2012 4th International Conference on Computer Research and Development
IPCSIT vol.39 (2012) © (2012) IACSIT Press, Singapore

Framework for Enhancing Sip Confidentiality to Prevent Unexpected High Sip Server Attacks by Using Crypto-Gateway Sip Server (Cgs)

Aws Naser Jaber [1], Kunalan Dava Rajoo [2] Selvakumar Manickam [3] + Azlan Bin Osman[4] , Ali Abdulrazzaq Khudher[5,] , Chen-Wei Tan [6]

[1] National Advanced IPv6 Centre (NAv6)

6th Floor, School of Computer, and Mathematical Sciences Building Universiti Sains Malaysia 11800
Penang, Malaysia

Abstract. We present a secrecy enhancement strategy for Session initiation protocol SIP servers to avert eavesdropping attacks on the SIP server. Even though a SIP host is after a Network Address Translation and firewall, assailers may possibly target these security features using several attack techniques, which includes spoofing the SIP package and scanning SIP users. Spoofing facilitates an attacker to acquire information about authentic SIP authority holder, and use these details to log on, thereby making calls. Such attacks may bring about severe financial losses to the organizations and VoIP companies, especially in case where a SIP proxy has provided with valuable facilities in collaboration with various other VoIP providers.The strategy proposed herein deploys SIP via confidentially applying deployed security gateway end-to-end SIP UA servers.. Results indicate that the deployed security policy for SIP provides substantial benefits in addressing security issues. Particularly, the proposed scheme allows the implementation of security measures ahead of time before attack has attempted on the SIP. Lastly, we review and evaluate the scheme along with other relevant security enhancement methods. Most of these methods are got analyzed by simulation, whilst the feasibility of the scheme considering the present work is verified through a case study.

Keywords: SIP Gateway Server (SGS);; RSA ; Opensis, Asterisks

1. Introduction

The Session Initiation Protocol (SIP) [1] is an application layer used for signaling protocols specified by the Internet Engineering Task Force (IETF). For the media establishment IETF already made a specific Real time Protocol (RTP) [2]. The Transportation of SIP message has to convey by transport-layer over IP protocols, such as SIP over UDP or TCP.

Since, it has been derived from Hypertext Markup Language (HTML), transaction cases of SIP are similar to HTML. Fig.1; shows the basic SIP call flow between user agent “A” and “B”. Table 1 below contains six requests used by SIP. Table 1: “REGISTER, INVITE, ACK, CANCEL, BYE, and OPTION”. User agents’ uses the ‘REGISTER’ requests to show its present IP address. Nevertheless, it has not only the URLs must be IP, but also it can be canonical telephony number, therefore, it can be managed with PSTN. Though, SIP is a smooth protocol for managing with other networks

Each SIP request carries a different meaning and is defined as:

- INVITE: Establishes a media session among User Agents (UA)
- ACK: When approval of the handshake among SIP messages are complete, the call will be established.
- CANCEL: Implies any previous session that is sent by a client.
- BYE: Ends the total sessions between two users, for example, ends the conference session by sending BYE request.
- OPTIONS: The user query for proxy server or other user before the “invite” request.

+ Corresponding author. Tel.: + (0060174725765); fax: +(+604-6533001).
E-mail address: (aws_z2010@yahoo.com).

Even though, the defects still there in the security influenced us to further enhance it as this digest authentication did not satisfied the security specifications in SIP-based IP telephony service. This protocol supports more flexible applications than others are such as mobile applications, and can be implemented in various wired and wireless networks, however suffering from security issues

TABLE I SIP where response messages

Description	Status code	Example
Informational	1xx	100 Trying
Success	2xx	200 Ok
Redirection	3xx	300 Multiple choices
Client error	4xx	400 Bad request
Server error	5xx	502 Bad geteway
Global failure	6xx	603 Decline

Our framework emphasis that for local networking encryptions / decryption that which is connected to internet backbone the internet ; however, for the outside network, we believe it might not work for the other side of the table, as we never know what algorithm has been applied on the other side for outside network. The purpose of the Gateway is usually to prevent eavesdropping inside the lab campus

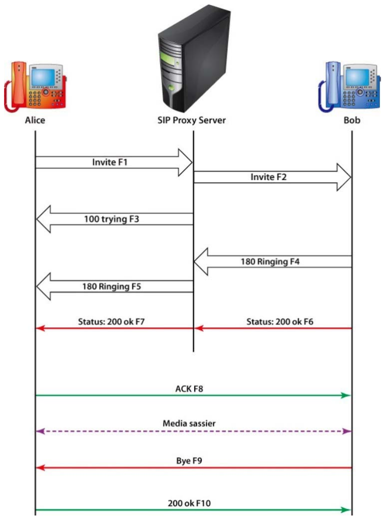

Fig. 1. SIP transaction

1.1. Related Works

SIP security explains and described for IETF works in RFC's 3329 [3], 4189 [4], and more others , some of them still under work and update. However, on the bright light, there appearance is of developed and secure whole SIP server instead of securing the extension its self, IETF already done A good related work that propose building security gateway as a third party support , that hold SIP the encryption inside the network. Especially, when they used pre-shared key and Multimedia Internet KEY (MIKEY) that used [5].

In other cases, the deployment on gateway foxes on monitoring for security issues especially on VoIP enterprise networking [6]. Other research enforce the authentication between sip proxies by blinding sip proxy server with user agent server (UAs) and remote database, the authentication enhancement will motivate on batch a deployment request for sip proxy.

A study held to propose a verification mechanism that will ensure the integrity of a call flow that does not require lots of effort as for the UA. This mechanism will help us to ensure the end-to-end integrity of a call flow and that without a user-level PKI. The application of verification mechanism and its validation is done on ZRTP that is a key-agreement protocol for SRTP [7] .

In an effort to deploy SIP over TLS, network operators should attempt to maximize the diligences of secure connections: this will require to reset the TLS connection. To compel a connection to readjust that is frequently indication the security among phones and gateways, is not hard to attempt. To reset that connection, the attacker needs to send the right kind of junk packet. This will interrupt the signalling channel between the phone and call server [8].

For the SIP cryptographic deployment, much recommendation effective protective technique of seclusion for an end-to-end VoIP ; an efficient solution that is applicable on both: the Elliptic-Curve-Diffie-Hellman (ECDH) algorithm (for key settlements), the key generation function (KGF) (for changing key dynamically in a VoIP call session). Such 2-tier key distribution plan offers effectual and strong security for VoIP voice packets at the time of end-to-end call sessions. To experiment with this proposed design, it is deployed on an open source SIP-based phone that of our test-bed on the web. The outcome of this experiment with the Internet mechanics of the lost packet embedded on the test-bed proved: this proposed scheme provides less hazardous VoIP call, additionally, it preserve the excellence of the transferred voice packets[9]. The SIP security mechanisms are categorized as; end-to-end, and hop-by-hop protection. End-to-end mechanisms: it involves the caller and/or called SIP user agents and realized by features of the SIP protocol that are specifically designed for this purpose (e.g., SIP authentication and SIP message body encryption). Hop-by-hop mechanisms secure the communication between two successive SIP entities in the path of signaling messages. There are no specific features provided for hop-by-hop protection by SIP, thus it relies on network-level such as IPsec [10].

2. Framework Goals

SIP has deduced from HTTP Digest Authentication, it has vulnerabilities against brute force attacks. Using dictionaries, weaker passwords can be identified by comparing the result of the digest algorithm in use. The reason that the most implementations use the HTTP Digest Authentication is its easy implementation and excellent performance. We found a rise in the SIP calls at six hours constant attack. We confer with the legitimate user and he revealed that he did not make the calls in the time we mentioned to him and the attacking time was out of working days' time. We went deep through in Asterisks reports We observed that the SIP extension was been hacked and used by any other person anywhere on this planet. A few numbers had appeared to be called frequently. Thus, open source materials such as Opensis which acting as a crypto-gateway and new formula for encryption and decryption . In addition, Asterisk acting as user client server. .further, methods used for encryption depend of RSA – 256 byte key length described in the paper

2.1. Framework Concepts

. Security consideration and selection for the Session Initiation Protocol (SIP) operation which is to prevent against various SIP vulnerability would be a vital procedures. The methods of attacking the User Agent Client (UAC), User Agent Server (UAS) or SIP Gateway are evolving throughout time. Securing the vulnerabilities and prevents the attacking methods is also improving by implementation of various security mechanisms. Current implementation of TLS [12] over SIP gateway, proxies, redirect server or registrars is provide better security for SIP signalling by offering strong authentication and encryption between SIP components [13].

However, improper configuration and low security implementation will result on compromising User Agent Server or unauthorized possession of user access credential. This will result to information theft or high cost of credits charges.SIP network infrastructure proposed as illustrated in Fig. 2. Contain the common component in a SIP environment which majority organization would implement and connection to VoIP provider. The User Agent Server with provider or manufacturer independent system which operated only the customize operating system, the SIP services and dependency packages or applications. This will reduce the loads of the processing by customized operating system which removed of non-important services or application and maximum input on the SIP signalling processing on the core system. The User Agent Server is also required Transport Layer Security (TLS) for encryption of the SIP traffics/signals between both end-points; User Agent Server and User Agent Client. Even though TLS provide a strong authentication and encryption between SIP components [13], but current evolving methods of SIP attacking/penetrations especially registration hijacking[14] and gateway/proxy impersonation[15] , the TLS features reliability becoming major concern to organization and VoIP providers. The new encryption algorithm proposed to be used is based on cryptography stream cipher (CSC) algorithm. Which is in fact , designed for bulk encryption of long streams of data [16].As it will be more efficient and faster in data encryption. In the proposed solution, the CSC mechanism is implemented over TLS encryption in User Agent Server. So the encryption and decryption will be occurred in process authenticating variety User Agent Client, as provided in Table 2.

Network Address Translation (NAT)[18] is proposed after review different network architecture. The network architecture provides protection from untrusted networks and the Internet to the dedicated User Agent Server network. The SIP Gateway device with the NAT and Firewall features, the ability of control and manipulation the traffic flow, legitimate connection or session, and data monitoring would possible compare with other network architecture implementation.

TABLE II. Encryption and Decryption Process

User Agent Client		SIP Gateway	User Agent Server
Global, Untrusted, Internet Network	IP PBX	SIP Gateway Server (SGS)	SIP Server
	SIP Phone		
	VoIP Provider		
Private Network	SIP Phone	-	SIP Server

3. Implementation and Results

As for the User Agent Client, required to include the features of SIP, TLS support, STUN support (NAT support) and CSC over TLS support. The CSC is assigned with encryption key which able to authenticate by the User Agent Server. This feature enables the authenticated User Agent Client devices (SIP Phones) to send TLS and CSC encrypted SIP signals to the User Agent Server, such as double encryption features. Our arguments when upon registration between User Agent Client and User Agent Server, negotiation message are conducted such as TCP Handshake and TLS Handshake. A high development by additional message is negotiated between User Agent Client and User Agent Server which is cryptography stream cipher (CSC) Handshake for authenticating the crypto key which verified between these two SIP components. The User Agent Client access credential such as extension number and password is protected by the encrypted messages. This is also applicable for various User Agent Client such as SIP Phones, IP PBX, Software Phones, VoIP Provider (trunk mode) and others which is located on the none trusted network or in the Internet. Thus, the aim of public key cryptosystems each client has two Public (Kpub) and Private (KPR) keys, which are produced by an authorized SIP server . So, the Public keys are stored in a database in SIP server and each client also keeps his privet key. RSA cryptosystem[19] has been established based on the discrete logarithm hard problem and encryption in this cryptosystem is defined as the taking the (Kpub) the roots modulo of n such that C=m ^ (K _ Pub) (mod n) , which is obtained by multiplying two large prime numbers (n= p × q). By the same way the value of C could be decrypted by = C ^ (K _Pr) (mod n) . By using the RSA algorithm authentication between two client users will be secure and also by the same way after completing the authentication clients can communicate secure by requesting the Pub key of the other party.

Step 1: User "**A**" Agent Client, requests the server to get the public key of User Agent Server.

Step 2: Server sends back the public key of User Agent Server to User Agent Client. (Kpub-S)

Step 3: User "A" encrypts the VOIP-ID of User "B" by his private key (Kpub-S) and sends to User Agent Server.

C = E (Void-IP-B, Kpub-S)

Step 4: User Agent Server decrypts the encrypted VOID-IP to identify the requested party's ID.

Void-IP-B =D(C, Kpr-S)

Step 5: User Agent Server encrypts the VOID-IP-A by public key of B (Kpub-B) and sends to User B to identify who wants to call to User B.

C1 =E(Void-IP-A, Kpub-B).

Step 6: User B agent client decrypts C1 to identify the requested party's ID.

Void-IP-A =D(C1, Kpr-B)

The attacker (Anonymous) point of view, unable to neither decrypt the messages nor SIP signalling as they would require the CSC encryption keys (Public & Private) to decipher to the original messages. Additional requirement proposed to be implemented in the SIP Gateway Server is the monitoring tools to monitor Inbound and Outbound traffic, monitor SIP traffic latency, monitor registration hijacking or other attacking methods and other required application

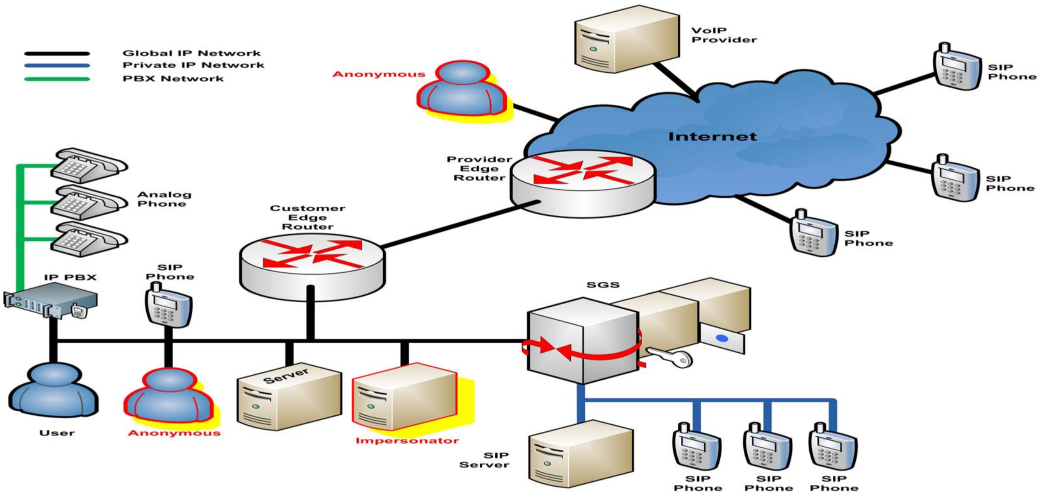

Fig.2. Proposed solution

4. Conclusions

A new framework is established in process of enhancing the security features to implement in SIP signalling. The proposed solution will ensure the integrity and confidentiality of the SIP traffic or session is preserved from the attacker

The framework intends to become a general guide that can be implemented and extended to have a correlation step. Other benefits of the proposed framework are We implement Security Gateway server, a security system influenced by good, strong, easy to apply for future work. The integration of firewall advanced rule set, Network Address Translation (NAT) in SIP Gateway and cryptography stream cipher algorithm over TLS encryption and decryption features in User Agent Server will increase the security and reliability comparing to SIP signalling eavesdropping and attacking methods in the current implementation.

5. References)

[1] J. Rosenberg , H. Schulzrinne , G. Camarillo , A. Johnston , J. Peterson , R. Sparks , M. Handley , E. Schooler, SIP: Session Initiation Protocol, RFC Editor, 2002 Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V. (2003) RTP: A Transport Protocol for Real-Time Application.

[2] J. Arkko , V. Torvinen , G. Camarillo , A. Niemi , T. Haukka, Security Mechanism Agreement for the Session Initiation Protocol (SIP), RFC 3329, 2003 K. Elissa. K. Ono and S. Tachimoto, “Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP),” RFC 4189,Oct. 2005

[3] Perez-Botero, D.; Donoso, Y.; , "VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures," Networking and Distributed Computing (ICNDC), 2011 Second International Conference on , vol., no., pp.192-196, 21-24 Sept. 2011.

[4] Nassar, M., Niccolini, S., State, R., Ewald, T.Holistic VoIP intrusion detection and prevention system (2007) Proceedings of the 1st International Conference on Principles, Systems and Applications of IP Telecommunications, IPTComm '07, pp. 1-9.

[5] Takahara, H.; Nakamura, M.; , "Enhancement of SIP Signaling for Integrity Verification," Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on , vol., no., pp.289-292, 19-23 July 2010

[6]]El Sawda, S., Urien, P., El Sawda, R. A trust communication with SIP protocol (2010) 2010 ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2010, art. no. 5587028, .

[7] Shen, C., Nahum, E., Schulzrinne, H., Wright, C.The impact of TLS on SIP server performance(2010) Proceedings of IPTComm 2010 - Principles, Systems and Applications of IP Telecommunications, pp. 59-70.

[8] Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” IETF RFC 2401, Nov. 1998.

[9] Tim Dierks and Eric Rescorla. RFC 5246--The Transport Layer Security (TLS) Protocol Version 1.2. http://www.ietf.org/rfc/rfc5246.txt, August 2008.

[10] Basic Vulnerability Issues for SIP Security - Mark Collier - Chief Technology Officer, SecureLogix Corporation - March 2005.

[11] Shan, L., Jiang, N.Research on security mechanisms of SIP-based VoIP system (2009) Proceedings - 2009 9th International Conference on Hybrid Intelligent Systems, HIS 2009, 2, art. no. 5254494, pp. 408-410.

[12] Geneiatakis, D., & Lambrinoudakis, C. (2007). A lightweight protection mechanism against signaling attacks in a SIP-based VoIP environment. Telecommunication Systems, 36(4), 153-159.

[13] Metzler, R.E.L., Agaian, S.S. Cipherstream covering for secure data compression (2011) Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, art. no. 6084190, pp. 3370-3377.

[14] Kim, S.-H., Vedantham, S., Pathak, P.SMB gateway firewall implementation using a network processor (2010) Network Security, 2010 (8), pp. 10-15.T. Hain, "Architectural Implications of NAT", RFC 2993.