Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 21 – 29 ISSN 1896-7094

Securing Voice over Internet Protocol

Ahmad Ghafarian, Randolph Draughorne, Steven Grainger,
Shelly Hargraves, Stacy High, and Crystal Jackson

North Georgia College & State University
Dahlonega, GA 30005
aghafarian@yahoo.com, electronchaser6@earthlink.net
steven.grainger@verizon.net, shellzz@cox.net
stacy.high-brinkley@ngc.com, crystalejackson@hotmail.com

Abstract. In recent years, there has been significant increase in VoIP and internet telephony usage. The users, whether corporate or individuals are subject to the same security risks that have affected data networks for many years. This is mainly because voice networks are IP-based and all IP protocols for sending voice traffic contain flaws. In this paper, we study the security risks associated with the VoIP including vulnerabilities, man-in-the-middle attack, and denial-of-service. We will also review the protection measure that can be taken to make VoIP more secure, such as authorization, authentication, transport layer security, and media encryption.

Keywords: VoIP, Security, IPSec, Security Levels, Media Gateway Control Protocol

1 Introduction

Voice over Internet Protocol (VoIP) is a technology that has reached a level of maturity and reliability such that it can now be applied to the enterprise environment. VoIP has the potential to reduce communications costs considerably and opens a new path in the development of new devices. However, like all technologies VoIP comes with a number of inherent risks that while serious can be managed provided the enterprise takes the appropriate precautions.

This paper will examine the risks faced by the VoIP service provider and describe methods to reduce the risk for both the service provider and the enterprise. In addition, we examine the security risks associated with VoIP and has organized these risks in several categories from a layered perspective: weaknesses related to IP, the combined use of legacy and new technology, gateway considerations, security levels associated with VoIP, service provider challenges.

2 Internet Protocol Weaknesses

2.1 Resource Exhaustion (Denial of Service)

Resource Exhaustion, carried out via DoS (Denial of Service) attacks which reduces the number of available IP addresses, bandwidth, processor memory, and other router/server functions. A VoIP based DoS attack bombards a call processing/managing application with large amounts of simultaneous requests that it cannot process, causing the application to shut down, thereby denying service to authorized or intended users.

Before describing how to safely secure a VoIP network, its weaknesses must first be understood. VoIP is carried across the backbone of the Internet using Internet Protocol (IP) addresses to locate customers operating on the voice communications network [4]. However, IP has its own flaws, which are then inherited by all VoIP networks.

2.2 Network Sniffing

Network Sniffing attacks occur when an individual is observing network traffic. Typically, any system on a network sharing a transmission medium has the ability to view other system traffic (Univ. of London Information Security Group, 1998, pp.6-7).

2.3 Message Replay Attacks

According to the University of London Information Security Group [12], this type of attack occurs when network sniffing is done between two systems. Recording of the conversation is done during the sniffing which may be replayed to other parties in an altered state.

3 VoIP Security Levels

As illustrated in Figure 1 (see Appendix A), VoIP security can be divided into four levels: configuration security, signaling packet security, voice packet security, and data packet security [6]. The details of each level are described in the following subsections.

3.1 VoIP Configuration Security Level

The goals of VoIP security include authorization, authentication, integrity, privacy, and non-repudiation. Authorization is achieved through proper configuration, which is established during set-up of a new subscriber [10] by authorizing the device in the network system. Authentication can also be done either during configuration or at a later stage. Once the device is authorized to the network, the customer premise

equipment (CPE) must provide a secure identification number to the network server. An authentication key is then exchanged between CPE and the network server. The CPE gateway is authenticated, and then the server provides an encryption key. The encryption key is used for secure communication between CPE and the network server. Popular protocols that are used for this handshake and secure communication include: Session Security Layer (SSL), Transport Layer Security (TLS), File Transfer Protocol (FTP), Trivial FTP (TFTP), and Secure Hyper Text Transport Protocol (SHTTP). Configuration security protocols and methods of implementation are usually provided by individual service providers.

During the configuration of VoIP, separation of voice and data traffic is placed into different LAN segments. This process involves the creation of a separate VLAN for Voice and another VLAN for Data. The advantage of the separate VLANs is the isolation of the voice signals from data signals as they travel across the network.

Another security measure that must be taken into consideration during configuration is the creation of Security Association (SA). SA is a virtual secure connection between two or more devices. The SA process involves authentication and exchange of tokens, or certificate, to produce encryption keys. Once the SA is established, a security mechanism will perform key exchange. In addition to the establishment of a SA between a CPE and a configuration server, each pair of CPE also needs a SA. The reason SA establishment is recommended during the configuration stage is because it is a time consuming process to be established during the signal packet transmission. Since pre-establishment of SA between all CPEs is difficult to manage in terms of CPU usage, they are generally established as needed. It is also possible to reuse a previously established SA between two CPEs. Establishing a SA with IPSec requires between 2 to 10 seconds. However establishing SA with TLS requires 1.5 seconds [8].

3.2 VoIP Signal Packet Security Level

In VoIP, after the call is set, a complex series of packet exchanges must take place depending on a signaling protocol. The problem is that the computer systems are addressed by their IP addresses, but users enter an ordinary telephone number using the Universal Resource Indicator (ULI) to place a call. The first step in this process is converting analog voice signals to digital, using an analog-digital converter. Since digitized voice requires a large number of bits, a compression algorithm can be used to reduce the volume of data to be transmitted. This process is called signal pocketing. Next, the voice signals are inserted into data packets and hence voice packets are constructed [8].

The signal packet security set-up is engaged in the authentication process, which identifies one or more parties in a SA. The SA is not established on a per-call basis. This is because setting up signal security for each call would cause unwanted delays and latencies in the placing of VoIP calls. At the signal layer, the authorization/encryption process begins with an exchange of the keys generated at the configuration level or a new signal security key can be generated and exchanged independently. During earlier security implementation of VoIP, IP Security (IPSec) and Internet Key Exchange (IKE) protocols were used at the transport layer. Once the transport layer is secured, the signal layer and voice layer can run on top of the transport layer. Due to performance considerations, this approach has been changed

and currently the Transport Layer Security (TLS) protocol largely is deployed on top of TCP for signal security.

TLS is an advanced version of SSL and is used for privacy of the communications for VoIP users. TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption methods, such as the Data Encryption Standard (DES). The TLS Handshake Protocol allows the server and CPE to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. It is also more efficient, reducing the computational and consequent processing burden that other protocols generate.

Recently, Internet Engineering Task Force (IETF) proposed the use of TLS over Stream Control Transmission Protocol (SCTP) or User Datagram Protocol (UDP). Although SCTP has open stream sockets at the transport layer and provides a rich set of features, such as good reliability and multiplexing, it may be too ponderous and code-intensive for VoIP applications that require greater agility. TLS over UDP is not gaining market attention since SIP clients only need to support SIP over TCP; support for UDP is optional.

3.3. Voice Packet Security Level

The latest standard voice encryption standard is the Secure Real-Time Transport Protocol (SRTP) with advanced encryption standard (AES). SRTP provides message confidentiality, authentication, integrity checking, and replay protection for voice packets on a per-packet basis. Initially, the data, minus the header information, is encrypted using AES and then a hash of the header and encrypted data is created using Keyed-Hashing for Message Authentication Secure Hash Algorithm-1 (HMAC-SHA1) [5].

SRTP+ [5] is presented as an approach to overcome the overhead problem and reduce an attacker's ability to exploit this vulnerability. The first two techniques center on mapping a pseudorandom number generator (PRNG) number with an authentication tag, creating a mapping pattern that must be known by both terminal nodes at the time the authentication tag for the outgoing packet is generated and also for verifying the tag of an incoming packet. Packets that are not authenticated are assumed to be malicious and are discarded.

A third technique eliminates the need for either a PRNG or a hashing function. In this technique the sender calculates in advance a series of random numbers and uses one of these numbers as the authentication tag for each packet. The receiver stores the N random numbers after decrypting the payload. These random numbers correspond to the sequence numbers for the next N expected packets and are compared to the authentication tags for succeeding packets for authentication. Before the first packet can be authenticated, the first N random numbers must be sent to the receiver, possibly during the SRTP key exchange. Figure 4 illustrates this technique (see Appendix A) [5].

3.4 Data Packet Security Level

Data packets in a VoIP implementation may be protected at the IP level using the Internet Protocol Security (IPSec). IPSec uses two protocols, the a uthentication header (AH) protocol and the e ncapsulating security payload (ESP), to provide integrity, confidentiality and authentication of data communications over IP networks [2]. In conjunction with an arbitrary 32-bit security parameter index (SPI) and the destination IP address, the protocol uniquely identifies the SA for the specified header field of each data packet or the entire data packet depending on the operational mode. Although these mechanisms validate the authenticity and integrity of the packet, the data itself is not encrypted so the data can still be viewed by unintended parties.

The sequence number field of the header in used to prevent replay attacks and is required to be sent by the origin host but not necessarily processed by the destination host. The sender's counter and the receiver's counter are initialized to "0" at SA and incremented with the first packet sent using a particular SA, i.e. a sequence number (SN) of "1". The transmitted SN must never be allowed to "replay"; hence, anti-replay must always be enabled by the origin host.

The header fields associated with security are not significantly different between AH and ESP but since ESP supports encryption, an initialization vector (IV) [2] field is included to account for encryption algorithms that require cryptographic synchronization data. I PSec supports two encryption modes [2]: Transport and Tunnel. Transport mode encrypts only the data portion of each packet while the tunnel mode encrypts both the header and the payload by encapsulating the original packet in a new packet masking of the source and destination IP addresses.

Key management is critical and IPSec supports both the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley protocols [1] . These protocols use two phases of negotiations to establish an SA prior to data transmission.

4 VoIP Solutions

IP weaknesses are not the only security issues to consider. Since VoIP is a relatively new technology, companies are currently in the process of implementing it. One common method is by using a hybrid approach combining older circuit-switched technology with new VoIP technology.

4.1 Circuit-switched Technology Vulnerabilities

- Toll Fraud is a classic IP attack where the attacker impersonates an employee or performs Console Cracking (asking the operator for an outside trunk) to make long distance calls. However, the attacker impersonates a valid user and IP address by plugging in their phone or spoofing the MAC Ethernet address.
- Eavesdropping occurs when an attacker intercept voice messages. This allows the attacker to listen to voice conversation at ease without the target knowing. Easily available programs such as VOMIT (Voice over Misconfigured Internet Telephony) perform this function.

- Call Hijacking is when an attacker a SIP Response and redirects a caller to a rogue SIP address. This allows the attacker to intercept the call.

4.2 VoIP Technology Vulnerabilities

- IP Phone – "The IP Phone is a new desktop phone configured and equipped specifically for IP-based phone calls" (ISS, 2004, p.4). Working much like a regular landline phone, the IP Phone's Operating System (OS) may support a web browser; the user can access the phone's webpage and attempt to modify phone features and options [3].
- PC-Based Phone – According to [7] (ISS), PC-based phones utilize a software application that provides the phone with IP capabilities when using a PC. However, since the phone can only be used in conjunction with a PC, it is as vulnerable as the OS and applications installed on the computer.

5 VoIP Gateway Vulnerabilities

VoIP gateway technologies are also a potential weak point. When VoIP is used externally, gateway technologies convert data packets from the IP network into voice before sending them over a public switched telephone network. When VoIP is used internally, the gateways route packetized voice data between the source and the destination. The concern here is that such gateways can be hacked into by malicious attackers in order to make free telephone calls. The trick to protecting against this lies in having strict access-control lists.

As with traditional telephony, eavesdropping is a concern for organizations using VoIP; and the consequences can be greater. Because voice travels in packets over the data network, hackers can use data-sniffing and other hacking tools to identify, modify, store and play back voice traffic traversing the network. A hacker breaking into a VoIP data stream has access to a lot more calls than he would with traditional telephone tapping. As a result, "one of the big differences is that a hacker has a much higher probability of getting intelligent information" from tapping a VoIP data stream than from monitoring traditional phone systems [13].

6 VoIP Security Challenges for Service Providers

According to Verizon Business [9] the issues repeatedly seen by their security services assessment group falls into a number of categories they see repeatedly when assesses existing enterprise VoIP systems:

- The enterprise is not using a VPN to gain access to a VoIP environment
- There is poor support for access controls and passwords
- There is widespread use of unauthorized devices such as personal soft phones in enterprise networks and thereby thwart firewall rules.

The major security challenge for service providers can be viewed in terms of creating a way to transport VoIP packets safely across the provider's infrastructure.

Service provides need to insure a secure solution to transit the VoIP data across their network and deliver it to the customer interface. The CPE is often an enterprise border firewall, whose configuration rule set is a sensitive issue because it is the first line of defense in a corporate security system. Making this issue even more complex is the large number of competing VoIP protocols both standards based and proprietary.

Mandating specific IP phones is not practical because it limits choices available to the customer community and IP phone technology is moving rapidly. Another problem with IP phones is the ability to support a direct connection to the customer's site reveals a matter of IP destination address exposure.

Therefore, it can be seen that the principle issue that service providers need to address is the ability to securely transit VoIP traffic across their network, deliver it to the CPE, and insure that the VoIP traffic is not compromised as it transits the service provider's network. Service providers need a solution set that solves the fundamental problems associated with VoIP. Service provider must also insure they have the proper network infrastructure to accommodate these advances and deliver VoIP traffic safely across their infrastructure.

6 Mechanisms for Securing VoIP

Because of the time-critical nature of VoIP, and its low tolerance for disruption and packet loss, many security measures implemented in traditional data networks are simply not applicable to VoIP in their current form; firewalls, intrusion detection systems, and other components must be specialized for VoIP.

Firewalls, gateways, and other such devices help keep intruders from compromising a network. However, another layer of defense is necessary at the protocol level to protect the voice traffic. In VoIP, as in data networks, this can be accomplished by encrypting the packets at the IP level using IPSec, or at the application level with SRTP. This way if anyone on the network, authorized or not, intercepts VoIP traffic not intended for them (for instance via a packet sniffer), the packets will be unintelligible.

To implement VoIP securely, start with the following general guidelines, recognizing that practical considerations might require modification and adjustment:

- Put voice and data on logically separate networks.
- At the voice gateway, which interfaces with the PSTN, deny access to H.323, SIP, or Media Gateway Control Protocol (MGCP) connections from the data network.
- As with any other critical network management component, use strong authentication and access control on the voice gateway system.
- Choose a mechanism to allow VoIP traffic through firewalls. Various protocol dependent and independent solutions exist, including ALGs for VoIP protocols and session border controllers. Stateful packet filters can track a connection's state, denying packets that aren't part of a properly originated call.
- Use IPSec or Secure Socket Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

- Use IPSec in tunnel mode when available instead of in transport mode because tunneling masks the source and destination IP addresses, securing communications against rudimentary traffic analysis.

7 Conclusion

This paper has addressed VoIP security in terms of its configuration, risks, and potential usage by service providers who need to manage those risks. While VoIP is certainly a viable technology great care must be taken in its use and configuration. A number of VoIP specific recommendations conclude the paper.

However, beyond these specific recommendations, an enterprise must use a layered security architecture, which provides the most effective defense against VoIP attacks. Defensive layering must start beyond the enterprise border and originate in the service providers network to insure the secure transport of VoIP to the enterprise. Enterprises must continue to review their security posture in terms of risk mitigation, not risk avoidance because new technology and vulnerabilities will always arise alongside the new technology, like VoIP.

References

1. Barbieri R., Bruschi D., Rosti E. (2002). *Voice over IPsec: Analysis and solutions.* 8 th Annual Computer Security Applications Conference. pp. 261.
2. Berger T. (2006). *Analysis of current VPN technologies.* First International Conference on Availability, Reliability, and Security. Pp. 108-115.
3. Bednarz P. (2002). *How VoIP is changing the network security equation.* Retrieved October 16, 2006 from `http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=16505939`
4. Casteel J. (2005). *Sound Choices for VoIP Security* . Retrieved October 20, 2006 from `http://www.ebcvg.com/pdf/dl/sound_choices_voip_security.pdf`
5. Garg S., Singh N., Tsai T. (2005). *SRTP+: An efficient scheme for RTP packet authentication.* Retrieved Nov. 2, 2006 from `http://pubs.research.avayalabs.com/pdfs/ALR-2004-001-paper.pdf`
6. Greenstreet D., Scoggins S. (2005). *Building Residential VoIP Gateways: A Tutorial* Part IV: VoIP Security Implementation. Retrieved Oct. 23, 2006 from: `http://www.analogzone.com/nett0913.pdf`
7. Internet Security Systems (2004). Retrieved October 16, 2006 from `http://www.iss.net/documents/whitepapers/ISS_VoIP_White_paper.pdf`
8. Kuhn R., Walsh T. J. and Fries Stephen, (January 2005). *Security Considerations for Voice over IP Systems.* National Institute and Standards and Technology Publications. Retrieved, Oct. 21, 2006 from: `http://www.arcert.gov.ar/webs/textos/SP800-58-final.pdf`
9. Marsan C. (2006). *VoIP Security Services Taking Hold.* Network World, Vol. 23, Iss. 26, pg. 25, July 2006.

10. Scoggins S, *Implement Maximum Security for VoIP.* Reprieved October 25, 2006 from
http://www.eetasia.com/ARTICLES/2006APR/PDF/EEOL_2006APR03_RFD_NETD_SECD_TA.pdf
11. The Internet Society. (2004). *Request for comments: 3711 The secure real-time transport protocol (SRTP).* Retrieved October 31, 2006 from: http://www.ietf.org/rfc/rfc3711.txt
12. University of London Information Security Group (1998). Internet Protocol Security Flaws.
13. Vijayan, J. (2002) *VOIP: Don't Overlook Security.* Computerworld, Security.

Appendix A: Figures

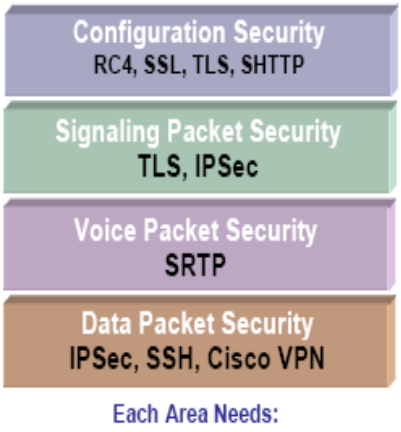

Fig. 1. VoIP Security Area

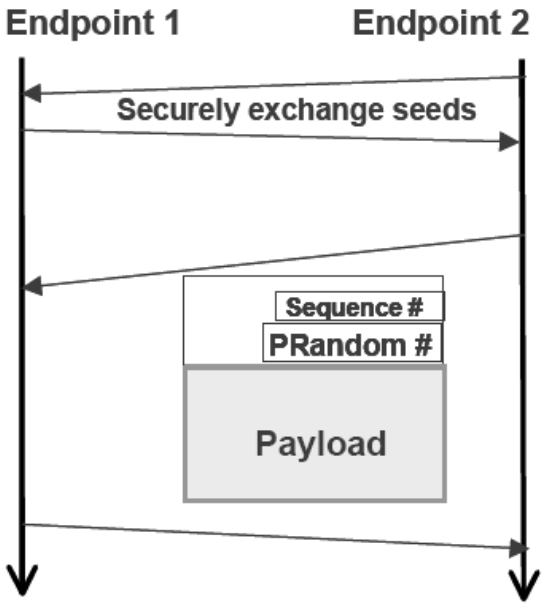

Fig. 2. SRTP+ Exchange for Technique 1

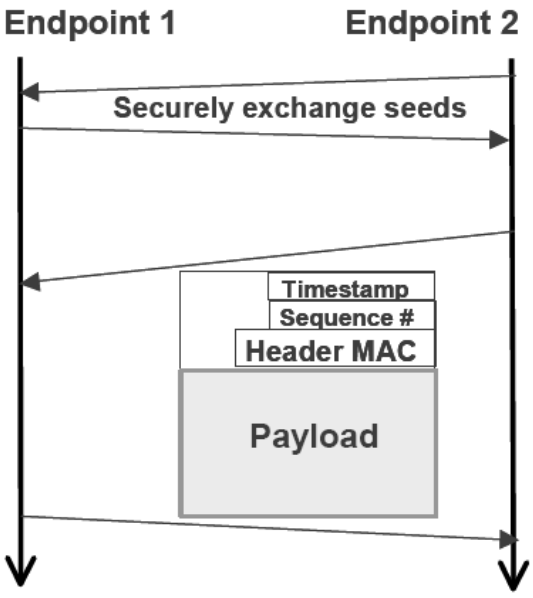

Fig. 3. SRTP+ Exchange for Technique 2

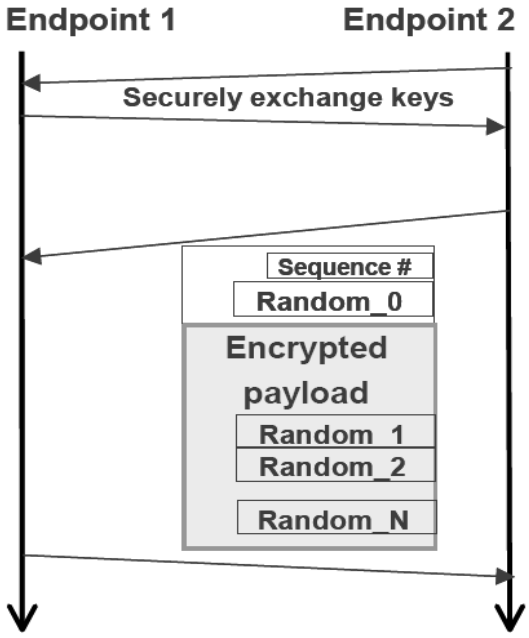

Fig. 4. SRTP+ Exchange for Technique 3