Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 8, August 2013, pg.63 – 69

RESEARCH ARTICLE

Safety Dimensions of Session Initiation Protocol

K.V.N.R. Sai Krishna
S.V.R.M. College, Nagaram, India
saikrishna@svrmc.edu.in

Abstract— With the appearance of multimedia applications and the upcoming age of Voice over IP (VoIP), Voice setup and resources control protocols such as SIP and H.323 over the Internet are becoming increasingly attractive applications. In the last few years as a real competitor in traditional telephony services (PSTN), SIP has gained much attention when compared with H.323. SIP works at presentation and application layer thus it mainly faces security issue at these layers. The objective of this thesis is to describe the most relevant SIP related security issues and then present security mechanisms that can be deployed to overcome the SIP security related issues. This effort demonstrates the tasks necessary to enhance the SIP security both inside and outside of the network. It is divided into three main parts, where the first part describes the SIP architecture, for example, the SIP rivals, SIP components and how a SIP system works. The second part is about some vulnerability issues of concern to SIP, study of the proposed security mechanism and also analysis on how possible threats to the SIP system such as call hijacking, message tempering and DoS attack, affect the SIP based VoIP system. The third and final part describes different steps that have been taken to avoid SIP attacks, by implementing some of the proposed security mechanisms.

I. INTRODUCTION

Session Initiation Protocol (SIP) [4][5] is a standardized Internet Engineering Task Force (IETF) signalling /controlling protocol, for initiating, manipulating, managing and terminating a session. SIP is use to setup IP-based multimedia services such as audio and video streaming, instant messaging, and other real-time communication across commonly used packet networks [1]. SIP is a text based client-server protocol like HTTP and due to its simpler nature and flexible design; this protocol is becoming more popular than the H.323 family of protocols and will likely emerge as the dominant standard in coming years. The text-based nature of SIP messages however opens many opportunities for several attacks such as registration hijacking, impersonating a proxy and denial of services (Dos). SIP is a signalling protocol, and during the signalling phase several parameters are exchanged between the end users. These parameters contain the sensitive information like the user name and the location of the user. These parameters should be kept secret. Security issues of SIP are becoming a serious problem due to rapid development and wide adoption of SIP based VoIP system. The security services desire for SIP based VoIP systems are as follows:

- **Confidentiality:** SIP needs confidentiality and integrity of messages.
- **Authentication:** SIP needs authentication and privacy for the participant in a session.
- **Availability:** SIP needs availability of secured voice resources [2].

II. METHODOLOGY

The methodology of this study involves both theoretical and practical implementation. First, the SIP functionality is discussed, which gives a clear picture to find out why SIP system is vulnerable for different

attacks and what steps are necessary to secure it, so at the beginning, the project work discusses the general SIP architecture which includes; SIP components, SIP behaviour and how SIP performs different tasks during the communication process. Secondly, after understanding the SIP functionality, a SIP system is designed, which contain different security parameters such as firewall configuration and implementation of Demilitarize Zone (DMZ), IPSec and also TLS. To check the performance of proposed security solutions, different tests have been taken and the results are conducted into two scenarios. In the **1st scenario,** the SIP system is tested before implementing the security measurements. In the **2nd scenario,** the system is tested after configuring the proposed security measurements. The test results are also compared at the end. The implementation of this thesis consists of routers, switches, IP-soft phones and also including the attacker system.

III. HISTORY OF SIP

SIP emerged in the mid-1990s from the research of Henning Schulzrinne. He was an associate Professor of Department of Computer Science at Columbia University along with his research team. He was also the co-author of Real Time Streaming Protocol *(RTSP)* [9] for controlling streaming audio-video content over the web. In 1996, he submitted a proposal to IETF *(Internet Engineering Task force)* that actually contained the key elements of SIP. The IETF started working on SIP and issued its final specification "RFC 3261" in 2001. Several additional RFC's were issued after that but no fundamental work was done for security and authentication. Earlier SIP based services were introduced by the specific vendors but today's SIP based services are commonly used by different vendors. Organizations such as Sun Microsystems' Java are defining application program interfaces *(APIs)*. The developers are able to build components and applications that support SIP for service providers and enterprises. SIP received huge publicity with 3GPP's endorsement and publication of Microsoft's Windows messenger. Mass deployments began to appear in 2004 when the consumer prize of SIP terminals sank below $100[3] and open source SIP servers became available. The SIP is defined only at the root level and there is no network specification. SIP is viewed as a large Gateway that translates millions of SIP calls into the Public Switched Network. The most interesting part is that the SIP equipment does not specify how to integrate SIP equipment into a consistent network but the users of the SIP find it easy to add functionalities of network architecture according to their open-source SIP server's usage [3].

IV. SIP COMPONENTS

The session initiation protocol has two fundamental components, although it works in conjunction with other protocols and technologies. The main components are as follows:

- **User Agents**: the end points that make a call (the devices that participate in a call)
- **SIP Server:** provides different services such as requests from the clients and sends back the responses to the clients

V. SIP SERVERS

SIP Servers are basically used to resolve the username to an IP address so that the request can be directed properly from one user agent to other. Firstly the user registers himself with the SIP server (with username and current IP address), and then establishes their current location on the network. They also verify his online status before starting the session. If the user is available then they send the invitation. If the user is on other domain then they use a different SIP server for communication (pass on the request to another server).

- SIP servers are intermediary nodes which process can SIP request. They handle the signalling, associated with multiple calls, providing name resolution and user location. They are called SIP Network Servers.
- There are three types of SIP network servers that perform several different functions which are as follows: [12]
- **Proxy server** – it is a central element residing in the network which handles incoming invitations and performs routing. A SIP proxy between the UA, handles routes requests (from UAC to UAS) and responds back to these requests [3]. When a user places a call to a recipient Uniform Resource Identifier *(URI)*, the caller UA initiates the SIP Invitation messages to a proxy server and this server send routes to receiving User Agent. Commonly there are two types of SIP proxy servers: stateful proxy server (stateful proxy server keeps track of all requests and saves previous routing information) and stateless proxy server (stateless proxy server forwards incoming requests without maintaining any state). A Proxy server is a single physical entity in the SIP network that assumes the properties of both, a UAC and a UAS.

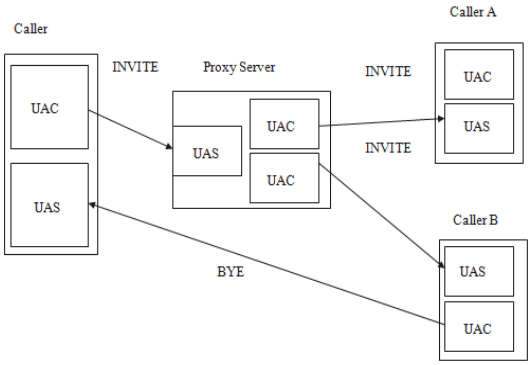

fig: UAC and UAS in a single network

Redirect Server – A Redirect server is another specialized instance of a UA. It does a very simple job, to answer the incoming request with a suggestion for UAC to try again for some other destination. In contrast to an SIP proxy server, it does not forward user requests [3]. It performs a lookup of a receiving message and replies with a location of its destination URI. The caller UA then sends an invitation request to the target URI. This can be very useful, for example if someone leaves a company and he requests that all incoming calls are redirected to his new address.[13]

Registrar Server - There is a major problem with the simplest-possible two-party call flow. The caller must know the IP of address destination equipment. It is very hard to remember the IP address of a caller, because they are temporary and frequently change. In SIP the solution to this problem is the concept of SIP permanent addresses that are known as Address of Record *(AoR)* [3]. The main purpose of the registrar is to process the register requests sent by a user to update his location address, which temporarily bind the user SIP URI to the current location and then the registrar stores the binding information into a location service [13].

VI. SIP SECURITY ISSUES

There are several security issues concern to SIP based VoIP system.

- *SIP Vulnerabilities*
- SIP was designed with simplicity just like many other Internet protocols for voice, but without built-in security. In SIP, different vulnerabilities are inherent, but most of the vulnerabilities were introduced by different developers during developing the SIP protocol into the product. [33]
- *SIP Protocol Vulnerabilities*
- As we mentioned earlier, the SIP protocol resides in an application layer. It is a text based client-server protocol within the UDP or TCP Transport that exchanges plain-text messages. It is easy to modify and readable to any malicious efforts that compromise with VoIP. However, SIP does not use any encryption mechanism, so it is very easy to access the sensitive information contained in the SIP protocol like:
- Information of sensitive IP address
- Address of the contact
- Information of Port address
- SIP compliance capabilities
- Username
- Media steam attribute
- Type of MIME Content

In SIP there are limited built-in security labels *(RFC 3261),* which have security-related item as “Should” rather than “Must”, and some other items are labelled as “Recommended”. SIP also supports different vendors, which are also interoperability and can be an issue from a security point of view, because all components should support the common security standard. For implementation and transporting, SIP messages use connection-less User Datagram Protocol *(UDP),* which is an unreliable form of packet transfers and also does not use re-transmissions or sequence numbers. It opens the gates for an attacker to spoof the UDP packets. Whereas TCP is guaranteed-delivery transport protocol because it is connection-oriented and more secure than UDP [16].

VII. NEED ADDITIONAL SECURITY IN A SIP SESSION

SIP sessions are used by network elements for modifying, terminating a session, and resource discovering. Therefore SIP security such as authentication, Confidentiality and authorization is an essential element. Different attacks like Denial of the

SIP Attacks

A SIP based system is vulnerable to common IP and VoIP attacks. The lists of attacks that are unique to SIP are as follows:

Registration Hijacking

This attack occurs when an intruder in the network impersonates a valid UA into a registrar and replaces his address as a legitimate user. Then all of the incoming calls send to the attacker legitimate address

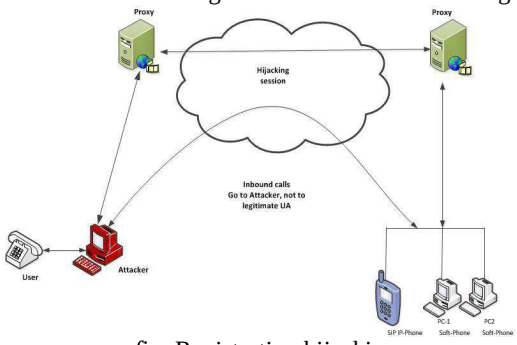

fig: Registration hijacking

The Registration process normally uses UDP protocol that provides a weak security mechanism. It is easier to spoof the request, as mentioned earlier, because it only requires username and password. In RFC 3261 standard, there is only challenge registration that is known as "Recommended" messages. Most of the registrar just requires a simple username and password. It can easily be defeated by generating dictionary-style attacks. In dictionary-style attacks, an attacker needs just to know the username and then he steps through a list of built-base passwords like enterprise name, office branch name or organization name. Some organizations use a shared mechanically generated weak password such as an extension with additional word, so this way an attacker may learn one of enterprise's passwords and then he may be able to learn all of its passwords. [16].

VIII. PRINCIPLE AND SECURITY REQUIREMENTS TO AVOID ATTACKS

There are different requirements for SIP applications security, for example if the call is being established between expected trusted parties, then the conversation between the parties should be protected by applying different security parameters. One party should be able to discard or reject any unwanted call. It means that in the system a different option should be available for the user to manage or limit the incoming calls. Lastly the information should not be revealed to an outsider, during the communication between the parties. [13]

8.1. Privacy

Privacy is defined by the VOIP alliance as "The Concept about the Privacy is the privilege to have their communication systems and content free from unauthorized access, interruption, delay or modification."[24]. In other words, users should know what kind of information is delivering, and it should be encrypted and finally it should successfully reach the intended party. Privacy issues between the parties present many threats to the applications such as message tampering, and message eavesdropping [13]. Privacy requires an implementation of a set of secure interfaces, which provide authentication, authorization and integrity

8.1.1. Confidentiality

In overlay storage we can provide confidentiality for each record and value. SIP URI can reveal party calling information. As mentioned earlier, a hash record key with a shared secret is used between the parties to prevent malicious users from call monitoring. These value-records contain the information such as caller presence status, buddy list and contact address. Then the system would be vulnerable to many attacks like message tampering, and eavesdropping without confidentiality.

To achieve confidentiality, there are different encryptions techniques, which provide user authentication, are as follows: Symmetric encryption. Asymmetric encryption.[13]

Integrity

To protect the source of data we use Integrity that provides user authentication. It is used for origin integrity, and without integrity control, any non-trusted system has the ability to modify the different contents without any notice.

Availability

The ability to access desired information or services on demand referred to as "Availability". When a user requires or requests any services, a system should ensure the user can access the required service without any problem. Sometimes it is called services on demand. Sometimes it is not possible due to various attacks such as DoS attacks or DDoS attacks. [14]

SIP Security Mechanism

There are different numbers of security protocols or schemes that should be integrated with the SIP protocol or used together with the SIP, to improve the security. These protocols and schemes are suggested and recommended by IETF, but most of them originated from communications communities. [26].

IX. FIREWALL

Firewall is a real mainstay of enterprise security and most of the private networks are widely adopting this technology. Firewall is a first defensive line against the unauthorized access and malicious traffic. Firewall is usually placed between the private network and outside Internet, in such a way that all incoming and outgoing packets pass through the firewall. The main function of the firewall is to examine all of the incoming and outgoing packets and then decide whether to accept these packets or discard them. These functions are called "Policies". Policies basically specify the sequence of rules [27]

- The polices rules are formed by two functions that are as follows
- Predicate
- Decision

Predicate of the rules are Boolean expressions, which represent the source and destination IP address along with source and destination port number. They also represent the Protocol type of the network. A packet matches a rule in such a way that the packet satisfies the predicate of roles that ensure that every packet matches at least one rule in the firewall. [27]. **Decision** of the rules decides whether the traffic can be accepted or discard. Sometime, the decisions can be combined with other options such as logging options. In the firewall these rules often conflict with each other for example if they overlap or if they have different decisions. Sometime, the rules are also conflicts, if one packet matches more than two rules.

X. HOW A FIREWALL WORKS

On the WAN (internet) each machine is assigned a unique address that refers to an IP address. These IP addresses contain 32-bit numbers that are expressed in dotted decimal numbers such as 4-octect 209.165.100.1/24 [28]. In domain names IP addresses are represented as human readable text name, such as www.staffwork.com. It is a very easy way to remember the name of the domain instead of an IP address. A Firewall in the company may block all access to this domain or allow access only to a certain domain. Protocols are pre-defined way of service. Protocols are texts, which define how the conversation starts between the clients and servers. There is a set of different protocols that the company firewall sets for filter such as IP *(Internet protocol)*, UDP (*User Datagram Protocol)*, FTP (File Transfer Protocol), ICMP *(Internet Control Message Protocol)*, and many other protocols. Firewall searches through each information packet for an exact match of the text that is listed in the filter list of the firewall [28].

XI. CONCLUSIONS

The SIP is such a protocol, which does not have any built-in security. This makes it more vulnerable to common VoIP attacks. In this implementation of the SIP security threats and countermeasures, the SIP secure model is designed to provide security mechanisms by following the best practices for securing a SIP based VOIP system. It offers standards-based security for all of the SIP system components. The implementation of the firewall and IPSec features are used to achieve the maximum security level against various SIP related attacks such as packet sniffing, call hijacking, message tempering and the DoS attack. The firewall implementation consists of different policies which have been configured in such a way that it monitors both the inbound and the outbound traffics. To provide security services at the network layer, the IPSec protocol is used to encrypt the SIP traffics. To enhance security, the IETF-standard Transport Layer Security (TLS), which is based on the Secure Socket Layer (SSL), is deployed into the designed model. Most of the SIP-based end points used the SIP-TLS to provide an added level of the security.

Finally, in this whole SIP system is inside a Demilitarized Zone (DMZ), which is a neutral zone between the private and public network and protects the system against all kinds of DoS attacks. The SIP server has also been prepared in such a way that it can protect itself from various attacks by acting as a firewall.

On behalf of security, the firewall and the IPSec VPNs can be the best solutions for real time traffic, but the solutions which provides best security, may not provide best performance. It may affect the QoS of the call by packet losing, jitter and synchronization etc. During the implementation of the firewall and the IPSec, the delay and low performance has also been observed. The IPSec imposes high CPU overhead on the SIP gateways (due to encryption process and voice traffic load). To overcome this problem there are two solutions. The first solution is to use a new VoIP over VPN security protocol [30], which supports IPSec tunnelling protocol in the combination with cRTP *(compressed Real Time Protocol)* and IPHC *(IP header compression)*. Secondly, as encryption mechanism requires a great amount of CPU and bandwidth, the separate installation of VPN accelerator card [31] is a good technique in such a way that it is exclusively dedicated to the data encryption/decryption mechanism. In this way the router is only involved in routing information, which also

increases the routing performance. High internet connection may be a good solution for reliable and high performance voice communication. For the remote user**,** remote VPN configuration can be used to protect sensitive information between the trusty parties.

REFERENCES

[1] Z.Rusinovic and N. Bogunovic "Self-healing Model for SIP-Based Services," Telecommunications, 2009. ConTEL 2009. 10th International Conference on IEEE 8-10 June 2009.

[2] Liancheng Shan Ning Jiang "Research on Security Mechanisms of SIP-based VoIP System" Hybrid Intelligent System 2009. HIS09. Ninth interbation conference on IEEE 12 august 2009

[3] Dorgham siasalem, John Floroiu, Jiri Kuthan, Ulrich Absent, Henning Schulzrinne, "SIP SECURITY BOOK" Chapter 3Intrduction to SIP, pp 44-77, WILEY publisher 2009.

[4] J. Rosenberg, H. Schulzrinne Columbia, A. Johnston WorldCom J. Peterson, Neustar R. Sparks dynamicsoft M. Handley ICIR E. Schooler AT&T"SIP: Session Initiation Protocol ",RFC 3261 June 2002

[5] G. Camarillo Ericsson" Internet Assigned Numbers Authority (IANA) Registration of the Message Media Feature Tag ", RFC 4569July 2006

[6] T. Berners-Lee,R. Fielding,H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0" network Working Group, RFC 1945 (Informational) 05 May 1996

[7] Jonathan B. Postel,"SIMPLE MAIL TRANSFER PROTOCOL", Information Sciences Institute RFC 821, August 1982.

[8] O. Levin," H.323 Uniform Resource Locator (URL) Scheme Registration" Network Working Group, RFC 3508 (Informational) ,2003-04

[9] H. Schulzrinne (Columbia U), A. Rao(Netscape), R. Lanphier (Real Networks), "Real Time Streaming Protocol (RTSP)" RFC 2326 (Proposed Standard) 04 April 1998.

[10] N. Greene (Nortel Networks), M. Ramalho (Cisco Systems), B. Rosen (Marconi) Media "Gateway Control Protocol Architecture and Requirements", RFC 2805 April 2000

[11] http://www.iptel.org/info/trends/sip.html (access 22 des 2011)

[12] SIPArchitecturehttp://media.techtarget.com/searchVoIP/downloads/Building_a_VoIP_Network_Ch%5B1%5D._8.pdf "

[13] Cheevarat Jampathom "P2P SIP SECURITY", HELSINKI UNIVERSITY OF TECHNOLOGY" Faculty of Information and Natural Sciences Department of Computer Science and Engineering Espoo", June 30, 2008

[14] Mudassir Fajandar (M.S. Telecommunications). "Implementing an Authorization model in a SIP User Agent to Secure SIP sessions" B.E., Bombay University 2003

[15] Ross Carter,Microsoft Real-Time Communications: Protocols and Technologies "Request or Response Version" Updated.

[16] Mark Collier, Chief Technology Officer Secure Logix Corporation, "Basic Vulnerability Issues for SIP Security.pdf ",1 March 2005.

[17] Introduction to 3CX Phone System for windows http://www.3cx.com/phone-system/ (access 25 Jan 2012)

[18] http://www.3cx.com/VOIP/voip-phone.html (access 25 Jan 2012)

[19] http://www.wireshark.org/about.html (access on 23 Jan 2012)

[20] Developed by Richard Sharpe .and updated by Ed Warnicke and more recently redesigned and updated by Ulf Lamping.

[21] http://nmap.org/, introduction (access on 23 Jan 2012)

[22] IP Traf, Source http://iptraf.seul.org/about.html (access 23 Jan 2012)

[23] http://www.manageengine.com/products/vqmanager/help/intro.html (access 25 jan 2012)

[24] VoIP Security and Privacy Threat Taxonomy "Public Release 1.0 24 October 2005" (access 29 Jan 2012)

[25] Jonas Kullenwall "Study of security aspects for Session Initiation Protocol" Division of Information Theory Department of Electrical Engineering Linkoping University Reg nr: LiTH-ISY-EX-3234-2002

[26] Alex X. Liu "Department of Computer Science and Engineering", "Formal Verification of Firewall Polices" Communications, 2008. ICC '08. IEEE International Conference on 2008. Michigan State University.

[27] Liu, Alex.X, and Mohamed G. Gouda, Member, IEEE"Firewall Policy Queries" Parallel and Distributed Systems, IEEE Transactions on 2009

[28] http://computer.howstuffworks.com/firewall2.htm (access on February 2012)

[29] Dimitrios Konstantaras; Mustafa Tahir, Växjö University, "Securing Network Connected Applications with Proposed Security Models" 2008.

[30] Wafaa Bou Diab, Samir Tohme, Carole Bassil "VPN Analysis and New Perspective for Securing Voice over VPN Networks" Networking and Services, 2008. ICNS 2008 Fourth International Conference on IEEE 2008.

[31] Perez, J.A.; Zarate, V.; Montes, A.; Garcia, C.;" Quality of Service Analysis of IPSec VPNs for Voice and

Video Traffic" Telecommunications, 2006. AICT-ICIW '06. International Conference on Internet and Web Applications and Services/Advanced International Conference on IEEE 2006.

[32] Application"www.ingate.com/appnotes/Ingate_Security_Best_Practices.pdf" note 02 September 2008 (access 04 April 2012)

[33] SIPFundamentals"http://www.computerweekly.com/news/2240081825/SIP-fundamentals" 29 June 2007 (access 06 April 2012)

[34] Daniel Petri "Understanding VPN Remote Access Mechanism" http://www.petri.co.il/understanding-vpn-remote-access-mechanism.htm January8, 2009 (access on 05 March 2012)

