SVIP-Enhanced Security Mechanism for SIP Based VoIP Systems and Its Issues

D. Chandramohan[1], D. Veeraiah[2], M. Shanmugam[1], N. Balaji[1], G. Sambasivam[1], and Shailesh Khapre[1]

[1] School of Engineering, Department of Computer Science and Engineering, Pondicherry University, Pondicherry
[2] Department of Computer Science, Vignan University
{pdchandramohan,d.veeraiah,maddy.shan,nbalajime1983, gsambu,shaileshkhaprerkl}@gmail.com

Abstract. As the SIP based VoIP system is entirely based on IP network, the vulnerabilities in it affects the VoIP system. This may result in degrading of quality of service in three aspects such as confidentiality, integrity and availability. This paper diagnose the security issues such as registration hijacking, session teardown, message tampering, IP spoofed flooding, disguised proxy and Spam over Internet Telephony (SPIT) and as well as the enhancements to improve the security mechanism to overcome the issues and to provide the quality of service to the legitimate users.

Keywords: Voice over IP (VoIP), Session Initiation Protocol (SIP), User Agent (UA), Real Time Protocol (RTP), Spam over Internet Telephony (SPIT), Transport Layer Security (TLS), Secure Real Time Protocol (SRTP) Introduction (Heading 1).

1 Introduction

VoIP has reached rapid development in the IT sectors for communication which is associated with Session Initiation Protocol as a signaling mechanism for connection establishment. As the VoIP [4] relies on the IP network, the vulnerabilities of the IP network affect the VoIP system. The effects of vulnerabilities affect the three major services to the legitimate users such as confidentiality, integrity and availability. The interception of attackers may hack the user's data and the personal information which may affect the confidentiality to the legitimate users. Through Real Time Protocol (RTP) packets illegal users tap the phone conversations of the legitimate users which make the absence of integrity to authorized and authenticated users. The service provided by the VoIP system is denied indirectly by the VoIP system to the legitimate users because of message tampering and flooding of SIP requests to the VoIP system by the attacker which results in affecting the quality of service and availability of service to the authorized and authenticated users.

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 81–86.
springerlink.com

2 Functions of VOIP

VoIP stands for Voice over Internet Protocol which transmits voice as an IP packet through internet. VoIP digitalize the voice into data packets, sending them and reconverting them into voice at destination. The digitalized signal is more noise tolerant than the analog signal. For conversion of digital into analog and vice versa the VoIP [2] system uses the convertor as well as the compression algorithm like Pulse Code Modulation (PCM) and Adaptive Differential Pulse Code Modulation (ADPCM) at both ends of the communication media. VoIP data packets are transmitted through RTP associated by UDP/IP packets. VoIP doesn't use TCP/IP because it is too heavy for real time applications, so UDP/IP is used. UDP has no control over the order in which packets arrive at the destination and the time duration to deliver the packets. Both of these are important for voice quality and conversion quality. RTP solves the problem enabling the receiver to put the packets back into the correct order and not for waiting long time for delivery of packets

3 Essential Components of SIP

IETF developed SIP [4] for IP based multimedia communications control protocol in the following aspects of function user location, session setup and session management and performance management. There are several types of SIP components such as SIP User Agent (UA) and SIP Registration Server, SIP Proxy Server and SIP Redirect Server. SIP Proxy Server receives the call requests through hop-by-hop technique. The SIP Redirect Server performs the routing which routes the called IP address to the Caller IP address. SIP Registration Server receives the information about the particular user, who wants to make use of VoIP communication and it provide the location based services.

4 Security Threats in SIP

SIP signaling mechanism is subjected to six types of attack, registration hijacking, disguised proxy, and malformed message, IP Spoofed Flooding, Session Teardown and Spam over Internet Telephony (SPIT).

4.1 Registration Hijacking

In order to make voice communication media between two end users, users must register themselves with basic information with user name and password. The requests sent by the user is simply a SIP request message[2], where the body of the message contains the user information, the username as well as the password and the FROM field which contains the IP address of the user and the destination is mentioned in the TO field. Twist (0) = O (1) = Z/2. An attacker can intercept and performs the Man-in-Middle attack captures the packets modify the FROM field to their own IP address and gain the username and password of the legitimate user. Through which the attacker can modify, listen and crack the data of the particular

user's signals and media packets. Model of Hijack threads involved indicated and described by following mathematical steps,

Twist (0) = O (1) = Z/2
Twist (1) = U (1) = SO (2)
Twist (2) = Sp (1) = SU (2)
Twist (3) = Sp (1) x Sp (1)
Twist (4) = Sp (2)
Twist (5) = SU (4)
{And && • ⋂⋂, Union → UU}
q□ (Hq • Im HƎp • qp□ (•┬q))
(q1, q2) • Im HƎp • q1pp□ (•┬q2))
⟦HP⟧^1 ≅ Twist•S^2

4.2 Disguised Proxy

Generally UDP packets are used for signaling between user agent and the proxy server where the security level is at low, this paves the way for the attacker to impersonate as a proxy through whom an attacker will be able to access all SIP messages and complete control of VoIP system call. Twist (1) = U (1) = SO (2). The illegal user disguises himself as a proxy by spoofed Domain Name Service (DNS) and camouflage Address Resolution Protocol (ARP) which is similar to the registration hijacking. If an attacker spoofed the DNS system of a particular domain, the attacker can make calls to any of the domain without any authentication and can also monitor and record the calls by intercepting the communication media.

4.3 Spam over Internet Telephony (SPIT)

Spam over Internet Telephony (SPIT) [1] is also called as VoIP Spam (VAM) is a bulk of message broadcasted over VoIP to phones connected to the internet. Marketers already using the voice mail for commercial messages, IP telephony makes a more effective channel because the sender can send messages in bulk instead of dialing each number separately. Twist (2) = Sp (1) = SU (2). Unscrupulous markets can use spam bots to harvest VoIP address or may hack into a computer used to route VoIP calls.

4.4 IP Spoofed Flooding

This is one of the denial of service where the attacker flood the SIP requests with different IP address spoofed from any mail server to the Twist (3) = Sp (1) x Sp (1) SIP server making the server overload and to terminate all calls which are currently in progress.

4.5 Malformed Message

The attacker sends a malformed or otherwise malicious SIP INVITE request to a telephony server which causes a crash of that server. Twist (4) = Sp (2). This is

specifically a problem for operators that run their servers on the public Internet. Because SIP allows the usage of UDP packets, it is easy for an attacker to spoof any source address in the Internet and send the malformed message from untraceable locations. By flooding these requests periodically, attackers can completely interrupt the telephony service.

4.6 Session Tear Down

Session tear down occurs when an attacker observes the signaling for a call, and then sends spoofed SIP "BYE" messages to the UAs. Twist (5) = SU (4). Most SIP UAs do not require strong authentication, which allows an attacker to send a properly crafted BYE messages to the two UAs, tearing down the call. If the UA does not check the value of the call, the attacker simply sends the "BYE" message if the user is active by spoofing the IP address of the UA which causes the calls to be tear down.

5 Enhancing the Security Mechanism in SIP

5.1 TLS over SIP

Session Initiation Protocol (SIP) is not inherently secure. It is essentially a communications-specific version of the HTTP protocol that makes up the basis for web data. Just as HTTP uses Secure Sockets Layer (SSL) [4] and security certificates to encrypt communications and ensure secure data transmission on the Web, SIP needs some additional layer of protection to ensure that VoIP and other audio/video communications that rely on SIP are secure. The majority of VoIP communications are secured using Message Digest 5 (MD5) authentication. MD5 has some known weaknesses and recently vulnerable to spoofing which could allow an attacker to fake an MD5 certificate. The much more secure alternative is Secure Multipurpose Internet Mail Extensions (S/MIME) which does not have the weaknesses of MD5 and can encrypt data directly within the SIP packets. Basically, just as HTTP rides on SSL, SIP rides on Transport Layer Security (TLS). Encrypting SIP transmissions with TLS helps to protect communications from man-in-the-middle attacks, eavesdropping, or unauthorized access. Secure SIP (SIPS), or SIP over TLS [4], enables the session to be encrypted on a hop-by-hop basis between the source and destination, providing better security than basic MD5 authentication, but without the complexity and overhead imposed by S/MIME. The SIPS URI ensures that SIP over TLS is used to encrypt and protect communications between hops and provide a secure connection from end-to-end.

5.2 Internet Protocol Security (IPSec)

IPSec [6] may be used to secure data transmissions between SIP gateways and proxy servers within a network, but IPSec is not suitable for protecting VoIP and unified communications data from end to end. IPSec establishes a secure connection between the source and destination devices, meaning that SIP proxies and hops along the way are unable to decrypt or modify the information in the SIP packets. TLS is a less complex and easier to manage solution that accomplishes the protection of the SIP session while still allowing the interim hops to work with the SIP data.

5.3 Secure Real Time Protocol (SRTP)

SRTP [2] is a security profile for RTP that adds confidentiality, message authentication, and replay protection to that protocol. It is an action item in the IETF Audio-Video Transport Working Group. Similar to RTP, SRTP is primarily used in VoIP communications. SRTP uses authentication and encryption algorithms to reduce the risk of a denial of service attack. It has the ability to achieve a high throughput in numerous communication platforms, including both wireless and hard-wired devices. SRTP mainly aims at ensuring the authenticity of a communication partner. For this purpose, communication partners usually exchange individual keys for each connection, with which message transmission is encrypted. Consequently, intruding parties cannot send messages, the originator of which is apparently a different person. Securing the confidentiality of RTP payload.RTP data is encrypted before its transmission for this purpose. This makes it difficult for intruding parties to read along sent messages. SRTP [6] Guarantees the integrity of RTP payload and header. This disables an intruding party to alter a message unnoticed. The authentication algorithms used in SRTP are MD5 and Hash Message Authentication Code (HMAC).

5.4 S/MIME

The Session Initiation Protocol specification currently details optional support for the use of secure MIME [4]. In general, the encryption of SIP message end-to-end is problematic because there are certain SIP entities, which need to view and modify the SIP headers and bodies. However, there will still be two standards ways how to encrypt SIP messages at SIP layer. Firstly, S/MIME [6] can be used to encrypt the SIP bodies. This is the most common and traditional use of MIME. Secondly, S/MIME can also be used to encrypt confidential SIP headers together with SIP bodies using a special SIP S/MIME tunneling mechanism. In SIP S/MIME tunneling, a SIP message can be protected and wrapped in S/MIME.

Table 1. Table of Requirements

Requirements	Solutions
Communicating to correct callee	TLS, S/MIME, IPSec
Correct invoicing	TLS, S/MIME, IPSec
Signal Protection	TLS, S/MIME, IPSec
Authentication of both end-user	TLS, S/MIME, IPSec
Secured Communication Media	TLS, SRTP, IPSec

```
Q′ (Hq • IM HϽP • QP′ (•┬q))

(Q1, Q2) • Im , H Ϟ P • Q1 PP′
(•┬Q2))

⟦HP⟧^1 ≅ Tw•S^2
```

Table 1 discusses about the issues and so the requirements for SIP based VoIP and as well as the solutions to tackle over the requirements needed for SIP based VoIP System to give the best quality of service to the authorized and authenticated users.

6 Conclusion

We have discussed about the functionality of VoIP, security issues in session initiation protocol and the enhancement of security mechanism in SIP based VoIP through which confidentiality, integrity and availability can be provided to the legitimate users and we have also discussed about the requirements and the protocols to overcome the requirements to provide a secure way of communication for SIP based VoIP.

References

1. Shan, L., Jiang, N.: Research on Security Mechanism of SIP basedVoIP System. In: 2009 IEEE Int. Conf. on Hybrid Intelligent Systems, pp. 408–410 (2009)
2. Albers, J., Hahn, B., McGann, S., et al.: An Analysis of Security Threats and Tools in SIP-Based VoIP Systems [EB/OL] (September 2005), http://www.colorado.edu/policylab/Papers/Univ_Colorado
3. Rosenberg, J., Schulzrinne, H., Camarillo, G., et al.: SIP: session initiation protocol [EB/OL] (June 2002), http://www.ietf.org/rfc/rfc3261.txt; Lucky, R.W.: Automatic equalization for digital communication. Bell Syst. Tech. J. 44(4), 547–588 (1965)
4. Zourzouvillys, T., Rescorla, E.: An Introduction to standards- Based VoIP. IEEE Internet Computing, 69–73 (2010)
5. TLS, SRTP, S/MIME, http://www.wikipedia.org (referred on January 2, 2011)
6. Salsano, S., Veltri, L., Papalilo, D.: SIP security issues: the SIP authentication procedure and its processing load. IEEE Network 16(6), 38–44 (2002)
7. Nanda Kishore, M.S., Jayakumar, S.K.V., Satya Reddy, G., Dhavachelvan, P., Chandramohan, D., Soumya Reddy, N.P.: Web service suitability assessment for cloud computing. In: Wyld, D.C., Wozniak, M., Chaki, N., Meghanathan, N., Nagamalai, D. (eds.) NeCoM 2011, WeST 2011, WiMoN 2011. CCIS, vol. 197, pp. 622–632. Springer, Heidelberg (2011)
8. Chandramohan, D., Jayakumar, S.K.V., Khapre, S., Nanda Kishore, M.S.: DWSE-Simulator For Distributed Web Service Environment. In: IEEE-International Conference on Recent Trends in Information Technology, ICRTIT-2011, pp. 1203–1208 (2011)
9. Chandramohan, D., Jayakumar, S.K.V., Khapre, S.: DTDWS-Design of TestBed for Distributed Web Service Environment. International Journal of Engineering Science and Technology (IJEST) 3(3), 2399–2404 (2011)
10. Chandramohan, D., Khapre, S., Ashokkumar, S.: A Study of Finding Similarities in Web Service Using Metrics. Selected for Publication in International Journal of Scientific & Engineering Research (IJSER) 2(6) (June 2011) ISSN 2229-5518
11. Khapre, S., Chandramohan, D.: Personalized Web Service Selection. International Journal of Web & Semantic Technology (IJWesT) 2(2), 78–93 (2011)