VoIP security - attacks and solutions

Journal Item

VoIP Security - Attacks and Solutions

Santi Phithakkitnukoon, Ram Dantu, and Enkh-Amgalan Baatarjav

Dept. of Computer Science & Engineering, University of North Texas, Denton, TX, 76203 USA

{santi, rdantu, eb0050}@unt.edu

Abstract

Voice over IP (VoIP) technology is being extensively and rapidly deployed. The flexibility and cost efficiency are the key factors luring enterprises to transition to VoIP. Some security problems may surface with the widespread deployment of VoIP. This article presents an overview of VoIP systems and its security issues. First, we briefly describe basic VoIP architecture and its fundamental differences compared to PSTN. Next, basic VoIP protocols used for signaling and media transport, as well as defense mechanisms are described. Finally, current and potential VoIP attacks along with the approaches that have been adopted to counter the attacks are discussed.

1. Introduction

VoIP (Voice over Internet Protocol) has fast emerged as a standard for voice communication using the Internet. As VoIP uses the existing IP network, it dramatically reduces cost of communication typically with traditional PSTN (Public Switched Telephone Network). In addition, ease of deployment and reduced communication hardware make VoIP a compelling solution for voice communication on the Internet. Further, VoIP provides a flexibility of value-added and personalized services for defining customized solutions. As a result, most of the control which existed in PSTN's central infrastructure has been transferred to the end devices by deploying the VoIP communication infrastructure.

With the advent of VoIP technology, an increasing number of telecommunication service providers have stated to integrate VoIP solutions into their systems and provide VoIP services to their

customer base. Equipment manufacturers and end users have greatly benefited from performance advancements, cost reduction, and feature support provided by the VoIP technology.

VoIP is a technology for transmitting voice packets on the existing IP network. Unlike PSTN, an IP network is packet switched. In PSTN, when a phone call between two parties is initiated, there exists a physical circuit connecting the two parties. After the call is established, the parties communicate and the circuit is reserved until the parties finish the communication. In contrast, on an IP network, all communication is carried out using IP packets. When a calling party communicates with a called party, the analog signals are digitized, encoded, and packed into an IP packet at the transmitting end and converted back to analog signals at the receiving end.

VoIP is adding a third dimension to voice communication with the PSTN and cellular networks being the other two. A call can be made to any PSTN phone and mobile phone anywhere in the world using VoIP. Although certain services can only function on computer or a special VoIP phone; others allow a caller to use a traditional phone with an adapter. VoIP promises to enable migration of the existing circuit-switched, public switching telecom network to a packet-switched network. With VoIP, widespread acceptance by telecommunication markets of all sizes, advanced features have started emerging. However, the convergence of the voice and data worlds introduces not just opportunities but also security risks. The much lower cost and greater flexibility are key factors luring enterprises to transition to VoIP. VoIP should not, however, be installed without careful consideration of the security problems it can introduce.

Security issues in VoIP are unique and, in most cases, quit complex. This article aims to provide an overview of VoIP security issues including basic VoIP architecture, existing defense mechanisms, and current attacks, as well as an outlook on potential attacks such as SPIT and their possible solutions.

To facilitate the ensuing discussion, we briefly describe the basic VoIP network architecture. The VoIP infrastructure can be visualized as three layers; end user equipment, network components, and a gateway to the traditional phone network (see Fig. 1). We define each of these layers as follows.

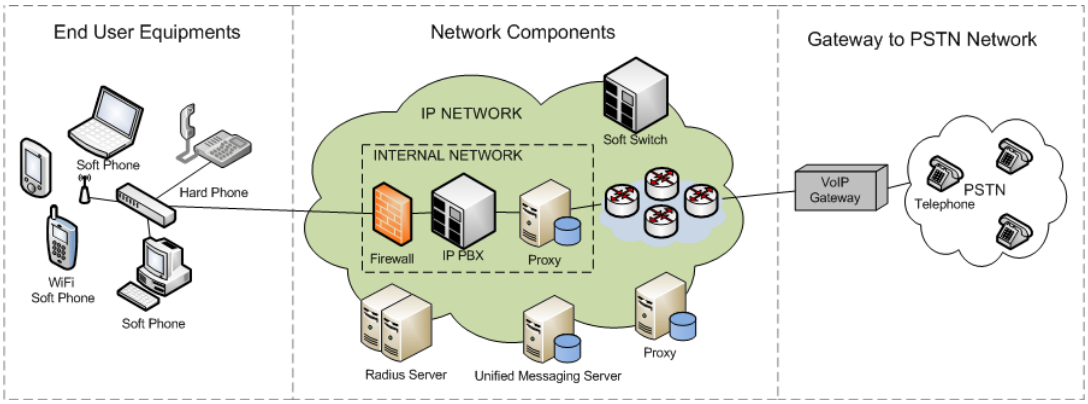

Fig. 1 VoIP network.

1. End-user equipment: The end-user equipment provides an interface for users to communicate with other end users. Equipment could be "hard phones" with an interface similar to a conventional telephone or a "soft phone," software that emulates a telephone. The security of such end-user components depends upon how they are installed. Mostly, this end-user equipment often deployed in campus networks, at home, or in hotels. Rarely, however, does the equipment have security features built-in, making them vulnerable to exploitable flaws.

2. Network components: VoIP normally uses the existing IP network and thus inherits its vulnerabilities. Each network component has its own security concerns which have surfaced over the past few years (e.g. Goodin, 2008; Chou, 2007). Adding voice traffic to these components increases their list of vulnerabilities. The IP network components, including routers, switches, and firewalls, must also be VoIP-aware to provide security features specified to VoIP.

3. VoIP gateways: Gateway plays an important role in integrating the IP network with the PSTN and thus, care should be taken to ensure that its security policies do not introduce vulnerabilities. The primary functions of a VoIP gateway include voice compression or depression, signaling control, call

routing, and packetization. VoIP gateways interface with external controllers such as SIP proxies, H434 Gatekeepers, Media Gateway Controllers (MGC), network management systems, and billing systems. These interfaces can be a potential weakness because malicious attackers can exploit them to make free telephone calls. Any security framework must counter these attacks quickly and efficiently.

The rest of the article is structured as follows. Section 2 describes basic signaling and transport protocols used in VoIP network. Section 3 presents defense mechanisms in signaling and transport, and key management. The current and future VoIP attacks and possible solutions are discussed in Section 4. Finally, this article is summarized and concluded in Section 5.

2. VoIP Protocols

In order to communicate on the phone, a call must be initiated. Placing a phone call in a traditional phone system involves dialing a sequence of digits, which are then processed by the telephone company to ring the called party and form a connection when the call is answered. With VoIP, the user enters the calling number, which can be either a number on a telephone keypad or the Universal Resource Indicator (URI), and after that a sequence of packet exchange will occur based on VoIP "signaling protocol". Once the called party answers, voice signal is digitized and segmented into a stream of packets for transmitting based on "transport protocol".

2.1 Signaling Protocols

Current VoIP systems use either a proprietary protocol, or one of two standards, H.323 and the Session Initiation Protocol (SIP). Although SIP seems to be gaining in popularity, neither of these protocols has become dominant in the market yet, so it is essential to understand both protocols.

2.1.1 H.323

H.323 is a set of protocols recommended by the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) and consists of family of protocols that are used for

call setup, call termination, registration, authentication, and other functions (International Telecommunication Union, 2000). H.323 is widely adopted in the enterprise environment because it is a binary protocol which can be easily integrated with PSTN. An H.323 network consists of several components including Gatekeeper, Gateway, Multipoint Control Unit (MCU), and Back End Service (BES).

2.1.2 SIP

The session Initiation Protocol (SIP) (Rosenberg, Schulzrinne, Camarillo, Johnson, Peterson, Sparks, Hardley, & Schooler, 2002) is the Internet Engineering Task Force (IETF) specified protocol for creating, modifying, and terminating unicast or multicast sessions. SIP is a text-based protocol and can transfer different types of payload with different encodings. SIP supports both UDP and TCP as transports. The architecture of a SIP network is different from the H.323 structure. A SIP network is composed of Endpoints, Proxy servers, Location servers, and Registrar.

2.2 Transport Protocols

The majority of the VoIP deployments use RTP for actual media (e.g. voice or video) transport. The RTP is specified by IETF in RFC 3550 (Schulzrinne, Casner, & Jabobson, 2003) and RFC 3551 (Schulzrinne, & Casner 2003). It is a simple protocol that runs on top of UDP and therefore has “best effort” delivery but does not assure delivery of the packets since real-time properties of the streams are more important than reliability of transport (i.e. having to repeat a speech is better than having a long delay in phone conversations). The quality and fault tolerance of the media stream is defined by the actual media codec where different error-correction algorithms can fix the problems created by packet loss. The compression rate and quality of the codec determine the bandwidth requirement. The Real-time Transport Control Protocol (RTCP) is used together with RTP, but it is not required for RTP streams to work. The RTCP is primary used for collecting data on the efficiency and quality of the

connection. The RTCP messages travel on the same route as RTP and report information such as latency, jitter, and packet loss. The RTCP messages are typically collected and responded by the media gateway.

3. Defense Mechanisms

The basic protocols used in VoIP have been described in the previous section. The focus of this section is on analyzing protection mechanisms associated with VoIP protocols along with their strengths and weaknesses.

3.1 Signaling Defense Mechanisms

This section describes protection mechanisms associated with signaling protocols including H.235, S/MIME, and IPSec.

3.1.1 H.235

The H.235 is a security framework that provides authentication, confidentiality, and integrity, along with interfacing with key exchange protocols to support distributed communications for H.323 based systems. Several messages, procedures, structures, and algorithms are recommended by H.235 for the security concerns of signaling, control, and media communications under H.323 architecture. A typical H.323 setup using H.235 takes approximately 300 to 400 ms depending on the implementation.

H.235 provides end-to-end security and supports multicast and unicast security, however it does not scale well for Internet communications and it also requires greater level of implementation complexity compared to SIP.

3.1.2 S/MIME

RFC 3851 (Ramsdell, 2004) defines the Secure/Multipurpose Internet Mail Extensions (S/MIME) which can provide end-to-end confidentiality, integrity, and authentication for application protocols such as

SMTP and SIP. An S/MIME message is based on MINE, which defines a set of mechanisms to encode and represent complex message formats such as multimedia contents (e.g. audio, video) and foreign characters (e.g. Chinese, Greek) within other protocols such as SMTP or SIP. In addition to MINE functionality, S/MINE incorporates Public Key Cryptography Standards (PKCS) to maintain its security.

The S/MIME provides confidentiality for the data in SDP, integrity of information within the SDP portion of the SIP message, and authentication of sender. Although, S/MIME provides great flexibility and end-to-end confidentiality, integrity, and authentication, it requires more effort to implement due to its complexity and infrastructure requirements (e.g. PKI).

3.1.3 IPSec

Security architecture for the Internet Protocol (IPSec) (Kent & Atkinson, 1998) provides protection to applications that transport using UDP or TCP. Due to the extensive coverage of IPSec, this section only focuses on its impact on SIP.

IPSec provides confidentiality, integrity, and authentication for signaling and media streams by creating secure tunnels between end points. With SIP, if a call is to established between two endpoints and a IPSec tunnel is created for each communication link (caller-and-caller's proxy, caller's proxy-and-callee's proxy, and callee's proxy-and-callee), there will be three IPSec tunnels which will take about 20 seconds of call setup time where media stream link (RTP) will take about 10 seconds for setup (Thermos & Takanen, 2008). If the IPSec associations have been established, there is almost no delay in routing signaling messages.

Although, IPSec provides a secure channel that can support UDP, TCP, SIP, and RTP, its infrastructure requirement must be carefully considered for appropriate situations (e.g. an extremely secretly phone call may find IPSec a great option where 20 seconds of call setup time is necessary).

3.2 Transport Defense Mechanisms

This section discusses protection mechanisms associated with transport protocols including SRTP, and SRTCP.

3.2.1 SRTP

The Secure Real Time Protocol (SRTP) is a profile for the RTP defined by RFC 3711 (Baugher, McGrew, Naslund, Carrara, & Norrman, 2004) to provide confidentiality, integrity, and authentication of the message payload of media streams (voice and video). SRTP provides protection for both RTP packets and RTCP messages. As discussed previously that RTCP is used primarily to provide QoS feedback to the endpoints of a session. RTCP messages are transferred separately from the RTP messages, thus both RTP and RTCP need to be protected during a multimedia session. By using a native key derivation algorithm (Menezes, Van Oorschot, & Vanstone, 1997), SRTP is able to minimize computation and resource consumption for generating cryptographic keys through an external key management mechanism.

Although SRTP can provide confidentiality, integrity, and authentication for media content, it cannot maintain end-to-end message integrity and authentication for the media stream transmitted from an IP network to PSTN.

3.2.2 SRTCP

The format of SRTCP packet is similar to SRTP with two additional headers; SRTCP index and encrypt-flag for authentication. In an RTCP message, the originating party and the contents of the report are sensitive information which needs to be protected. Therefore these headers are encrypted.

3.3 Key Management Mechanisms

Key management is an essential element of protecting Internet multimedia applications such as VoIP. Key negotiation protocol is required for the multimedia communications such as VoIP that can provide

robust and extensible capabilities for multicast as well as unicast communications. Currently, there are several existing and emerging key management standards. As MIKEY and ZRPT are currently gaining population in VoIP environments, this section focuses on these two key management protocols.

3.3.1 MIKEY

Multimedia Internet KEYing (MIKEY) is a key management protocol which was designed for real-time applications. MIKEY is defined in RFC 3830 (Arkko, Carrara, Lindholm, Naslund, & Norrman, 2004) and used to support SRTP. MIKEY endures the negotiation of cryptographic keys and security parameters for one or more security protocols. It also provides independency of a specific communication protocol such as SIP and H.323. The 2-way handshake fashion for initiating key material of MIKEY makes it suitable for real-time multimedia scenarios.

3.3.2 ZRTP

ZRTP (Ziemmermann, 2008) is another cryptographic key agreement protocol that can be used to support secured RTP. The negotiation of the cryptographic key using RTP instead of signaling route is the main difference between ZRTP and MIKEY, such that the key negotiation is performed between endpoints directly without engaging intermediate terminals such as SIP proxies to pass along the keying components.

ZRTP has an edge on MIKEY as it provides independency of signaling protocols therefore only the endpoint software is required for the change but not the core VoIP elements (e.g., SIP proxy or an H.323 gatekeeper). However, one limitation that both protocols suffer is that they cannot support the calls that are transmitted between VoIP network and PSTN.

4. VoIP Attacks and Solutions

Attackers typically target the most popular and well-publicized systems and applications. VoIP has become one of such application. Several VoIP weaknesses have been revealed recently, thus protocol

designers need to address it before successfully deploying VoIP on the global scale. In this section, we present a study of attacks on the VoIP infrastructure. We classify the attacks into five primary types, including: Denial of service (DoS), Eavesdropping, Masquerading, Toll Fraud, and Spam over Internet Telephony (SPIT). Furthermore, we discuss approaches that have been adopted to counter the attacks.

4.1 DoS

DoS attacks pose perhaps the greatest threat to enterprise VoIP systems. DoS attack is ranked first in the top five VoIP security threats of 2008 (Higdon, 2008). DoS attacks can be directly toward any network element to disrupt the system's functionality or the networking capabilities of the corresponding component such as user's devices, signaling components, media components, management systems, billing systems, and security systems.

4.1.1 DoS Attacks Reported

There has been a report that certain VoIP phones are susceptible to both DoS attacks and communication interception vulnerabilities, and certain VoIP routers are also vulnerable to malicious traffic (Leyden, 2004). In addition, an open-source IP PBX and an open-source VoIP client have been reported to have vulnerabilities that can allow hackers to compromise VoIP networks with DoS attacks (Network Computing, 2006). National Cyber-Alert System (2005) has reported that another type of VPN Routers allows remote attackers to cause a DoS (crash) via an IPSec IKE packet with a malformed Internet Security Association and Key Management Protocol (ISAKMP). Another type of IP phones has also been reported that it is rendered unusable by bombarding them with specific IP traffic (Mier, Birdsall, & Thayer, 2004).

4.1.2 Proposed Solutions for DoS Attacks

Sisalem, Kuthan, & Ehlert (2006) recommended some countermeasures to handle DoS attacks in SIP VoIP systems including:

- Monitoring and filtering – to maintain lists of suspicious users and deny those users from establishing sessions.
- Authentication – to verify the identity of a user before forwarding his/her messages.
- Stateless proxy – to reduce the risk of memory exhaustion attacks (DoS) thus stateless proxy can be used to perform other security checks such as authenticating users, registering third party, and filtering spam sources.
- Server design (e.g. CPU, memory, and network connection) – to be the first line of defense against DoS attacks.

Sengar, Wijesekera, & Jajodia (2008) also proposed a technique to detect DoS attacks by using statistical approach based on abnormal variations in traffic flows measured by Hellinger distance.

4.2 Eavesdropping

Eavesdropping is the attempt to collect sensitive information to prepare for an attack or gain intelligence. In VoIP, this is a scenario where the attacker is able to monitor signaling or media contents exchanged between users in order to analyze communications to prepare for other future attacks.

4.2.1 Eavesdropping Attacks Reported

The Internet Security Systems' X-Force team discovered VoIP security flaws in a vender's call manager that would give an attacker the ability to eavesdrop or redirect calls, in addition to gaining unauthorized access to networks running the VoIP products (VoIP Magazine Editorial Staff, 2005). If attackers exploited the vulnerabilities, they could set off a heap overflow within the call manager, causing a DoS condition, and compromising the call manager.

4.2.2 Proposed Solutions for Eavesdropping Attacks

Long (2002) recommends four strategies to prevent eavesdropping:

- Employing flawless hardware.

- Ensuring that access to wiring closets is restricted to authorized personnel only.
- Implementing port based MAC address security on any vulnerable network point; for example, on a reception courtesy phone.
- Initiating a procedure to regularly scan the network for devices running in promiscuous mode.

Another solution is encryption of VoIP traffic, which is a good method for preventing eavesdropping, however it adds additional overhead.

4.3 Masquerading

Masquerading is the ability to impersonate a user, device, or service to gain access to a network, service, network element, or information. Masquerading attacks can be used to commit fraud, unauthorized access to sensitive information, and even service disruption. Perhaps the worst case is that the attackers pretends or takes over someone's identity in the service. Manipulating protocols that provide support for VoIP can also be realized as a masquerading attack in VoIP networks.

4.3.1 Masquerading Attacks Reported

There has been a report that a bank and on-line payment service were victims of attacks where the attacker called a credit-card customer and duped the customer into revealing account information by claiming there had been fraudulent activity on their accounts (Higgins, 2006).

4.3.2 Proposed Solutions for Masquerading Attacks

An effective authentication module combined with encryption would be an effective solution to masquerading and spoofing attacks.

4.4 Toll Fraud

Toll fraud is the ability to have unauthorized access to the VoIP services for personal or monetary gain. For telecommunication carriers and providers, this is one of the most critical attacks. Toll fraud can be

realized by manipulating the signaling messages or the configuration of VoIP components, including the billing systems.

4.4.1 Toll Fraud Attacks Reported

The financial implications of toll fraud are more profound than perceived by telephone subscribers. The Communications Fraud Control Association (CFCA) conducted world-wide survey (Communications Fraud Control Association, 2006) and estimated that telecommunication fraud losses range from US$54.4 to 60 billion (52% increase from 2003's CFCA Survey results). Fraud has been reported as the largest area of revenue leakage for telecommunication operators. According to the Telecomasia.net survey (Chau, 2007), the overall levels of revenue leakage among global telecommunication operators were increased from 12.1% in 2006 to 13.6% in 2007. In recent scam (Blackwell, 2006), a Spokane resident hacked into an unprotected corporate IP network and into the networks of several VoIP providers. Attacker routed traffic from the company's customer through the corporate network to the VoIP providers. The providers were left with the interconnect charges (as much as $300,000 per victim). A Miami service provider was reported to have hacked into other provider networks, routing his customers' calls onto their networks, and then billing his customers (Teal, 2006).

4.4.2 Proposed Solutions for Toll Fraud Attacks

VoIP providers can prevent toll fraud by properly configuring firewalls and by protecting ports. VoIP providers must also actively monitor their networks, so that they know who is accessing the network and with what frequency, and who is generating what kind of traffic.

4.5 SPIT

Due to its much lower communication costs, VoIP network has become more attractive as an alternative to the current PSTN as well as a target for spammers. VoIP spam or also known as Spam over Internet

Telephony (SPIT) is expected to be a serious problem for VoIP networks and even more severe than e-mail spam problem because of its attacking nature for which requires a real-time defense mechanism.

4.5.1 SPIT Reported

SPIT problem does not really exist in the current VoIP networks just yet. However, as VoIP community becomes larger, SPIT is expected to be one of the greatest threats. For current VoIP systems, SPIT are in forms of phishing (or also known as "Vishing" in VoIP networks) as can be seen in the following reports. Gonsalves (2006) reports an attack where a con artist sent VoIP spam disguised as if coming from a small bank and collected personal identification numbers. Ryst (2006) reports that an attacker sent e-mails that appeared to come from the account-validation team at an online-payment service. Unlike most phishing schemes that direct the recipient to a fraudulent web site, this scam instructed victims to call a phone number, where they are asked to divulge account information. A security vendor reports a worm that spreads through the chat feature of a popular VoIP service (Kirk, 2006). Users receive a message asking them to download a file call "sp.exe." The executable is a Trojan horse that can steal passwords. If a user runs the Trojan, it triggers another set of code to spread itself.

4.5.2 Proposed Solutions for SPIT

Despite inexistence of the problem, there has been an increasingly number of solutions proposed to combat the SPIT due to its potential threat. The overview of the SPIT problem are well provided by Rosenberg & Jenings (2007), Radermacher (2005), Niccolini (2006), and Baumann, Cavin, & Schmid (2006), who analyzed the problem and discussed various possible solutions to detect and mitigate VoIP spam.

Jenings (2007) suggested using cryptographic puzzles to detain spammers (especially DoS attackers) by increasing the cost of the request of the communication by requiring a suspicious caller who attempts to establish a connection to solve a small puzzle which is computational expensive. The

drawback of this solution is that the puzzle challenges may overwhelm a legitimate caller's slow machine which may cause undesirable delay.

Payment at risk (Abani, Burrows, Birrell, Dabek, & Wobber, 2003) is another idea to increase the cost of the communication by having a caller deposits some amount of money into callee's account in order to establish a call. This may reduce spam dramatically but it might as well reduce legitimate callers since the main advantage of VoIP network over the PSTN is cost.

Black and white lists have also been studied and utilized to reduce SPIT (e.g. Dantu & Kolan, 2005; Rohwer & Tolkmit, 2006; Schwartz & Sterman, 2005; and Sterman, 2005) where spam filter maintains two lists of addresses, white list for wanted callers and black list for unwanted callers or spammer. However, this approach may disable a legitimate caller who is not on the white list to make a call. In case that the black list is used alone, then spammer can easily reach the recipient by changing IP address.

Greylisting (e.g. Radermacher, 2005; and Shin & Shim, 2005) is also an effective technique to filter SPIT, however it only works well in the case that spammer does not change IP address and attempts to reestablish a call within a certain time period with a certain rate of calling. The cost of false negative can be too high caused by emergency calls from legitimate callers.

Reputation systems have also been applied to combat SPIT (e.g. Dantu et al., 2005; Hansen, Hansen, & Moller, 2006; and Balasubramaniyan, Ahamed, & Park, 2007). Dantu et al. (2005) proposed a multi-stage VoIP spam filter using reputation inference based on social networks (associated and trusted neighbors) from which the user was willing to receive calls. This approach needs high collaborative effort from several different domains and its high complexity of the filter may cause undesired delay in initiating connection. Hansen et al. (2006) utilized a reputation system by rating a call based on meta-data of the call such as caller identity and call origin. Balasubramaniyan et al. (2007)

also applied reputation mechanism by assigning credential value for each user to determine social network linkages to distinguish between legitimate users and spammers. However, these reputation approaches require high collaboration from proxy servers to maintain as well as exchange reputation or trustworthiness values between users.

There are also SPIT detection techniques proposed based on anomalous characteristics of the spam call (e.g. Shin et al., 2005; Vinokurov & MacIntosh, 2005; and Sengar, Wang, Wijesekera, & Jajodia, 2007). Vinokurov et al. (2005) proposed a technique to detect SPIT based on recognizing abnormalities in signaling message statistics. Shin et al. (2005) used graylisting technique to recognize abnormality of the call based on calling rate. Sengar et al. (2007) proposed the use of Hellinger distance to detect abnormalities of the call behavior to identify spam call. The drawback of the abnormality detection approach is that it requires learning period and its false negative rate is critical.

5. Conclusion

VoIP has become a key enabling technology for multimedia communication on the IP network. In addition, the Internet being an open network virtually eliminates geographic limitations for placing phone calls. However, as VoIP uses the existing IP network and thus inherits its vulnerabilities. To study the security issues related to VoIP, one must understand the basic VoIP architecture and existing defense mechanisms as well as current and potential threats and attacks on VoIP networks. In this article, we describe the basic VoIP architecture which consists of end-user equipment, network components, and VoIP gateway, as well as the fundamental differences compared to PSTN. The protocols used in VoIP systems for signaling such as H.323 and SIP, and for media transport such as RTP and RTCP have been described. We further discuss the existing defense mechanisms that are deployed in current VoIP systems to protect signaling (S/MIME, IPSec, and H.235), media transport (SRTP and SRTCP), and handle key management (MIKEY and ZRTP). Finally, the current VoIP attacks (e.g. DoS,

Eavesdropping, Masquerading, and Toll fraud) and their possible solutions are discussed followed by a discussion of the potential VoIP attacks such as SPIT and a survey of proposed solutions.

To secure the VoIP networks, we must have the basic knowledge of VoIP systems and its available security tools. Thus, we hope that this article provides such knowledge and useful information for readers who have interests in VoIP deployment and security.

References

Abani, M., Burrows, M., Birrell, A., Dabek, F., & Wobber, T. (2003). Bankable Postage for Network Services. In Proceedings of the 8th Asian Computing Science Conference, 2003.

Arkko, J., Carrara, E., Lindholm, F., Naslund, M., & Norrman, K. (2004). MIKEY: Multimedia Internet KEYing. RFC 3830.

Balasubramaniyan, V. A., Ahamad, M., & Park, H. (2007). CallRank: Combating SPIT Using Call Duration, Social Networks, and Global Reputation. In Proceedings of the 4th Conference on Email and Anti-Spam, August 2007.

Baugher, M., McGrew, Naslund, D., Carrara, E., & Norrman, K. (2004). The Secure Real-time Transport Protocol (SRTP). RFC 3711.

Baumann, R., Cavin, S., & Schmid, S. (2006). Voice Over IP – Security and SPIT. *Swiss Army FU Br 41, KryptDet Report*, University of Berne.

Blackwell, G. (2006). FoIP (Fraud over IP). From VoIP Planet website: http://www.voipplanet.com/trends/article.php/3616771.

Chau, F. (2007). Telecom fraud growing: survey. From Telecomasia website: http://www.telecomasia.net/article.php?id_article=5760.

Chou, W. (2007). VoIP Network Security. *IT Professional magazine*, Vol. 9, Issue 5, pp. 42-46, Sept.-Oct. 2007.

Communications Fraud Control Association (2006). World-wide telecom fraud survey 2006. From CFCA website: http://www.cfca.org/Documents/fraudloss_press_release.pdf.

Dantu, R. & Kolan, P. (2005). Detecting Spam in VoIP Networks. In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop, pp. 31–37, Cambridge, MA, 2005.

Gonsalves, A.(2006). Phishers Snare Victims with VoIP. From TechWeb Technology News website: http://www.techweb.com/wire/security/186701001.

Goodin, D. (2008). UK's number one router open to VoIP hijacking. From The Register website: http://www.theregister.co.uk/2008/01/21/bt_home_hub_voip_hijacking/.

Hansen, M., Hansen, M., & Moller, J. (2006). Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT. In Proceedings of the 3rd Annual VoIP Security Workshop, Berlin, June 2006.

Higdon, J. (2008). The Top 5 VoIP SecurityThreats of 2008. From VoIP-News website: http://www.voip-news.com/feature/top-security-threats-2008-012408/.

Higgins, K. J. (2006). Vishing' Attacks Use VOIP. From Dark Reading News Analysis website: http://www.darkreading.com/document.asp?doc_id=98787.

International Telecommunication Union (2000). Implementers Guide for H.323, H.225.0, H.245, H.246, H.283, H.235, H.450 Series, and H.341 Recommendations. From ITU website: http://www.itu.int/md/T01-SG16-001113-TD-PLEN-0058/en.

Jenings, C. (2007). Computational Puzzles for SPAM Reduction in SIP draft-jennings-sip-hashcash-06. IETF Internet-draft: http://tools.ietf.org/html/draft-jennings-sip-hashcash-06.

Kent, S., & Atkinson, R. (1998). Security Architecture for the Internet Protocol. RFC 2401.

Kirk, J. (2006). Worm may be spreading via Skype chat. From IDG News Service website: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=voip&articleId=9 006239&taxonomyId=81.

Leyden, J. (2004). Cisco VoIP kit open to 'snooping attacks'. From The Register website: http://www.theregister.co.uk/2004/02/20/cisco_voip_kit_open/.

Menezes, A., Van Oorschot, P., & Vanstone, S. (1997). *Handbook of Applied Cryptography*. CRC Press.

Mier, E., Birdsall, R., & Thayer, R. (2004). Breaking Through IP Telephony. From Network World Lab Alliance website: http://www.nwfusion.com/reviews/2004/0524voipsecurity.html.

National Cyber-Alert System (2005). Vulnerability Summary CVE-2005-1802, National vulnerabilities database, From National Cyber-Alert System website: http://nvd.nist.gov/nvd. cfm?cvename=CVE-2005-1802.

Network computing (2006). Security Big Security Flaws Found In Asterix PBX, IAX VoIP Client. From Network Computing website: http://www.networkcomputing.com/channels/networkinfrastructure/showArticle.jhtml?articleID=189400851.

Niccolini, (2006). SPIT Prevention: State of the Art and Research Challenges. From IPTEL website: http://www.iptel.org/voipsecurity/doc/07%20-%20Niccolini%20-%20SPIT%20prevention%20state%20of%20the%20art%20and%20research%20challenges.pdf.

Radermacher, T. A. (2005). Spam Prevention in Voice over IP Networks. *Master's thesis*, University of Salzburg.

Ramsdell, B. (2004). Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. RFC 3851.

Rohwer, T., & Abwehr von, T. C. (2006). Spam over Internet Telephony (SPIT-AL). White Paper.

Rosenberg, J. & Jennings, C. (2007). The Session Initiation Protocol (SIP) and Spam. RFC 5039.

Rosenberg, J., Schulzrinne, H., Camarillo, H., Johnson, A., Peterson, J., Sparks, R., Hardley, M., & Schooler. (2002). E. SIP: Session Initiation Protocol. RFC 3261.

Ryst, S. (2006). The Phone is the Latest Phishing Rod. From Business Week website: http://www.businessweek.com/technology/content/jul2006/tc20060710_811021.htm.

Sengar, H., Wijesekera, D., & Jajodia, S. (2008). Detecting VoIP Floods Using the Hellinger Distance. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, No. 6, pp. 794-805.

Schulzrinne, H., & Casner, S. (2003). RTP Profile for Audio and Video Conferences with Minimal Control. RFC 3551.

Schulzrinne, H., Casner, S., & Jabobson, V. (2003). RTP: A Transport Protocol for Real-Time Applications. RFC 3550.

Schwartz, D. & Sterman, B. (2005). SPIT (SPAM for Internet Telephony) Prevention Security Model. White Paper, Kayote Networks.

Sengar, H., Wang, H., Wijesekera, D., & Jajodia, S. (2007). SPS: A SPIT Prevention System for Voice-over IP Telephony Services. White paper, Voice & Data Security (VoDaSec) Solutions.

Shin, D. & Shim, C. (2005). Voice Spam Control with Grey Leveling. In Proceedings of the 2nd Workshop on Securing Voice over IP, 2005.

Sterman, B. (2005). Proposal for a SPIT Prevention Security Model. White Paper, Kayote Networks.

Teal, K. M. (2006). VoIP Network Security: How a Hacker Took Advantage of Vulnerabilities. From New Telephony website: http://www.businessweek.com/technology/content/jul2006/tc20060710_811021.htm.

Thermos, P. & Takanen, A. (2008). *Securing VoIP Networks*. Pearson Education, Inc.

Vinokurov, D., & MacIntosh, R. W. (2005). Detection and Mitigation of Unwanted Bulk Calls (Spam) in VoIP Networks. US Patent No. US2005/0259667 A1. November 2005.

VoIP Magazine Editorial Staff (2005). ISS Finds Flaws in Cisco VoIP. From VoIP Magazine News website: http://www.voip-magazine.com/index.php?option=com_content&task= view&id=272.

Ziemmermann, P. (2008). ZRTP: Media Path Key Agreement for Secure RTP draft-zimmermann-avt-zrtp-06. IETF draft, http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-06.

Santi Phithakkitnukoon is currently pursuing Ph.D. in Computer Science and Engineering at the University of North Texas, Denton. He received B.S. and M.S. degrees in Electrical Engineering from Southern Methodist University, Dallas, Texas, in 2003 and 2005, respectively. His research interests are focused on statistical learning algorithms, mobile social computing, and security in VoIP networks.

Ram Dantu (Corresponding Author) received the B.Eng. degree from the Madras Institute of Technology, Tamil Nadu, India, the M.Eng. degree from the Madras University, Tamil Nadu, and the Ph.D. degree from Concordia University, Montreal, QC, Canada. Since his Ph.D., he has over 20 years of experience in the networking industry with Cisco, Nortel, Alcatel, and Fujitsu, where he was responsible for advanced-technology products from concept to delivery. He is currently an Assistant Professor with the Department of Computer Science & Engineering, College of Engineering, University of North Texas, Denton. His research focus for the last five years has been on spam detection (in VOIP networks), network security, and next-generation networks.

Enkh-Amgalan Baatarjav received the B.S. degree in Computer Science in 2007 from the University of North Texas (UNT), Denton. He is currently pursuing Ph.D. degree in Computer Science and Engineering at UNT. His research interests include computer network, behavioral analysis of online social networking, and VoIP security.