoS. In VoIP world, maximum packet delay is set to 150 ms (in some cases higher) but the multi-layer nature of security infrastructure could add significant delays and jitter that would make the VoIP services unusable.

There is also the issue of balance between encryption and QoS. Existing encryption engines will introduce additional jitter and delay that would be cumulative due to hop-by-hop encryption schemas foreseen to be used by VoIP calls. For the foreseeable future PSTN and VoIP networks will coexist and require media gateways that provide internetworking between carrier's IP network and TDM based PSTN networks. This could enable cross-network security attacks impacting existing PSTN networks.

VoIP is a real time service, i.e., it is happening in real-time and no information is stored anywhere on the network. As result any loss of information cannot be recovered or retransmitted. This makes the VoIP services very susceptible to worms and DoS attacks that could very easily disrupt voice communication.

Also, the complex nature of VoIP infrastructure consisting of a wide range of components and applications such as telephone handsets, conferencing units, mobile units, call processors/call managers, gateways, routers, firewalls, and specialized protocols requires system level approach where security is built into all the infrastructure layers and coordinated via centralized control center.

### **VoIP Security Threats**

For VoIP infrastructure and services to function properly requires appropriate hardware, operating systems, supporting services such as DNS, DHCP and AAA, IP and VoIP specific protocols such as SIP, H.323, RTP and TCP/UDP. A number of VoIP applications such as call managers, voice mail, SIP servers, call centers and soft-switches are running on the top of this infrastructure. In turn, these applications are part of VoIP service offerings with appropriate billing mechanisms, large number of features and binding Service Level Agreements (SLA).

The VoIP security threats can be categorized in three distinct functional categories: attacks that aim at compromising VoIP service availability, malicious activities where the goal is to compromise integrity of the services, and eavesdropping.

As already discussed, VoIP high sensitivity to QoS parameters amplifies the threat of the known attacks such as Denial of Service (DoS) attacks, viruses and worms.

These threats use VoIP specific protocols and VoIP application vulnerabilities to overload the network and impact VoIP QoS making the service unavailable. They also will target critical VoIP applications such as end-user phones and soft-clients, call managers, authentication servers and billing applications.

VoIP service integrity can be compromised by toll fraud, identity theft, and fraud attacks. For example, a hacker's VoIP phone can be connected to the network and then use stolen or guessed user account and password to place phone calls at the victim's expense. Also, VoIP conversations could be hijacked and the caller would be misled into communicating with the attacker, masquerading as a party to this call. In addition VoIP services are offered with many features such call ID, call forward, voice mail, three-way calling, etc. Each of these features could potentially be used for toll fraud, identity theft and spam.

A further area of concern for is that fact that for the foreseeable future PSTN and VoIP

## - Understanding Voice-Over-IP (VoIP) Security -

networks will coexist and require media gateways that provide internetworking between carrier's IP network and TDM based PSTN networks.

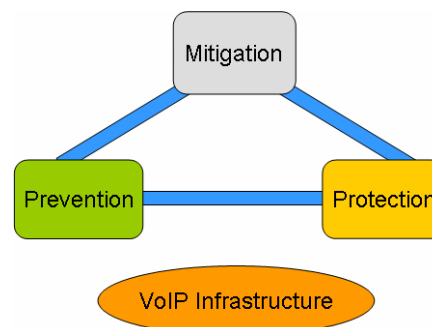
Eavesdropping on signaling and media paths allows the attacker to use Session Initiation Protocol (SIP) messages and Real Time Protocol (RTP) packets to obtain sensitive business or personal information. It also allows creating various man-in-the-middle attacks altering the content of the conversation.

### **VoIP Security Architecture**

An efficient and effective VoIP specific security infrastructure should consist of three, tightly integrated functional components:

- **Prevention:** This is the most cost effective way of improving VoIP security levels. VoIP-specific vulnerability assessments should be performed in the lab before the VoIP equipment and applications are deployed. This enables organizations to independently verify vendor claims and to identify security flaws before they can become real issues to the end-users. It is also highly advisable to perform vulnerability assessment across all the VoIP components prior to the commissioning of VoIP infrastructure. At this stage interactions and dependencies between VoIP applications and devices could create additional security vulnerabilities not visible during the lab stage assessments. Finally, periodic or, where justified, continuous vulnerability assessments should become part of the VoIP Operations, Administration, Maintenance and Provisioning (OAMP) process. Once the potential security vulnerabilities are identified they should be addressed by appropriate actions such as patching, re-configuration, and network tuning.
- **Protection:** Protection provides protection of the VoIP services from security threats during their life

cycle. There are number of various security architectures and solutions that could be deployed but all of them have to be "VoIP friendly" so they do not impact service quality and reliability. The deployment of a multi-layer security infrastructure that provides both perimeter as well as internal network protection will meet the protection requirements of most organizations. In most cases it will consist of a number of security devices and host based applications to protect VoIP networks such as SBCs, VoIP Network Intrusion Detection Systems (IDS), VoIP Network Intrusion Prevention Systems (NIPS), VoIP DoS defenses, Host IPS's, AAA servers, encryption engines, and VoIP anti-virus software.



- **Mitigation:** The experience of securing data networks tells us that no matter how good our prevention or protection is, that soon or later an attacker will successfully penetrate our defenses and wreak havoc on VoIP infrastructure. Currently, these incidents are being resolved through the combination of human intervention and security management tools however, VoIP networks cannot tolerate multi-hour or multi-day downtimes if they are required to support 99.999% availability (five minutes downtime per year). More automated VoIP security mitigation solutions are required to keep VoIP services running even in the presence of major security threats such as DoS

## - Understanding Voice-Over-IP (VoIP) Security -

or fast-spreading worms. VoIP is the first application that truly requires automated mitigation systems. These systems are able to respond autonomously to the detected security threats and keep their impact at the levels where VoIP services can still function albeit at lower QoS

### **Conclusions**

VoIP requires different approach to security which takes into account the unique nature of telecommunications networks and how greatly VoIP differs from traditional data security. The specific characteristics of VoIP networks combined with the mission critical importance of many voice applications imposes stricter requirements on the security applications and devices than we see with data networks. To effectively secure VoIP networks, organizations need to proactively address security at three levels – prevention, protection, and mitigation. By taking a holistic approach to VoIP security , enterprises, carriers and cable operators will be able to preserve the attributes of quality, reliability, and security that we've come to expect from the existing phone networks.

### **About the Author**

*Bogdan Materna is the CTO and VP of Engineering at VoIPshield Systems ([www.voipshield.com](http://www.voipshield.com)). He can be reached at [bmaterna@voipshield.com](mailto:bmaterna@voipshield.com) or (613) 224-4443.*

