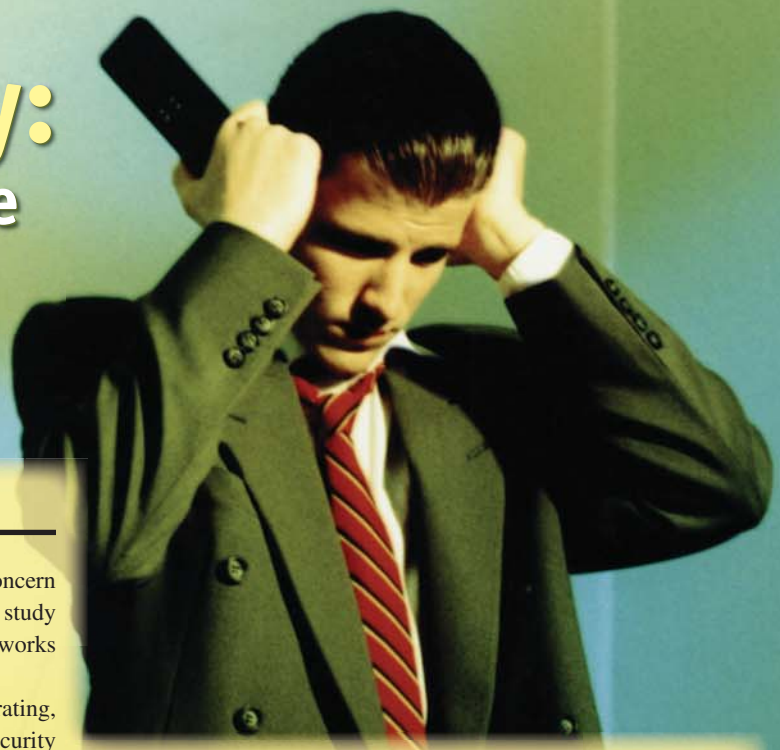
VoIP Security:
Who's Keeping An Eye On the Network?

By Bogdan Materna



INTRODUCTION

Security has consistently been cited as the number one concern for organizations deploying Voice-over-IP (VoIP). A recent study indicated that almost half of IT directors believe that VoIP networks are inherently insecure.

With the implementation of VoIP networks rapidly accelerating, there is greater uncertainty about the different types of VoIP security threats, the level of threat they pose, and how the VoIP network can be secured to prevent attacks.

Amid all the hype around VoIP security, organizations need to cut through the noise and gain an understanding of the VoIP security threat categories, as well as the potential outcomes of each type of attack. The perception and potential impact of security threats will strongly depend on business models and type of organization implementing VoIP infrastructure and services.

TRADITIONAL DATA SECURITY VS. VOIP SECURITY

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

- **VoIP is Real-Time:** First and foremost, VoIP is a real-time service as all phone conversations need to be conducted without any delays. As a result, security systems for VoIP need to provide an automated, real-time response to any threats in order to preserve very high availability expected by telephony users. Attacks that are common in the data security realm, and may render email or the computer network unusable for several hours, are simply not acceptable when it comes to Internet Protocol or IP-based communications.
- **New Hardware and Components:** VoIP infrastructures include a wide range of components and applications such as telephone handsets, conferencing units, mobile units, call processors/call managers, gateways, routers, firewalls, and protocols, all of which create new possibilities for would be attackers. Since VoIP communications are carried in the form of packetized voice there is a potential for such malicious activities as call eavesdropping, malicious replay or even identity theft.
- **New Types of Threats:** VoIP services are offered with many features such call ID, call forward, voice mail and three-way calling which open up service providers and end-users to a number of new threats such as toll fraud, service theft, and Spam over Internet Telephony (SPIT).
- **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. The challenge is that these technologies cannot be used for VoIP as they introduce delay, packet loss and jitter. For example, current firewalls/Network Address Translation (NAT) will delay or block call setups, encryption engines will introduce additional jitter and in-line IDS or IPS devices will add delay to inspected packets. A

further challenge of using data security devices for VoIP security is that there's an inherent lack of coordination between security devices, which makes them ineffective for protecting VoIP services from sophisticated, system-level attacks and internal threats.

- **New Technologies:** Introduction of new wireless technologies and concepts such as VoIP over Wi-Fi, Wi-Max and IP Multimedia Systems (IMS) creates another area of concern. 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 VoIP networks without any physical access to the network.
- **Gateways:** For the foreseeable future, existing traditional telephone and VoIP networks will coexist and require media gateways that provide internetworking between carriers' IP networks and Time Division Multiplexing (TDM)-based Public Switched Telephone Networks (PSTN) networks. This interaction may introduce new vectors of attack and provide opportunities for attacks on mission-critical PSTN through the VoIP network.

The stated goal of service providers and enterprises is to deliver VoIP services at availability levels approaching those of PSTN; that is, ensuring less than one minute downtime a year. Upon examining the unique nature of VoIP networks and how they differ from data networks, it becomes clear current security practices that rely on human-centered response are insufficient to counter the threats and to maintain availability and integrity of VoIP infrastructure at those levels. Additionally, the sheer scale of VoIP deployments creates a need for the security infrastructure to scale to these multi-million subscriber deployments.

NEW TECHNOLOGY, NEW SECURITY THREATS

With any new technology comes new threats to security, and VoIP is no exception. It is expected that as VoIP becomes more and more common, so will attacks on IP-networks. Currently, there are a number of possible threats to VoIP networks, which fall into three main categories: attacks that aim at compromising VoIP service availability, malicious activities with the goal of compromising integrity of the services, and eavesdropping.

Service Availability

The real-time nature of voice communications presents a number of unique challenges when it comes to attacks related to service availability. VoIP has very high sensitivity to Quality of Service (QoS) parameters which serves to amplify the threat of the known attacks such as Denial of Service (DoS) attacks, viruses, and worms. A virus attack on a data network that would merely slow down the network can quickly cripple a VoIP network as QoS is quickly compromised.

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

Other service availability threats include zero-day VoIP worms/viruses impacting VoIP servers, clients and QoS, buffer overflow related attacks on critical VoIP applications such as SIP servers. A common scenario is the flooding of VoIP components with signaling protocol packets causing exhaustion of resources and denial of service attacks. Another possible scenario includes a DoS attack that exploits loop and spiral implementation on a call manager to have two or more phones continually forwarding a single request message, back and forth, to each other until resources on the call manager are exhausted. This can quickly impact a large number of phones, leaving them unable to initiate or receive calls.

Service availability attacks such as DoS and virus attacks are viewed as the most significant VoIP security threats due to the possibility of lost revenues, system downtime, lost productivity and unplanned maintenance costs. Furthermore, such attacks are a major concern for enterprises and service providers providing public services such E-911, as even the smallest disruption could have significant or even catastrophic consequences.

Service Integrity

Threats to VoIP service integrity are those based on malicious activities which focus on compromising the network through toll fraud, identity theft and fraud attacks. Understandably, threats which compromise service integrity are of concern to service providers who may face consequences such as lost revenues and inaccurate billing.

A common scenario where service integrity is compromised involves a hacker using a VoIP phone which is connected to the network, and they gain access using a stolen or guessed user account and password to place phone calls at the victim's expense. There is also the potential for VoIP conversations to be hijacked and callers to be misled into communicating with the attacker, masquerading as a party to this call.

In addition to the possible attacks outlined above, VoIP services are offered with many features such call ID, call forward, voicemail, three-way calling, etc., which could potentially be used for toll fraud, identity theft and spam. For example, an individual could intentionally present a false identity in the form of false caller ID, voicemail or phone number. This type of misrepresentation is a common element of such attacks as phishing and SPIT.

Eavesdropping

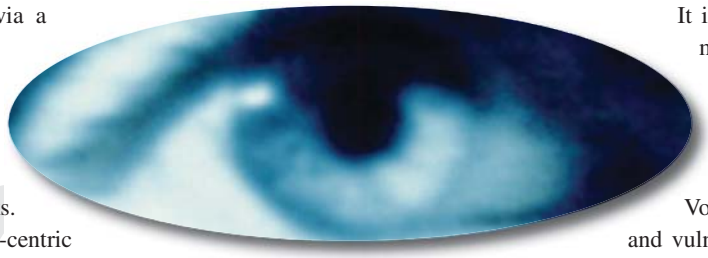
Eavesdropping on signaling and media paths allows the attacker to use Session Initiation Protocol (SIP) messages and Real Time Protocol (RTP) packets to obtain sensitive business or personal information. It also creates the possibility of various man-in-the-middle attacks where content of the conversation is altered. Privacy and confidentiality threats such as call eavesdropping, insertion and disruption, masquerading, registration hijacking, impersonation and replay are a major concern to the governments and financial institutions.

An example of an eavesdropping threat is a conversation reconstruction that involves collection of VoIP information included into packets

and then the translation of this information into plain speech. In this scenario important and confidential calls, such as those related to national security or financial information, could be intercepted and provide third parties with confidential information.

RECOMMENDATIONS FOR SECURING VOIP

The complex nature of VoIP infrastructure demands a unique approach to security. As we've established, VoIP networks consist 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 which operate across multiple layers of the network. As a result, a systems-level approach is required, where security is built into all the infrastructure layers and coordinated via a centralized control center.



With unique challenges and types of attacks, VoIP clearly requires a more sophisticated approach to security than those used to secure existing data networks. Solutions based simply on network-centric devices and signature-specific applications simply cannot address the real-time nature or complexity of VoIP infrastructure. The reality is that to maintain the integrity and reliability of VoIP services, organizations cannot rely on human-intervention to address security issues.

A system-based approach that combines network and host-based security devices and applications with a sophisticated, system level threat mitigation system is required to efficiently protect the entire VoIP infrastructure. In building a systems-level approach to VoIP security, unified VoIP-specific security consists of three functional components: prevention, protection and mitigation.

PREVENTION

Prevention enables organizations to proactively identify and fix VoIP-specific vulnerabilities before they impact 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 as interactions and dependencies between VoIP applications and devices could potentially create additional security vulnerabilities not visible during earlier assessments in the lab. Once VoIP is deployed, periodic or continuous vulnerability assessments should become the 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 any 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 service quality and reliability. Multi-layer security infrastructure that provides both perimeter as well as internal network protection is ideal. In most cases, it will consist of a number of security devices and host-based applications to protect VoIP networks such as Session Border Controllers (SBCs), VoIP Network Intrusion Prevention Systems (NIPS), VoIP DoS defenses, VoIP Network IDS, Host IPSs, Authentication, 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 a unified view of the end-to-end VoIP infrastructure.

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 the defenses and impact VoIP infrastructure. VoIP security and vulnerabilities are starting to emerge, and as VoIP becomes more mainstream, the number will continue to increase in the coming months and years.

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% availability (five minutes of downtime per year). Expect to see solutions emerge that are designed to provide real-time, automated VoIP security mitigation solutions to keep 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 networks present a unique challenge for network support and security professionals. There's an overwhelming need to understand the fundamental differences between traditional data and VoIP networks, as well as the possible types of attacks. In planning VoIP deployments, organizations must take a proactive, systems-level approach which will enable them to immediately protect against possible attacks and evolve to meet new and emerging VoIP security requirements. In sum, proactive security is the cornerstone of any successful VoIP deployment and with the right approach organizations will be able to reap the financial and business benefits of making the move to VoIP.

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