Security Traits of VoIP

Ramanpreet Kaur Lamba[1], Kamalpreet Kaur[2]
Computer Science & Engineering[1, 2]
Lokmanya Tilak College of Engineering[1], *Dr. B.R. Ambedkar National Institute of Technology*[2]
Email: raman.preet.lamba@gmail.com[1], *kamalpreet88.sandhu@gmail.com*[2]

Abstract- Voice over IP (VoIP) technology is speedily adopted by consumers, enterprises, governments and militaries. This technology offer higher flexibility and more features than traditional telephony (PSTN) infrastructures, as well as the potential for lower cost through equipment consolidation and, for the consumer market, new business models. Voice over IP (VoIP) communications is becoming critical to the corporate world. Perhaps, it should be viewed as an opportunity to develop new, more effective security policies, processes and infrastructure. These new policies and practices can have a positive impact on the security of the whole network not just voice communications. This paper serve as a starting point for understanding the security aspects of VoIP in a rapidly evolving set of technologies that are seeing increasing deployment and use. The main goal is to provide a better understanding of the security landscape with respect to VoIP security aspects.

Index Terms- VoIP, Public Switched Telephone Network, ITU-T H.323, Session Initiation Protocol, Media Gateway Control Protocol**.**

1. INTRODUCTION

In VoIP technology, VoIP is a technology for producing telephone services on IP-based networks. Traditionally, these telephone services have been provided by the public switched telephone network (PSTN/ISDN), which has been managed and completely controlled by single, national operators in each country. The voice signal is first separated into frames, which are then stored in data packets, and finally transported over IP network using voice communication protocol. Currently, most VoIP systems use either one of two standards; H.3231 or the Session Initiation Protocol (SIP) [1].

VoIP caused a lot of excitement towards the end of the 90s, with the promise of providing a viable technology for the migration from the monolithic public switched telephone network (PSTN/ISDN) to next generation networks, for which telephone services are produced on an IP-based network. At the turn of the millennium, it was announced that the IETF’s Session Initiation Protocol (SIP) standard would be chosen as the basis for the 3GPP IP multimedia subsystem (IMS). SIP at this point, was still in an early phase of development. Problems with poor voice quality for the early Internet-based offerings, along with the added barrier of cumbersome technology, e.g., having to phone from the PC made it difficult for consumers to embrace the new technology, and lead to slow adoption rate. The immaturity of the emerging SIP standard contributed largely to the slowdown of the roll out of VoIP services along with uncertainty in the economic and market related factors, and the lack of a solid business model. Today, VoIP is being used everywhere with different levels of success. Home users may use an Analogue Terminal Adapter (ATA) to use their legacy POTS telephone sets and make telephone calls over the Internet. PC users have a choice of applications that allow them a rich user experience and address book facility, and VoIP telephones are available both as desktop models and cordless handsets using Wi-Fi. Mobile nomadic users may use their VoIP accounts wherever they find a broadband Internet connection. As is usually the case in software and systems development, VoIP security has not received sufficient attention during the development phases and is lagging behind in the deployment [2].

2. VOIP PROTOCOLS

The two most widely used protocols for VoIP are the ITU standard H.323 and the IETF standard SIP. Both are signalling protocols that set up, maintain and terminate a VoIP call. In addition, the Media Gateway Control Protocol (MGCP) provides a signalling and control protocol between VoIP gateways and traditional PSTN (Public Switched Telephone Network) gateways.

2.1. *ITU-T H.323 Protocol*

H.323 is a comprehensive protocol under the ITU-T specifications for sending voice, video and data across a network. The H.323 specification includes several sub-protocols [3]:

- H.225 for specifying call controls
- H.235 for specifying the security framework for H.323 and the call setup
- H.245 for specifying media paths and parameter negotiations such as terminal capabilities
- H.450 for specifying supplementary services such as call hold and call waiting.

H.235 also provides security features such as authentication, integrity, privacy and some non-repudiation support in H.323 communications. It is designed to operate seamlessly with other protocols like H.245 and H.225. A call setup is secured through Transport Layer Security (TLS). Once established, a call control is initiated so that encryption and media channel information can be negotiated. H.323 utilizes RTP (Real-time Transport Protocol) / RTCP (Real-time Transport Control Protocol) as its transport protocol, which rides on top of UDP. Encryption is performed within the RTP packet by third party hardware, or at the network layer. Authentication under H.323 can be either symmetric encryption-based or subscription-based. For symmetric encryption-based authentication, prior contact between the communicating entities is not required because the protocol uses Diffie-Hellman key-exchange to generate a shared secret identity between the two entities. With reference to the H.235 recommendation, a subscription-based authentication requires a prior shared secret identity, and there are three variations of this:

- Password-based with symmetric encryption,
- Password-based with hashing, and
- Certificate-based with signatures

2.2. *Session Initiation Protocol (SIP)*

SIP is a text-based application layer protocol that addresses the signalling and session management within a packet telephony network. It is defined in RFC 32616. SIP uses a request-response model similar to the HTTP protocol. In SIP, authentication and authorization are handled either on a request-by-request basis with a response mechanism, or by using a lower layer scheme. As SIP is a lightweight protocol, its security capabilities are very limited. SIP requests and responses cannot be end-to-end encrypted because message fields such as the request and route need to be visible to proxy servers that are present in many network architectures to ensure SIP requests are routed correctly. Voice data is transmitted in clear text over UDP and TCP. Although SIP supports S/MIME-based encryption using digital certificates, certain header fields used in requests and responses cannot be encrypted. The SIP protocol relies on transport layer security mechanisms such as TLS or IPSec to provide the required security for the whole message [7].

2.3. *Media gateway Control Protocol (MGCP)*

MGCP is published by the Media Control Working Group as RFC 34358. It expects that MGCP messages will always be carried over secure Internet connections as defined in the IP security architecture as defined in RFC 2401, using either the IP Authentication Header, defined in RFC 2402, or the IP Encapsulating Security Payload, defined in RFC 2406. This allows for data origin authentication, connectionless integrity and optional anti-replay protection of messages passed between the Media Gateway (MG), which converts circuit-switched traffic to packet-based traffic, and the Media Gateway Controller (MGC) that dictates the service logic of the traffic.

3. SECURITY ASPECTS OF VOIP

VoIP systems rely on a data network, which means security weaknesses and the types of attacks associated with any data network are possible. For example, in a conventional telephone system, physical access to the telephone lines or a compromise of the office private branch exchange (PBX) is required for in order to conduct activities such as wire-tapping. But for VoIP, voice is converted into IP packets that may travel through many network access points. Therefore the data is exposed to many more possible points of attack that could be used for interception by intruders. In fact, all the security risks associated with IP, such as computer viruses, Denial of Service and man in the middle attacks, are also dangerous to VoIP systems. In particular, PC-based IP Phone hosts are more susceptible to attacks due to the prevalence of attack techniques pinpointing PC systems. These include operating system vulnerabilities, application vulnerabilities, service vulnerabilities, worms, viruses, and so on [4]. A PC-based IP Phone is also at risk from any attack aimed at the entire data segment upon which it is residing. Since voice communication protocols are session control protocols, IP addresses and TCP / UDP port information is enclosed in packets. In networks that use a Network Address Translation (NAT) technique, the IP address and port information in the packets cannot be encrypted because NAT devices require such information to perform the translation. This imposes another security constraint to these protocols. The H.323 protocol is secured by using TLS, where a pre-defined TCP port 1300 must be used for the establishment of the Call Connection Channel and where no other security. Mechanism is available for the first connection. This fixed and well-known port can be a threat to the protocol. For SIP, encryption is based on the use of S/MIME.

VoIP also includes associated supplementary services such as conferencing (bridging), call forwarding, call waiting, multi-line, call diversion, park and pick-up, consultation, and "follow-me", among many other intelligent network services. Voice-over-Internet is a particular case of VoIP deployment, in which the voice traffic is carried over the public Internet backbone.

ITU-T H.323 was the first VoIP protocol to be defined and is considered to be the cornerstone for VoIP based products for consumer, business, service provider, entertainment, and professional applications. Rec. ITU-T H.323 defines four major components for a network-based communications system: terminals, gateways, gatekeepers, and multipoint control units [5]. Additionally, as all the elements of an ITU-T

H.323 system can be geographically distributed and, due to the open nature of IP networks, several security aspects exist, as illustrated in Figure 1.

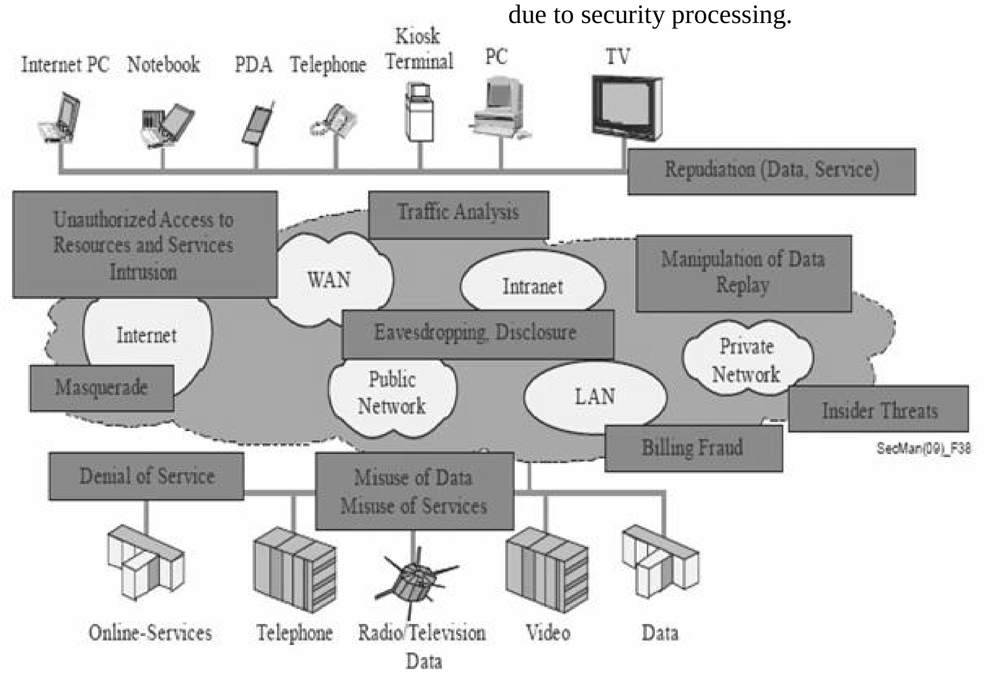

Fig. 1. Security aspects of VoIP

3.1. *The main security aspects in VoIP telephony are as follows:*

3.1.1 Server authentication:

Since VoIP users typically communicate with each other through some VoIP infrastructure that involves servers (gatekeepers, multicast units, gateways), users need to know if they are talking with the proper server and/or with the correct service provider. This applies to both fixed and mobile users.

3.1.2 User/terminal and server authentication:

This is needed to counter security *aspects*, such as masquerade, man-in-the-middle attacks, IP address spoofing and connection hijacking.

3.1.3 Call authorization:

This is the decision-making process to determine if the user/terminal is actually permitted to use a service feature *o*r a network resource (QoS, bandwidth, codec, etc.). Most often authentication and authorization functions are used together to make an access control decision. Authentication and authorization help to thwart attacks like masquerade, misuse and fraud, manipulation and denial-of-service.

3.1.4 Signalling security protection:

This addresses protection of the *signalling* protocols against manipulation, misuse, confidentiality and privacy. *Signalling* protocols are typically protected by using encryption as well as by integrity and replay protection measures. Special care has to be taken to meet the critical performance requirements of real-time communication to avoid any service impairment due to security processing.

3.1.5 Voice confidentiality:

This is realized through encryption of the voice packets and protects against eavesdropping. In general, the media packets of multimedia applications are encrypted as well as voice data. Advanced protection of media packets also includes authentication/integrity protection of the payloads.

3.1.6 *Key Management:*

This includes not only all tasks that are necessary for securely distributing keying material to users and servers, but also tasks like updating expired keys and replacing lost keys. Key management may be a separate task from the VoIP application (password provisioning) or may be integrated with *signalling* when security profiles with security capabilities are being dynamically negotiated and session-based keys are to be distributed.

3.1.7 Inter-domain Security:

This addresses the problem where systems in heterogeneous environments have implemented different security features because of different needs, different security policies and different security capabilities. As such, there is a need to dynamically negotiate security profiles and security capabilities such as cryptographic algorithms and their parameters. This becomes of particular importance when crossing domain boundaries and when different providers and networks are involved. An important security requirement for the inter-domain communication is the ability to traverse firewalls smoothly and to cope with constraints of network address translation (NAT) devices.

3.2. *Defined Aspects Terms*

3.2.1 Masquerading:

A masquerade is the pretence of an entity to be another entity. Masquerading can lead to charging fraud, breach of privacy, and breach of integrity. This attack can be carried out by hijacking a link after authentication has been performed, or by eavesdropping and subsequent replaying of authentication information. Using a masquerade attack, an attacker can gain unauthorized access to VoIP services. An attacker can steal the identity of a real user and obtain access by masquerading as the real user.

3.2.2 Eavesdropping:

Eavesdropping attacks describe a method by which an attacker is able to monitor the entire signaling and/or data stream between two or more VoIP endpoints, but cannot or does not alter the data itself.

3.2.3 Interception and Modification:

These classes of attacks describe a method by which an attacker can see the entire signaling and data stream between two endpoints, and can also modify the traffic as an intermediary in the conversation.

3.2.4 Denial of Service:

A denial of service (DoS) attack is an attack that is conducted to deliberately cause loss of availability of a service. We identify DoS attacks at several levels; transport-level, server level, signaling level.

- Transport level: An IP-level DoS attack may be carried out by flooding a target, e.g. by ping of death or Smurf attack.
- Server level: Servers may be rendered unusable by modifying stored information in order to prevent authorized users from accessing the service.

3.2.5 Misrepresentation:

The term misrepresentation is generically used to mean false or misleading communication. Misrepresentation includes the delivery of information which is false as to the identity, authority or rights of another party or false as to the content of information communicated.

4. CONCLUSION

This paper has discussed issues and the aspects to VoIP to mitigate these aspects. There is an increasing awareness of the potential problems and there are initiatives working to improve VoIP security. The true test of whether VoIP implementations are robust enough and provide sufficient security measures will come when VoIP essentially replaces the PSTN voice services. In the meantime, it is extremely important to rigorously test security of VoIP implementations to both test against resilience to known vulnerabilities as well as pinpointing unknown vulnerabilities and resolving other security issues.

REFERENCES

[1] B. Goode, “Voice Over Internet Protocol (VOIP)”. Proceedings of the IEEE, VOL. 90, NO. 9, Sept. 2002.

[2] P. Mehta and S. Udani, “Overview of Voice over IP”. Technical Report MS-CIS-01-31, Department of Computer Information Science, University of Pennsylvania, February 2001.

[3] Anonymous, “H.323 and SIP Integration”. White Paper, Cisco Systems, 2001.

[4] J. Larson, T. Dawson, M. Evans, J.C. Straley, “Defending VoIP Networks from DDoS Attacks”, GlobeCom 2004 VoIP Security Workshop.

[5] K. Siddiqui, M. Kamran, S. Tajammul, “Comparison of H.323 and SIP for IP Telephony Signaling”. In Proceedings of IEEE 4th International Multioptics Conference, Lahore, Pakistan, Dec. 2001.

[6] J. Thalhammer, “Security in VOIP-Telephony Systems”. Master Thesis, Institute for Applied Information Processing and Communications, Graz U. of Technology.

[7] H. Schulzrinne and J. Rosenberg. A comparison of SIP and H.323 for Internet telephony. In Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV), Cambridge, England, July1998.