A STUDY OF SIP AND H.323 PROTOCOL SECURITY IN VOIP SIGNALLING

Priya Chandran*

Dr. Chelpa Lingam Murthy**

ABSTRACT

VoIP is one of the commonly used services on internet. It provides a very important role in the field of communication. Since voice is transferred over the public network, where it is very easy to impersonate or modify data during transmission, there is a need for security mechanisms to protect the data. Many security mechanisms are already defined in the standards but they also have some limitations and many security problems remain unsolved. This paper focuses on the security aspects of the two commonly used protocols for VoIP signalling: SIP and H.323. During the comparative study, it is found that SIP is having more security mechanisms and thus less prone to error than H.323. TLS allows only those SIP entities to authenticate servers with whom they have a direct connection.

Keywords : VoIP,H.323,SIP,gateway,threats,TLS

* Assisstant Professor, BVIMIT, Navi-Mumbai

** Pillai's HOC College of Engg & Tech

INTRODUCTION

Before the wide use of internet, calls were made only using PSTN (Public Switched Telephone Network) systems. PSTN sets up a dedicated path between two parties for the duration of the call. Now the voice communication uses internet as a medium after the widespread use of internet. VoIP (Voice over Internet Protocol) is a technology that uses internet as a medium for sending ordinary telephone calls. So it is also known as internet telephony. It uses packet-switching technology unlike the traditional PSTN circuit-switching technology.

VoIP plays an important role in this field of communication. It provides a cheap and flexible service by utilizing packet-switched networks for voice data, providing a much cheaper solution than circuit-switched telecommunication services. The popularity is mainly because of the cheaper cost compared to the traditional telephones. Since it uses internet as the medium for transporting voice, the communication cost over distant geographical locations reduced. It also uses advanced communication applications. It transmits real time voice data using IP. When transmitted voice data through IP, voice is broken into small packets that are sent individually to their destination. Software called codec compresses the voice before transmission and decompresses them back to the original one at the receiver end.

VoIP is not restricted to internet only. It can be achieved on any network that uses IP, like intranets and Local Area Networks [3].

A typical VoIP system [8] is shown in figure1.

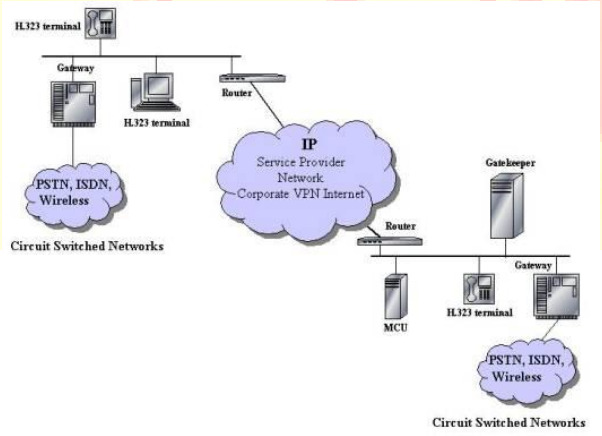

Figure1: VoIP Architecture

SECURITY ISSUES OF VoIP

In addition to all the above features and different services, VoIP is also having certain issues like call security, privacy of the communication, confidentiality and integrity of the message etc.

Since the data and voice passes through the common medium, internet, it is more vulnerable to threats. Protecting the security and integrity of data and thereby providing proper service is very important in VoIP.

Some of the common threats in VoIP systems are listed below:

- Remote eavesdropping
- VoIP Hopping
- VoIP phishing
- Invite flood
- Spoofing (Impersonation)
- Denial of Service (DoS) attack
- SPIT (Spam over Internet telephony)

VoIP PROTOCOLS

Voice over IP uses Internet Protocol (IP) for transmission of voice packets across the internet. All VoIP protocols are application layer protocols. Two very important and common signalling protocols used in VoIP application are H.323 and SIP (Session Initiation Protocol). Both this protocols support services like, setting up, control and terminating the VoIP call. This paper presents a study of these two protocols based on the security aspect of VoIP.

H.323 Protocol

This is a standard from ITU-T (International Telecommunication Union). It is an older and one of the most widely used standards for voice and video conferencing. It is a suit of standards like, H.225, H.235 etc. The following table shows the overview of H.323 protocol suite [4].

Name	The description of protocols
H.323	Specification of the system
H.225.0	Call control (RAS), call setup (Q.931-like protocol), and packetization and synchronization of media stream
H.235	Security protocol for authentication, integrity, privacy, etc.
H.245	Capability exchange communication and mode switching
H.450	Supplementary services including call holding, transfer, forwarding, etc
H.246	Interoperability with circuit-switched services
H.332	For large size conferencing
H.26x	Video codecs including H.261 and H.263
G.7xx	Audio codecs including G.711, G.723, G.729, G.728, etc

Table 1: Overview of H.323 protocol suit

H.323 is mainly used by VoIP gateways to connect IP network to PSTN. Gateway is used to covert telephony traffic into IP for transmission over a data network. H.323 can be carried over only by TCP.

ITU recommendation H.235 [ITU] specifies H.323 security requirements. It provides four security services- authentication, integrity, privacy and non-repudiation. Authentication is provided by admission control of endpoints through gatekeeper. Data integrity and privacy are provided by encryption. Non-repudiation ensures that no endpoint can deny that it participated in a call [6].

H.235 provides security procedures for H.323, H.225.0, H.245 and H.460 based systems. The scope of H.235 is to provide authentication, privacy and integrity for H.323 based systems. This standard mainly uses digital certificates and public-key mechanism for security implementation. H.235 includes some profiles which defines different levels of security and describes a set of possible security mechanisms offered by H.235 [5].

H.235v2 Protocol

Encryption is used to provide security to the message, This profile supports cryptography and Advanced Encryption System (AES). The message is encrypted at the sender side and decrypted at the receiver side. H.235v2 uses shared keys (Public Key Cryptography) and Digital Signatures.

H.235v3 Protocol

H.235v3 is introduced after H.235v2.It includes a procedure for encrypted signals, object identifiers for the AES encryption algorithm for media payload encryption, and the Enhanced Outer FeedBack (EOFB) stream cipher encryption mode for encryption media streams [5].

The following is a sample flow chart in the H.235 recommendations of encryption[7].

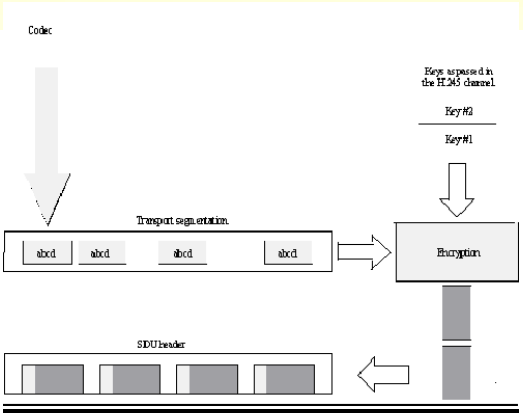

Figure2: H.235: Security and encryption for H.323

H.323 also uses authentication mechanisms of IPSec and TLS.

SIP (SESSION INITIATION PROTOCOL)

SIP is the standard from IETF (Internet Engineering Task Force) (RFC3261) for establishing VoIP connections. SIP is an application layer protocol that can establish, modify and terminate user sessions.

SIP architecture in shown in the following figure [8].

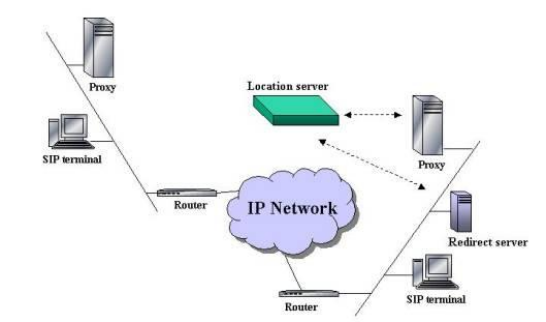

Figure3: SIP architecture

It can be carried by TCP, UDP, or SCTP. UDP can be used to decrease overhead and increase speed and efficiency, or TCP may be used if SSL/TLS is incorporated for security services. Now a day implementations use stream control transmission protocol (SCTP), developed in the IETF SIGTRAN working group (RFC 2960) specifically to transport signalling protocols [8]. SCTP offers increased resistance to DoS (Denial of Service) attacks through a four-way handshake method, the ability to multi-home, and optional bundling of multiple user messages into a single SCTP packet. Additional security services can be used with SCTP via RFC 3436 (TLS over SCTP) or 3554 (SCTP over IP Sec).

Overview of SIP protol suit is given figure4 [9].

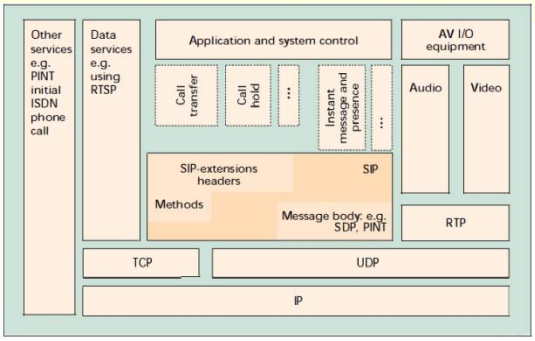

Figure 4: SIP protocol suit

Data authentication is used to ensure that the message is not altered during the transmission. End-to-end or hop-by-hop protection mechanism can be used to provide security in SIP. End-to-end mechanism involves the caller/callee SIP user agents are realized by features of the SIP protocol like SIP authentication and SIP message body encryption [11]. Hop-by-hop mechanisms secure the communication between two successive SIP entities in the path of signalling messages. Since the data can be modified during transmission, end-to-end mechanism cannot take care of that. Only hop-by-hop mechanism is applied in this context. Proxy-Authenticate, Proxy-authorization, authorization and WWW-Authenticate header fields are used for authenticating end system using digital signature. TLS (Transport Layer Security) protocol is commonly used with hop-by-hop security. TLS allows only those SIP entities to authenticate servers with whom they have a direct connection [12].

RECENT ADVANCES IN SIGNALLING SECURITY

Even though SIP and H.323 protocols are having their own security mechanisms, they are still vulnerable to attacks like eavesdropping, Denial of Service etc. Lots of researches are going on in the field of VoIP signalling security. Paper [13] proposed a new authentication mechanism to avoid eavesdropping in VoIP service where SIP protocol is used. The authentication scheme is based on end users Public key Infrastructure (PKI) certificate and one way hash function. In [14], the authors proposed a framework to detect DoS and other forms of intrusions by combining specification and anomaly based intrusion detection techniques.

CONCLUSION

SIP is the mostly preferred protocol compared to H.323 due to the simple architecture. Both the protocols are vulnerable to attacks, thereby reducing quality of service. Encryption is used by both protocols to secure data. The main concern is that it should not delay the communication. Since VoIP is a real time system, a very little delay also affects the quality of service. In order to provide the security, if the call processing is complicated, performance is affected.

REFERENCES

[1] Akshay Garg, Deepen Gupta, Vishwanath Sinha, 'Hybrid Packet Loss Recovery Scheme for Internet Telephony'.

[2] Rakesh Arora,' Voice Over IP : Protocols and Standards'. http://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols.pdf

[3]. Ismail Dalgic, Hanlin Fang,'Comparison of H.323 and SIP for IP Telephony Signaling'.

[4]. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries,' Security Considerations for Voice Over IP Systems',National Institute Of Standards and Technology.

[5]. T. Chown, B. Juby, 'Overview of Methods for Encryption of H.323 Data Streams'

[6]. http://www.javvin.com/protocolH235.html

[7].Mika Marjalaakso,' Security Requirements and Constraints of VoIP', http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/marjalaakso/voip.html

[8].Josef Glasmann-Munich University, Wolfgang Kellerer-DoCoMo Communications Laboratories, Herald Moller-Siemens,' Service Architectures in H.323 and SIP: A comparison', IEEE Communications Surveys and Tutorials,Fourth Quarter 2003.

[9]. Jan Seedorf, University of Hamburg,' Security Challenges for Peer-to-Peer SIP', IEEE Network , September/October 2006.

[10]. Stefano Salsano, DIE — Università di Roma "Tor Vergata"Luca Veltri, and Donald Papalilo, CoRiTeL — Research Consortium in Telecommunications,' SIP Security issues: The SIP Authentication Procedure and its Processing Load', IEEE Network , November/December 2002.

[11]. J. Rosenberg *et al.*, "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.

[12]. Srinivasan, R,' Authentication of Signaling in VoIP Applications',IEEE Asia-Pacific Conference,2005

[13]. Asgharian,Akbari,Raahemi,' A framework for SIP intrusion detection and response systems',International Symposim on Computer Networks and Distributed Systems on Feb 2011,IEEE.

[14] IEEE Commun. Mag., Special Issue on Internet Telephony, vol. 38, Apr. 2000.