A Proactive Approach to VoIP Security

Understanding VoIP security requirements, threats and architectures

A corporate whitepaper
by Bogdan Materna
Chief Technical Officer
and VP Engineering

www.voipshield.com

Introduction

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 new value-added services makes VoIP, as well as Internet Protocol (IP) TV, videoconferencing, IP Multimedia Subsystem (IMS) and presence services, a compelling solution for enterprises and service providers. Current voice services which are delivered using Public Switched Telephone Networks (PSTN) provide high voice quality, very high reliability (99.999 per cent), carry critical services such as E911, enable federal agencies with ability for lawful intercept, all while offering an extremely high level of security. For VoIP networks to become a reality, both enterprises and service providers must be able to ensure that voice networks are able to deliver the identical quality, reliability, flexibility and security to that of PSTN.

With enterprises, carriers and cable companies publicly committing to VoIP deployments, security has quickly emerged as one of the biggest barriers to the successful deployment of VoIP. To securely implement VoIP networks a proactive approach and an understanding of the differences between VoIP and traditional data networks is required. This document examines these differences, new types of attacks, and provides a comprehensive security architecture for VoIP networks in the context of practical VoIP security problems.

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. Similar to existing PSTN and Private Branch Exchange (PBX) offerings, VoIP has its own business models and features which are offered to the end-user. 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 must preserve these attributes in their VoIP offerings.

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

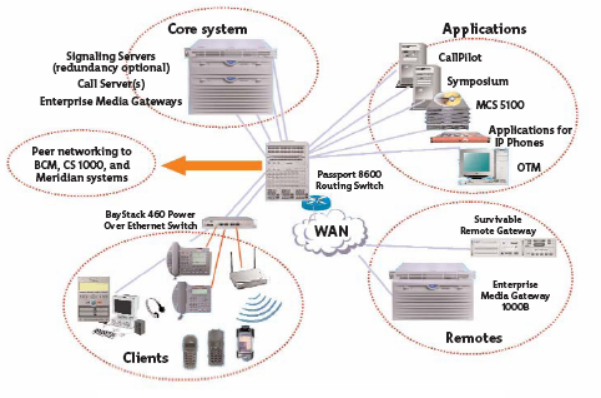

Fig 1: VoIP is a complex service

For example, in the data security realm, common attacks, such as Denial of Service (DoS), often result in email or computer networks being unusable for several hours. To meet the high reliability requirements of VoIP networks, which are approaching 99.999 per cent or a total of less than five minutes of downtime per year, any type of attack would have to be stopped in a matter of seconds. With such high reliability requirements, VoIP networks must have a security approach which enables an automated, real-time response. Any attack must be addressed before there can be any service disruption.

The high sensitivity of VoIP to QoS parameters such as packet delay, packet loss, and packet jitter makes most currently available data security solutions inadequate. Existing firewalls cannot efficiently handle new VoIP protocols such as Session Initiation Protocol (SIP) and a wide range of vendor proprietary protocols since they relay 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.

These techniques introduce delay 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. As PSTN and VoIP networks coexist media gateways that provide internetworking between carrier's IP network and TDM based PSTN networks will be required. This could enable cross-network security attacks which impact existing PSTN networks.

VoIP is a real-time service. All communications are 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 VoIP services very susceptible to worms and DoS attacks that could very easily disrupt voice communication.

Finally, the complex nature of VoIP infrastructure demands a different approach to security. A VoIP network consists 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. As a result, a system-level approach where security is built into all the infrastructure layers and coordinated via a centralized control center is required.

VoIP Security Threats

For VoIP infrastructure and services to function properly appropriate hardware, operating systems, supporting services such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) and Authentication, Authorization and Accounting (AAA), IP and VoIP specific protocols such as SIP, H.323, Real-Time Transport Protocol (RTP) and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) are required. 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).

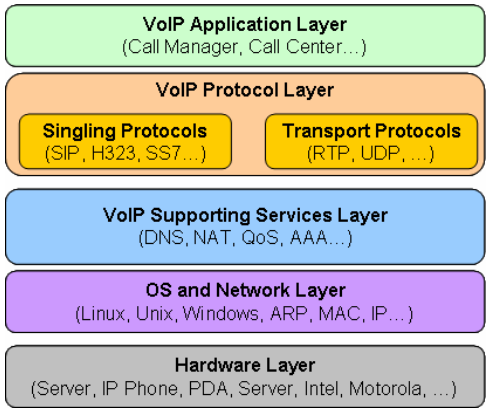

Fig 2: Layers of VoIP network

Since VoIP security attributes and characteristics are different than those of existing data networks there are also different types and categories of security attacks specific to VoIP networks. VoIP security threats can be categorized in many ways and fall into four main categories: attacks that aim at disrupting or VoIP service availability, malicious activities the goal of which is to compromise integrity of services, Spam over IP Telephony (SPIT) and eavesdropping.

Service Availability

Service availability attacks are currently viewed as the most significant VoIP security threats to VoIP networks. This type of attack has the potential to quickly impact customers, resulting in lost revenues, system downtime, lost productivity and unplanned maintenance costs. Furthermore, such attacks are a major concern for service providers providing public services such E-911, as even the smallest disruption could have significant or even catastrophic consequences.

VoIP availability is the most important component of any commercial VoIP offering. If the availability of VoIP services is impacted, service providers and enterprise revenues could be affected. The very high QoS levels required by any voice service,

amplifies the threat of attacks such as DoS, viruses and worms. A generic worm attack can very quickly cripple a VoIP network, long before the data network is impacted, since it has a much higher sensitivity to QoS. What may cause a data network to slow down temporarily has the potential to rapidly knock out voice networks.

DoS, virus and worm-based threats will also use VoIP specific protocols and VoIP application vulnerabilities. These directed threats will be much more difficult to detect and stop in VoIP networks since the existing security devices do not have specific knowledge of these threats and vulnerabilities. Attacks will target critical VoIP applications such as end-user phones and soft-clients, call managers, authentication servers and billing applications.

Other common scenarios which impact service availability is the flooding of VoIP components with signaling protocol packets causing exhaustion of resources or DoS attacks that exploits loop and spiral implementation on a call manager. Open source call manager software provides easy access to potential attackers, enabling them to create peer-to-peer attacks on commercial soft switches and PBXs. For example, attackers could have two or more call managers continually forward a single request message back and forth to each other until resources on the targeted call manager/softswitch are exhausted. This method of attack can quickly affect a large number of phones leaving them unable to initiate or receive calls.

A final area of concern is that in the near-term VoIP and PSTN networks will co-exist. To facilitate internetworking between PSTN and VoIP networks, media gateways are required. Since placing of the calls from VoIP network via PSTN requires interaction between VoIP signaling protocols and PSTN SS7 infrastructure new vectors of attack are being introduced. Attackers now have new opportunities for attacks on PSTN through the VoIP network and the media gateway. Examples of these attacks include Destination Unavailable (DUNA) or Signaling Congestion (SCON) attacks.

Examples of VoIP Security Vulnerabilities

Services

- Voicemail exploits
- Dialing plan security (calls to 1-900 or other numbers)
- Transferring to '9011' extension for long distance exploits

Applications

- Buffer overflows
- Format-string exploits
- Scripts
- Password cracking
- Overload (DoS, DDoS)

VoIP Protocols

- Session tear-down
- Impersonation
- Session hijacking
- SIP-SS7 boundary messages tampering
- Malformed messages
- Loops and spirals
- Overload (DoS, DDoS)

VoIP Supporting Services

- DNS
- SNMP
- LDAP
- Web servers
- VPN
- Email
- SQL Database

VoIP OS and Networking

- Buffer overflows
- Format-string exploits
- Scripts
- Password cracking
- Overload (DoS, DDoS)
- ARP cache poisoning
- WEP

Service Integrity

Service integrity threats are focused on compromising VoIP services through toll fraud, identity theft and other fraudulent acts. Service integrity threats have the potential to impact service providers through lost revenue and damage to their reputation, while government organizations and enterprises may be impacted by the leakage of sensitive or proprietary information. Individual consumers may also be impacted as scams are developed which victimize them through identity and service theft.

As new, converged services such as IP TV are being deployed, content theft has the potential to become a major problem for service providers. In this scenario, a hacker could record the content of the broadcast and then sell it illegally. Another possible scenario is broadcast hijacking where a potential attacker intercepts an IP TV broadcast and re-broadcasts it to unsuspecting users.

VoIP services are offered with many features such call ID, call forwarding, voice mail and three-way calling which could be used for toll fraud, identity theft and spam. For example, a false identity in the form of a false caller ID, voice mail or phone number could be easily implemented by relatively unsophisticated hackers.

More sophisticated attackers could use interception/modification attacks that include conversation alternation, impersonation and hijacking. Conversation alternation, impersonation and hijacking includes various modifications of any voice, video, text and/or imaging data. First, attackers would collect and translate VoIP information. Then, the content of the conversation would be altered in real-time in order to deliver false and misleading information to a third party. Finally, VoIP conversations would be hijacked and the caller would be misled into communicating with the attacker, masquerading as a party to this call.

A hacker could also commit toll fraud via a VoIP phone that is registered using a stolen or guessed user account and password. Once this is accomplished, the hacker can place phone calls at the victim's expense.

SPIT

Spam has become a major concern in the data security world as millions of unwanted messages are sent around the world each day. It is expected that SPIT will fill up users' voicemail boxes just like email spam does today.

SPIT presents another potentially critical threat to VoIP services and to existing PSTN users. While there are advanced solutions that address e-mail spam such as blacklists and quarantines, combating SPIT is much more difficult due to the real-time nature of voice services. Also, the impact of having to deal with many unsolicited phone calls during the day and night may have a chilling impact on the deployment of VoIP services.

For example, a telemarketer interested in sending out an unsolicited advertisement could easily collect phone numbers for VoIP services. Any of these phones could be targeted. Then, the telemarketer would create an audio ad and send it to all VoIP users at the same time.

Eavesdropping

Eavesdropping on signaling and media paths enables attackers to obtain sensitive business or personal information. Once the information is collected and translated, various man-in-the-middle attacks altering the content of the conversation could be launched. Examples of these attacks are insertion and disruption, masquerading, registration hijacking, impersonation and replay.

A simple example of the eavesdropping threat could be the collection of VoIP information included in packets and then the translation of this information into plain speech. In this scenario, calls related to national security or financial information, could be intercepted and provide third parties with confidential information. In more sophisticated scenarios, valid VoIP calls to a financial institution could be intercepted and then re-directed to a bogus bank representative.

A Proactive Security Architecture for VoIP

With new challenges and types of attacks, VoIP clearly requires a more sophisticated approach to security than those currently used to secure data networks. Solutions based on network-based devices and signature-based applications simply are not going to address the real-time nature and complexity of VoIP networks. A system-based approach that combines network and host-based security devices and applications with sophisticated, systems-level threat mitigation systems will be required to efficiently protect the entire VoIP infrastructure.

In building a systems-level approach to VoIP security, a unified VoIP specific security infrastructure architecture consists of three functional components: prevention, protection and mitigation.

Prevention

Prevention enables organizations to proactively identify and fix VoIP-specific vulnerabilities before they impact end-users. A commonly used approach from the data security world, vulnerability assessment (VA) is particularly effective as a proactive strategy. By performing a VoIP VA in the lab, before any VoIP equipment and applications are deployed, organizations are able to verify vendor claims and identify security flaws early in the deployment cycle. Executing a VoIP VA of all components prior to the commissioning of the VoIP infrastructure is recommended. This process enables the identification of security vulnerabilities not revealed during earlier testing. Once VoIP is deployed, periodic or, where required, continuous vulnerability assessments should become cornerstone of an overall proactive VoIP security strategy. Once security vulnerabilities are identified they should be addressed by appropriate actions such as patching, re-configuration and network tuning. These actions should be clearly defined as part of the company's overall security policy to provide a framework for dealing with possible threats to VoIP security.

Protection

Within the VoIP network, various security architectures and solutions should be deployed to protect VoIP services from security threats during their life cycle. Any security architectures and solutions deployed must be "VoIP aware" so they do not impact VoIP service quality and reliability. It is recommended to deploy a multi-layer security infrastructure that provides both perimeter as well as internal network protection. In most cases, it will consists of a number of security devices and host based applications to protect VoIP networks such as SBCs, VoIP Network Intrusion Prevention Systems (NIPS), VoIP DoS defenses, VoIP Network Intrusion Detection Systems (IDS), Host IPSs, Authenication, Authorization and Accounting (AAA) servers, encryption engines and VoIP anti-virus software. All the devices and applications have to be coordinated via a higher level application providing unified view of the end-to-end VoIP infrastructure.

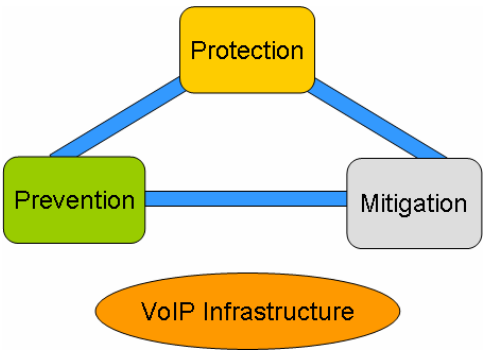

Fig 3: Security Architecture for VoIP

Mitigation

It is already widely accepted that no matter how good the prevention and/or protection in place may be, sooner or later an attacker or worm will successfully penetrate all the defenses and wreak havoc on VoIP infrastructure. To date, there have not been many widely publicized VoIP security attacks. However, as VoIP becomes more mainstream, it is really a matter of when and not if widespread attacks will occur. In dealing with these attacks, VoIP presents a unique challenge as IP services cannot rely on a human-based response for mitigation, as QoS will already be compromised.

Currently, a combination of human intervention and security management tools are being used to mitigate the impact of these attacks. As the VoIP market matures, and VoIP-specific attacks become more prevalent, these methods will not be sufficient as VoIP networks cannot tolerate multi-hour or multi-day downtimes if they are required to support 99.999 per cent availability. Expect to see solutions emerge which are designed to provide the real-time, automated VoIP security mitigation solutions needed to keep VoIP services running in the presence of major security threats such as SPIT, DoS or fast-spreading worms. Threat-mitigation systems should be 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. While VoIP threat mitigation systems are not currently available, they will become a key part of the VoIP security infrastructure in the next two to three years, and should be planned for.

Summary

VoIP requires a 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 strict requirements on security applications. 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.