An Overview on Security Analysis of Session Initiation Protocol in VoIP network

Tarendra G. Rahangdale[1], Pritish A. Tijare[2], Swapnil N.Sawalkar[3]
M.E (Pursuing) [1], Associate Professor[2], Assistant Professor[3]
Computer Science and Engineering[1, 2, 3]
Sipna C .O. E. T, Amravati, India[1, 2, 3]
tarendrarahangdale285@gmail.com

Abstract-VoIP is new rising technology for the delivery of voice communication and multimedia session over the Internet. In VoIP network voice and signals are multiplexed and travel as normal data within the IP network. This rising popularity is due to cost saving issue and suppleness of services. SIP is VoIP standard protocol for create, maintain and end the voice communication. As VoIP service gets popular, they are also becomes target to attackers for their malicious activities. During this paper we tend to primarily concern with different SIP protocol attacks and their impact on the VoIP. This paper also explains the impact of TLS over the SIP server performance for better security.

Index Terms- VoIP (Voice over Internet Protocol); TLS (Transport Layer Security); SIP (Session Initiation Protocol); IP (Internet Protocol).

1. INTRODUCTION

VoIP is a methodology and cluster of technologies for the delivery of voice communication and multimedia session over IP networks, such as web. VoIP is additionally known as Internet telephony that specially refers to the provisioning of communication service (voice, fax, SMS, voice-messaging) over the internet, Instead of via the public switch telephone network (PSTN) [2]. VoIP outline standard Signal Initiation Protocol (SIP) [8] because the signaling protocol that establishes the VoIP voice communication. SIP is application layer protocol for making, modifying and terminating session with one or more participant. VoIP conjointly uses Real Time Protocol (RTP) [3] for media transport once the session is established among the participant. The growing popularity of VoIP service is because of flexibility and reduced cost over the IP network compared to existing PSTN telephone services. However because of popularity and use of VoIP service at the massive scale it also increases the vulnerability and security issues over the past years. The cause of threats and vulnerabilities are due to threats that widespread in existing circuit switch telephone network such as eavesdropping and toll fraud. We tends to exposed to new types of attack that also rife within the Internet that act as carrier for voice data. TLS [4] is employed to secure the signaling channel. IPSec may be used as an alternative that is default security specification in IPv6 protocol.

The remainder of the paper organized in to different sections. Section 2 includes the background of SIP Protocol and RTP protocol for VoIP call specification. Section 3 presents a closed description of SIP protocol attacks on VoIP service together with their classification. Evaluating the impact of SIP protocol attack on Security side of the VoIP service is described in section 4. Section 5 consists of some Analysis Tools and security using asterisks.

2. BACKGROUND

2.1. *SIP operation overview*

The Session Initiation Protocol (SIP) is signaling protocol which creates the VoIP connection. SIP is an application layer control protocol for creating, modifying and ending the session among the SIP users or VoIP participants.

SIP network contains the various logical SIP entities. Every entities has specific function in SIP communication as Client or Consumer (initiates request), as a server (response to request), or as each [1].

The four types of different logical SIP entities given as follows:

2.1.1 *User Agent:*

User Agent (UA) is the endpoint entity that starts and ends session by exchanging requests and responses. User agent is an application that contains both the User Agent client and User Agent server. The devices that can have a User Agent function in a SIP network are: telephony gateways, workstations, call agents, IP-phones etc.

2.1.2 Proxy Server:

A proxy Server is an entity that acts as a server and a client both for the purpose of making request on behalf of other clients.

2.1.3 Redirect Server:

A Redirect server suggest to the User Agent Client to try again at some other destinations after accepting a SIP request.

2.1.4 Registrar:

Registrar is a server which accepts register requests to updating a location database with the contact information specified in the request by the user.

2.2 SIP Message Element:

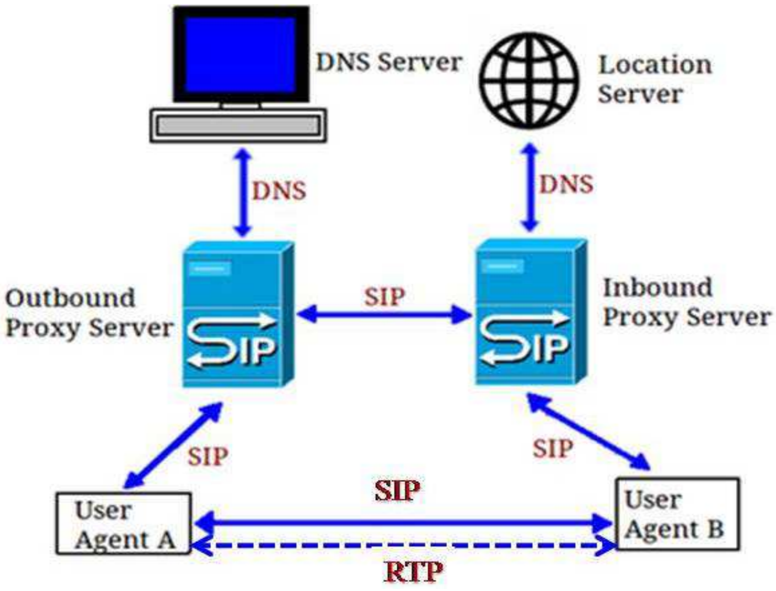
The main properties of the SIP protocol are that it is a client-server, request-response, text-based, transactional protocol. Every transaction involves the client who sends a textual request to a server, after that some computations are done by server and eventually server gives a final response to client. Each SIP message includes three identical parts structure namely first line, message header and message body. The first line shows the purpose of the message. For request it recognizes its type and the destination in form of URI which is important to SIP's routing mechanism.

Following are the two types of messages:
i. Requests → from client to the server.
ii. Response → from server to the client.

Table 1: SIP Request Message

Methods	Description
INVITE	Start a call, changes call parameters.
ACK	Make sure a final response for INVITE.
BYE	Disconnect a call.
CANCEL	Cancels the request
OPTIONS	Queries the ability of the other side.
REGISTER	Entry to the Location Service.

The response message contains the numeric response code. These response codes are representing in the different classes as follow:
1xx = tentative, searching, ringing, queuing etc.
2xx = succession of call.
3xx = redirection, forwarding the SIP request.
4xx = request failed (client mistakes).
5xx = server failed.
6xx = global failure (refusal).



2.3 SIP Call Flow:

In VoIP call, Session Initiation Protocol is standard to create, update and end the multimedia sessions between one or multiple participants. This VoIP call can be depicted by abstract network topology which regularly referred as the "SIP Trapezoid" shown in below Figure 1 which describes the interaction between SIP entities to interact with each other.

Figure 1: SIP Trapezoid.

The entities which are at bottom of trapezoid are represented by end-devices that interact with each other. SIP protocol creates the multimedia session and RTP protocol responsible for direct media transfer between user agents which is represented by dotted line.

Figure 2 shows the interaction between User Agent Client and User Server throughout the multimedia session creation and termination.

2.4 Real Time Protocol

Real-time Transport Protocol is a simple protocol to perform real-time data transmission between user entities as soon as the SIP session established [12].

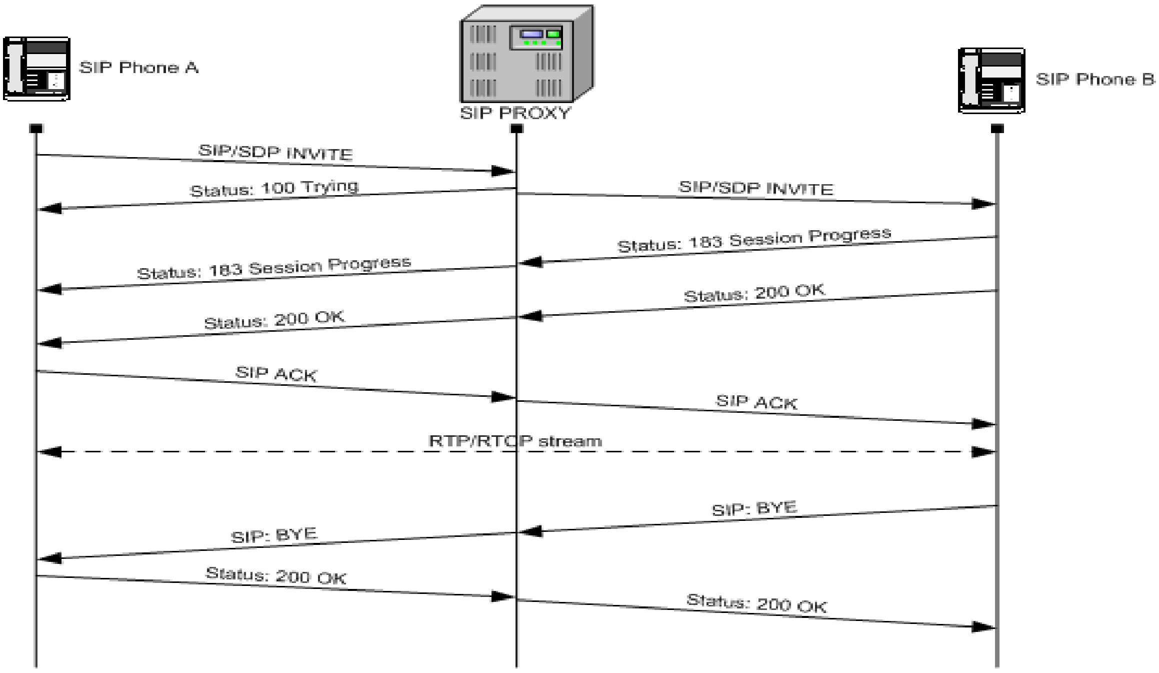


Figure 2: SIP call creation and termination.

3. SIP ATTACK CLASSIFICATION

SIP system is deployed in the Internet that can be Considered hostile environment, in which SIP messages may be exposed to a range of security threats and attacks. Following are some classified attacks on the SIP protocol.

3.1 SIP Dos attack

SIP DoS attack differ according to attack type, some attacks exploit vulnerabilities in SIP protocol implementation, wherever the others are resources consuming such as network bandwidth or agent processing capability.

Following are three categories of SIP Dos Attack [7]:

3.1.1 Message Flows Attacks:

In this attack throughout call establishment an attacker impersonate himself as legitimate SIP client to modify, deny, alter, or hijack VoIP calls.

3.1.2 Flooding Attacks:

These attacks depends on sending many legitimate SIP packets at high volume, so that the targeted

system is so busy in processing the requests that it is unable to process anything else.

3.1.3 Malformed Message Attacks:

This type of attacks depends on sending large numbers of malformed message to a SIP application server.

3.2 Message Flow Attack

SIP uses Requests/Response are text based and in most cases which are transmitted in clear text, hence they may be changed, spoofed or intercepted to perform attacks.

3.2.1 SIP Deregistration Attack:

In this attack the attacker sniff the network traffic, search for the registration message, and once found construct spoofed message similar to the captured and just change the expire field is set to zero, then direct it into the server. As a result server removes that client record and victim has no indication that he is not registered at the server.

3.2.2 SIP Cancel Attack:

The CANCEL request is employed to cancel a previous request sent by a client to which server does not give response yet. Attacker listens on the network traffic for new calls and then terminates every call using a Cancel request.

3.2.3 SIP BYE Attack:

By sending the SIP BYE request one of the call participants can terminate the VoIP calls. Several VoIP application servers and clients will process a BYE request without any authentication. Due to this it is easy to construct a BYE request and send it to the application server, so that it will then terminate the calls.

3.3 Faked Response Attack

SIP authentication is only provided to the SIP messages from the client to the servers; all the SIP messages from the SIP servers to client are remain unprotected. Offender can exploit this vulnerability to send a faked respond to the client, preventing him from creating calls, or redirect the call to different callee.

3.3.1 Call Hijacking / Transfer Attack:

Call Hijack attack refers to a state of affairs where one of the intended end points of the conversation is interchange with the assaulter. Once a call is hijacked, it is easy to forward it to the original callee.

3.3.2 Invite Attack:

Assaulter listens on network traffic searching for INVITE request, once get steal the authentication information and reconstruct spoofed INVITE request. Then redirect it to either callee or to the SIP server.

3.4 SIP Flooding Attack

There are large amount of bogus SIP massage that will require the allocation of process resources for decoding and interpreting. Causing system is busy in treating the bogus SIP massages, so that valid ones will treated at very slower rate and overall performance of conversation will decay [6].

3.4.1 SIP Register Flooding:

All the SIP devices send REGISTER requests at the time of start-up and at intervals thereafter. In networks where the numbers of deployed phones are large the processing load imposed on application server. So will easily reach to a point where the application server is too busy in processing REGISTER requests to handle new calls.

3.4.2 Invite Flooding Attack:

The Invite flooding attack is same as the Register flooding. The only difference is that rather than using Resister method it use the Invite method to launch the Invite flooding against the SIP server.

4. THE EFFECT OF SIP ATTACK'S AND SECURITY ISSUES

Considering the above vulnerabilities and attacks of the SIP protocol which produce terribly massive impact on the security issue of the VoIP system. Table 2 describes the SIP threats and security issue in VoIP system. It also gives the security requirement for the VoIP system [3].

Table 2: SIP Attack's, Security affair, and solution.

SIP Protocol risk	**Security affairs**	**Solutions**
Eavesdropping	Loss of Secrecy & affinity	Encryption mechanism such as TLS and IPSec

Reply Attack	Illegal Access	Encryption and Sequence of Message
SIP Flooding Message	DoS	Powerful authentication and configuration of Firewall
SIP Spoofing	Illegal Access	Powerful Authentication
Message Flow Attack	Authentication, Affinity, and Integrity	Encrypt Data by using encryption mechanism such as TLS and IPSec
Call Fraud	Integrity and Availability	Integrity and Availability

4.1 TLS Usages within SIP:

SIP's imposes the use of TLS (Transport Layer Security) [9] for proxies, redirect servers, and registrars so as to protect SIP messages. Use of TLS is recommended at end points for all VoIP network. TLS is in the position to shield SIP messages against integrity, confidentiality issues and replay attacks. It offers integrated key-management with mutual authentication and secure key distribution. TLS is applicable node-by-node security between User Agents/proxies or between proxies.

5. ANALYSIS AND SECURITY TOOLS

Following are some of the tools which are used for security analysis

5.1 Wireshark:

Wireshark is network analysis tool to eavesdropping
and analyze the VoIP call [14]. This tool used to analyze the VoIP network scenario.

5.2 SIP Attack Tools:

There are various tools and resources to study the vulnerability and threat exist in the VoIP network. These various open source tools are available on Internet for public domain [4].

5.3 Security Using Asterisk

Default transport utilized in Asterisk is UDP. To support the SIP over the TCP and SIP over TLS we can use the different option in "sip.conf" file. The worldwide options tlsenable and tlsbinder were set for the tls support. In sip.conf file for every user extension the transport option was set to tls to support TLS support for user security. After configure the server to the TLS support we need to also configure the SIP clients to support the tls for secure communication. We need to change the account setting along with additional features like TLS as transport protocol. Asterisk 1.8 version support the IPv6 network to connect the VoIP call using SIP IPv6 addressing scheme. The addition changes in the sip.conf file is to be done to support for the IPv6 configuration over the IPv6 network topology. [11, 13]

6. CONCLUSION

Securing the Session Initiation Protocol (SIP) protocol is one of the main goals while using secure VoIP network. By using the SIP over TLS based signaling, we can make it very secured against the SIP vulnerabilities and threats that we described above [5]. But using SIP over TLS for secure VoIP service brings the extra overhead on SIP server that makes bad impact on the VoIP performance and higher demands of hardware for both IPv4 and IPv6 network. IPv6 network provides some additional security against the certain attack as compared to the IPv4. But impact of SIP over TLS decrease the performance of SIP servers with very large scale as compared to SIP over UDP for both IPv4 and IPv6 based VoIP network.

REFERENCES

[1] Alan B. Johnston, SIP: Understanding the SessionInitiation Protocol, 2nd Edition, John Wiley & Son Ltd. 2009.

[2] Bassam, LIU, Jay, and Hajhamad "The Business of VoIP", Term Paper for the MBA course Technology Strategy, MIT Sloan School of Management, May 2005.

[3] C. Wieser, 1. Roning, and A. Takanen, Security analysis and experiment for Voice over IP RTP media streams, Proceedings of the 8th International Symposium on System and Information Security. Brazil, November 2006.

[4] F. Audet, Skype Labs, The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP). RFC [online] http://tools.ietf.org/html/rfc5630 October 2009.

[5] Ganesh Dadaji Sonwane, NITK Surathkal,Mangalore, India 2013IEEE. "Security Analysis of Session Initiation Protocol in IPv4 and IPv6 based VoIP network".

[6] Hemant Sengar, Haining Wang. Duminda Wijesekera, and Sushil Jajodia, "Detecting VolP floods using the Hellinger distance," IEEE Trans. on Parallel and Distributed Systems, Volume 19, No.6, pp. 794805, June 2008.

[7] Housam Al-Alloini, Alaa Eldin Rohiem, Mohammad Hoshen, Ali El-moghazy, VoIP Denial of service attacks classification and implementation,Radio Science Conference, 2009

[8] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson. SIP: Session Initiation Protocol, [online] http://tools.ietf.org/html/rfc3261 2002.

[9] Marima kulin, Tarik Kazak and Sasa Mrdovic, SIP Server Security with TLS: Relative Performance Evaluation, IX international Symposium on Telecommunications 2012.

[10] T. Dierks, E. Rescorla, The Transport Layer Security(TLS)Protocol,[online]http://tools.ietf.org/html/rfc5246 2008.

[11] Asterisk Get Started: What is Asterisk and what can you do with it? [Online] http://www.asterisk.org/get-started 2013

[12] Real-time Transport Protocol (RTP), [online] http://www.ietf.org/rfc/rfc3550.txt 2003.

[13] The Voice over IP Security Alliance, security tools [online] www.voipsa.org/Resources 2013.

[14] Wireshark Network Analyzer tool [online] http://wireshark.org 2013