Security Analysis of VoIP Architecture for Identifying SIP Vulnerabilities

Ubaid Ur Rehman
School of Electrical Engineering and Computer Science
National University of Sciences and Technology
Islamabad, Pakistan
12msccsurehman@seecs.edu.pk

Abdul Ghafoor Abbasi
School of Electrical Engineering and Computer Science
National University of Sciences and Technology
Islamabad, Pakistan
abdul.ghafoor@seecs.edu.pk

***Abstract*—Voice over Internet Protocol (VoIP) is an emerging technology that changes the way of communication services over IP networks. It provides flexible and low cost services to the users, which make it more popular than the existing Public Switch Telephone Network (PSTN). With the popularity of this technology, it became targeted victim of different attacks. In this paper we analyzed VoIP architecture, both theoretically and practically with more emphasizes on security of Session Initiation Protocol (SIP). In order to analyze theoretically, we performed a literature survey related to SIP security and classified it in term of existing SIP attacks and defenses. Our theoretical analysis reveals that most attacks on VoIP architecture were successful due to weaknesses of SIP, especially the authentication mechanism used in the session establishment phase. For practical analysis, we used open source Asterisk and pen-test it in different attacking scenarios using Kali Linux distribution. Our practical analysis studies revealed that open source asterisk server is still vulnerable to several attacks, which includes eavesdropping, intentional interruption, social threats, interception and modification, and unintentional interruption. We also provide a concise mitigating scheme based on Single Sign-On (SSO), which provides an efficient and reliable authentication mechanism for securing SIP.**

Keywords—Asterisk; VoIP; PSTN; SIP; Security; RTP

I. Introduction

Voice over Internet Protocol (VoIP) has the potential to change the way of voice and multimedia communication. It is an application layer protocol that provides a cheap alternative to the traditional Public Switch Telephone Network (PSTN) system. The term VoIP used for Internet telephony that delivers voice and multimedia data using the Internet. VoIP has two main components: (i) End System. (ii) Signaling Server. End System initiates, accept, reject, or forward request while Signaling Server use its location database, local policy, and DNS resolution to identify next signaling server or end point. Basic VoIP communication relies on two types of protocols: (i) Signaling Protocol that helps to establish, modify, or terminate a session. (ii) Media Transport Protocol that delivers multimedia data after the successful establishment of a session between entities. Normally, Session Initiation Protocol (SIP) [31] and Real-time Transport Protocol (RTP) [29] used as standard signaling and media transport protocol respectively. VoIP is mostly popular due its flexible, reliable, and low cost services as video calls, conference calls, instant messages, voicemails, and Interactive Voice Response (IVR). However, these services use the Internet as a communication medium, which make it more vulnerable to security threats because Internet vulnerabilities are also inherited to VoIP technology. VoIP security is also important because conversations on phones are transmitted in plaintext over the Internet, which helps the attacker to get access of communication channel due to weak authentication of SIP [22]. According to the security analysis of [19][20], the major cause of attacks on VoIP technology is due to vulnerabilities of SIP. As SIP was designed without any security concerns [31], it is vulnerable to several attacks as registration hijacking, impersonation, message tampering, eavesdropping, and man-in-the-middle attacks. Such attacks degrade the trust level of user to completely rely on VoIP instead of PSTN. In this paper our focus is on security analysis of VoIP architecture, especially to identify the weakness of Session Initiation Protocol (SIP).

The rest of the paper is organized as: Section 2 concisely describes an overview of SIP. Security analysis and countermeasures of SIP vulnerabilities based on literature survey are presented in section 3. Section 4 explains experimental setup, analysis tools, and discussion. Finally, section 5 summarizes the paper in terms of conclusion and future directions.

II. Overview of SIP

Hennin Schulzrinne and *Mark Handley* designed an application layer protocol SIP in 1996. The purpose of SIP was to provide a flexible and simplified framework, which helps to create, modify, and terminate user session. In 2000, third generation partnership project (3GPP) permanently accepted to use SIP as signaling protocol. In 2002, IETF advertised SIP in RFC-3261 [31]. Nowadays SIP is used as a standard signaling protocol for VoIP technology because of its flexible nature, integrating features and compatibility with devices. Most of VoIP service providers, smartphones, and increasing number of cordless devices also preferred to use SIP as a signaling protocol.

978-1-4799-6089-7/14/$31.00 ©2014 IEEE

A. *SIP Architecture*

SIP involves multiple elements to handle multimedia session over the Internet, which include user agent, registrar server, proxy server, and redirect server. *Figure 1* describes the generic architecture of SIP.

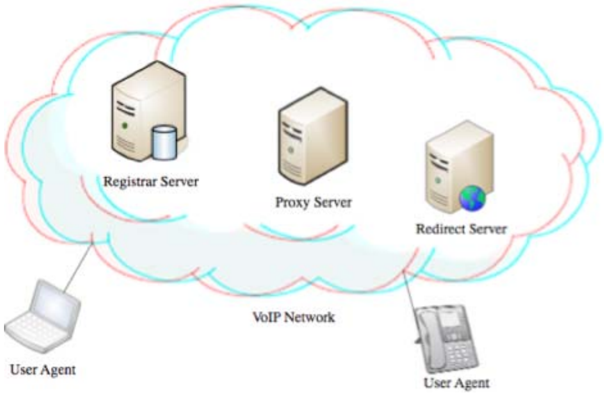

Fig. 1. The General Architecture of SIP

1) User Agent: User Agent may be client or server. The client user agent is responsible to initiate requests such as register, invite, bye, or cancel. The server user agent processes this request and respond in terms of provisional, success, or redirect, to the corresponding client.

2) Registrar Server: The registrar server maintains a database that contains locations and priorities of UA's.

3) Proxy Server: The proxy server receives requests from callers and forward it to corresponding callee, directly or through another server that is near to the actual location of callee.

4) Redirect Server: The redirect server provides information about the next hop server to the callers.

B. *SIP Layer Model*

According to RFC-3261, SIP is described in a layered stack. That isolates each layer from another layer based on its functionalities. *Figure 2* shows the layer model of SIP.

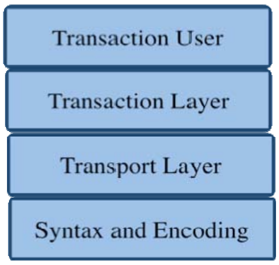

Fig. 2. The SIP Layer Model

1) Syntax and Encoding: The syntax and encoding is identified as the lowest layer of SIP, which is responsible for encoding of SIP data. The encoding is specified using Backus-Nour Form Grammar (BNF), a notation technique for a context free grammar.

2) Transport Layer: The transport layer describes the pattern of client side request and receives a response. Also define the mechanism of server side request processing and its response over the network.

3) Transaction Layer: The transaction layer is the major component of SIP, responsible for application layer retransmission, comparison of responses to requests, and application-layer timeout. The transaction layer is found in all SIP entities except the stateless proxy.

4) Transaction User (TU) Layer: The TU layer contains all SIP entities except the stateless proxy. It is capable of initiating and canceling of the client transaction instance.

C. *SIP Operation*

To initiate a SIP based call, the caller first required to register with an appropriate VoIP server. The VoIP server act as a gateway to forward request of caller to corresponding callee. The call establishment and protocol performance are briefly described in [23][31]. The flow of the call setup scenario is described in *Figure 3,* in which *User-A* requests to establish VoIP session with *User-B*. Initially *User-A (caller)* sends an *Invite* for *User-B* through a proxy server. The *Invite* contains certain information as *Request-Line*, *To*, *From*, *Contact*, and *Caller-ID*, which helps the intermediate proxy server to authenticate the received *Invite* and forward a regenerated *Invite* to corresponding callee. *User-B (callee)* received an *Invite* from the proxy server and responses back an *OK*, if callee is willing to talk. *User-A (caller)* received a response of *User-B (callee)* and send an *ACK*, which ensures that *User-A* also willing to talk. Thus VoIP calls established between both the entities. In order to terminate session, *BYE* is sent by a user and the call will be terminated after receiving *OK*.

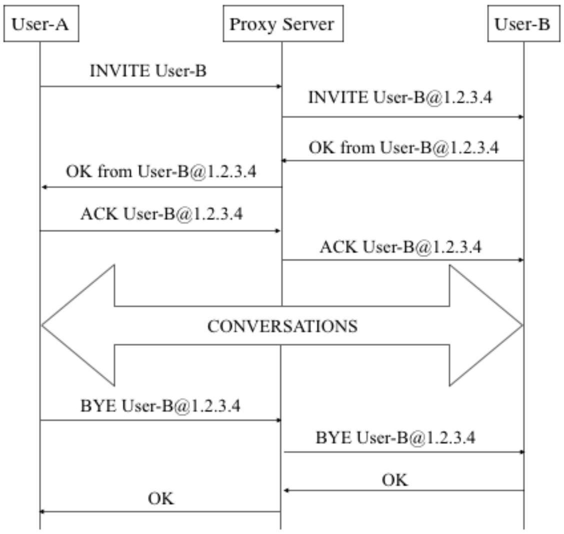

Fig. 3. The SIP based Call Setup Scenario

D. *SIP Security Threats*

The primary concerns of every communication protocol were reliability and efficiency, security was considered as a secondary feature. SIP was also designed without any security concerns and is vulnerable to several attacks. *Table 1* provides a concise description of SIP major attacks and its causes.

TABLE I. SUMMARY OF SIP MAJOR ATTACKS AND ITS CAUSES

Attacks	Registration Hijacking	Impersonating Server	Message Tampering	Session Teardown	Denial of Services
Descriptions	The SIP register message is vulnerable to modification. Therefore, the attacker gets registered on the user's behalf.	Attacker impersonates the identity of the remote server and intercept user agent requests.	A malicious server may change the character of the message or Session Description Protocol (SDP) body.	After successful establishment of session between two parties. It is critically ensured that certain requests are not forge as *Bye* or *Cancel,* which terminate a session.	The attacker redirects a huge number of *Register* requests to render a particular server unavailable.
Reasons	Lack of cryptographic assurance and message origin authentication.	Lack of mutual authentication between the communicating entities.	Lack of authentication and confidentiality.	Lack of message origin authentication.	Lack of secure SIP architecture and proper access control policies.

III. SECURITY ANALYSIS OF SIP

For the theoretical analysis, we have performed a literature survey related to SIP security and classified it in terms of existing SIP attacks and defenses, describe as follows:

A. Analysis of Existing SIP Attacks

1) Denial of Services (DoS): DoS attack compromises the availability of services and deny access of an authentic user to avail a service. In terms of the SIP, huge number of Invite and Register messages are used to crash SIP components. The flood of these messages triggers a variety of DoS attacks on end user terminal, registration server, and proxy server. *Geneiatakis et al.* [11] designed *Iancu algorithm* that counts the entire incoming request per IP address to avoid DoS attack. In [2], the authors designed a unique mitigation approach that distributes packets based on *weighted fair queues* based on *min-max-fair-share algorithm*. The *weighted queue* classified the *Invite* messages into legal and illegal queues based on its priorities. After classification the legal *Invite* queue messages are preceded to the server while illegal messages are discarded. A proxy model strategy was also used in [14], which detects *Invite flood* based on the user specified policy.

2) Eavesdropping: Eavesdropping is one of the common attack on a network, which provides a base for major attacks such as registration hijacking, impersonation, message tampering, spam over internet telephony (SPIT), and man-in-the-middle (MITM). The attacker uses some kind of tools as Wireshark or Nmap to analyze the network traffic. If the network traffic is not encrypted, the content may be exposed and tamper by the attacker. Several proof-of-concept shows that VoIP calls are easily wiretap as described in [3][13]. In [12], the authors designed secure SIP architecture named as *Touch Me Not*. The *Touch Me Not* divides an entire route between sender and receiver into several checkpoints. The main purpose of these checkpoints is, when an attacker tries to capture a packet or tap at any point, delay generator generates a non-removable popup that terminates the signal automatically. And both the sender and receiver are informed about the interception. *Karopoulos et al.* [18], proposed two types of solution that mitigates eavesdropping over heterogeneous network. In [15], the authors described that SIP servers are still vulnerable to eavesdropping attack and proposed a solution, which is applicable on both Elliptic Curve-Diffie Hellman (ECDH) algorithm and Key Generation Function (KGF). The cryptographic stream cipher was used for encryption of bulk data that ensure confidentiality and integrity.

3) Password Guessing Attacks: In password guessing attack, attacker captures a message, use different technique to guess password and verify it with the capture message [25]. The passwords that have low entropy are vulnerable to password guessing attack [26]. According to RFC-3261 [31], SIP uses HTTP digest authentication that is vulnerable to *password guessing* attack, the attacker guesses the password by using brute force techniques. *Yang et al.* [17] designed an authentication scheme that required high computation power for processing of the Discrete Logarithm (DL). *Durlanik et al.* [8] and *Wu et al.* [21] designed another authentication scheme based on *Elliptic Curve Cryptosystem*, which converge VoIP network and SIP services. The scheme concerns to processing load and size constraint. According to *Yoon et al.* [9], the proposed schemes of [8][21] are still vulnerable to several attacks such as *Denning-Sacco attack* [5], *password guessing* [27] and *stolen verifier attacks* [24]. *Pu et al.* [33] identifies several vulnerabilities in [9], which helps the attacker in guessing a password. And proposed a new scheme that provides mutual authentication using username and password.

4) Man-In-The-Middle (MITM) Attack: In MITM attack the attacker place itself into an ongoing communication between partners by spoofing the identity of the system. That helps the attacker to monitor, tamper, or hijack, VoIP signaling or media traffic. In [6], the authors designed *Massey-Omura Signcryption* scheme based on *Pairing Based Cryptography* that prevents MITM attack against SIP. The solution used public key cryptography for authentication, but no specific mechanism was described for the generation and storage of cryptographic key pair.

5) Parser Attack: The Parser attack uses malformed messages to retrieve data or analyze the behavior of VoIP system. These messages are difficult to detect that require a sophisticated algorithm to identify and discard it. *Geneiatakis et al.* [10], presented several solutions by using TLS, IPSec, and S/MIME, which provide partial prevention against insider and outsider parser attack.

6) Spam over Internet Telephony (SPIT): SPIT target individuals or group of users to generate a huge amount of unsolicited calls or messages using the IP network. It may also use as bots or zombies to launch attack on specific targets.

According to a survey in [30], we received 52% and 6% of unsolicited calls on landline and mobile phone respectively. The reason behind the less unsolicited call on mobile phone is due to the proper management of contact lists as compare to landline such as friends, family, VoIP users, and block lists. The issue of SPIT is more intensive than email spam. In [28][32], the authors provided several SPIT detection and prevention mechanisms. *Ono et al.* [30] presented two anti-SPIT solutions based on cross-media relation that required pre-shared information as email, token, or contact and use its hash value with HTTP. Another prototype of anti-SPIT, named as a *policy decision point* was also deployed in [4].

7) SQL Injection: SQL injection allows an attacker to send a malicious statement inside a query. Due to poor authentication, the statement passes to the backend database and executes, which leads to expose the stored data of backend databases. When SIP proxy or user-agent asks for authentication, the attacker may inject malicious SQL code. When the SIP server receives and execute the code, it makes the database services useless [11]. To prevent against SQL query tampering, we need to use digital signature, which help us to detect any kind of modified queries. The developer does not permit clients to modify SQL statements.

B. Analysis of Existing SIP Defenses

1) IP Security (IPSec): IPSec provides point-to-point SIP security, which required a pre-established trust between the communicating entities because intermediate nodes also take part in the communication.

2) Transport Layer Security (TLS): TLS uses public key cryptography, which does not require a pre-established trust. As we observed that SIP over TLS based solution utilize more resources, which proceed to the performance latency. Also, it does not ensure protection of the messages inside the recipient network as the last hop data is not encrypted.

3) Secure/Multipurpose Internet Mail Extension (S/MIME): S/MIME ensures end-to-end privacy, integrity and provide protection of the message against impersonation. It encapsulates SIP messages into MIME body, which create huge overhead and processing cost over SIP message.

4) SIP, TLS & S/MIME: In some situation, it is desired to use TLS and S/MIME at the same time, but it causes a problem, as the intermediate SIP proxy server requires specific fields of header for authentication. The TLS and S/MIME may use appropriately to secure SIP but still the hop-by-hop security problem remains there [32].

5) Secure Real-time Transport Protocol (SRTP): SRTP [1] provides authentication, privacy, and integrity of media data. It uses encryption and keyed hash to facilitate confidentiality and authentication respectively. But it is required to have pre-established trust and shared key.

IV. EXPERIMENTAL ANALYSIS AND DISCUSSION

In this section we have described the architecture of the experimental setup for pen-testing and practical analysis of behavior.

A. Experimental Setup

We have implemented experimental test bed to find the security issues in the practical implementation of open source Asterisk 11.9.0. We implement Asterisk on Linux distribution CentOS 6.5. The architecture of the pen-testing environment consists of Smartphones, Asterisk Server, Pen-testing and monitoring laptop, and iMac as demonstrated in *Figure 4.*

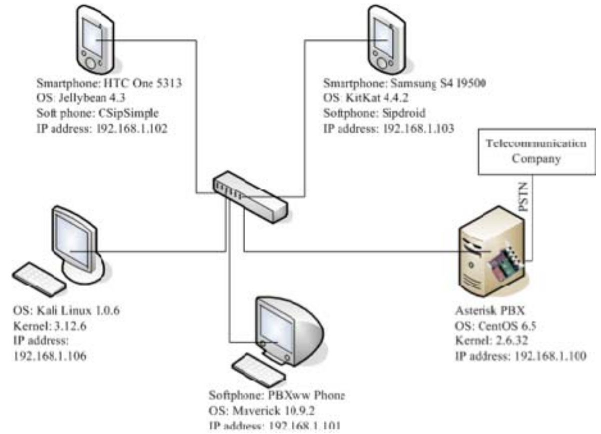

Fig. 4. Architecture of Experimental Setup

We have used *Samsung S4* and *HTC One* to install *Sipdroid* and *CSipSimple* softphones respectively. The *iMac* operates on *Maverick 10.9.2* that run open source *PBXww* Phone. All these softphones are registered to Asterisk Server, which also act as a gateway between Local Area Network (LAN) and Public Switch Telephone Network (PSTN) connected via *Digium TDM410P* card [7]. For pen-testing and monitoring the behavior of Asterisk server, we have connected a laptop on the same network and run different pen-testing tools on *Kali Linux.* The tools that are used to launch different attacks on Asterisk server are described in *Table 2*. We have analyzed the response of server on every attack and classified the attacks based on its behavior into five main categories: (i) Eavesdropping, (ii) Intentional Interruption, (iii) Social Threats, (iv) Interception and Modification, (v) Unintentional Interruption. Each category of attack has its own vulnerabilities and countermeasures, as presented in *Table 3.* From our vulnerability analysis results, we have concluded that most of the VoIP attacks are due to the weak authentication mechanism used during the session establishment phase. The cause of these attacks is due to some vulnerabilities of SIP, especially the digest authentication mechanism that is used during session establishment. Therefore, we also analyzed the existing authentication mechanisms of VoIP technology in terms of authentication, confidentiality and integrity, as described in *Table 4.*

TABLE II. LIST OF TOOLS TO LAUNCH SEVERAL ATTACKS ON ASTERISK SERVER

Attacks Tools	Brute-force Attack	Bye Flood	Dump SIP Session	Eavesdrop/Intercept Traffic	Fingerprint	IAX Flood	Identify Active Users	Inject Audio	Invite Flood	Password Cracking	Register Flood	RTP Flood	RTP Reconstruction	Scan	UDP Flood
AuthTool				x						x					
iaxflood						x									
inviteflood									x						
john				x						x					
nmap					x									x	
rtpbreak				x									x		
rtpflood			x									x			
rtpinsertsound				x				x							
sipcrack	x		x												
sipdump			x												
sipp		x							x		x				x
sipsak					x				x		x				x
svcrack										x					
svmap														x	
svwar							x								
Wireshark				x											

TABLE III. CLASSIFICATION OF SIP ATTACKS, ITS VULNERABILITIES AND COUNTERMEASURES

Attacks	Eavesdropping	Intentional Interruption	Social Threats	Interception and Modification	Unintentional Interruption
Results	Brute-force Attack	Denial of Services	Misrepresentation	Call Re-routing	Performance Latency
	Call Pattern Tracking	Flood Attack	Spam over Internet Telephony (SPIT)	Conversation Alteration	Power Fluctuation
	Conversation Reconstruction	Physical Intrusion	Spoofing	Conversation Hijacking	Resource Exhaustion
	Fingerprint	SQL Injection	Theft of Services	Dump SIP Session	
	Identify Active User		Unwanted Contract	Inject Audio	
	Password Cracking			Man-in-the-Middle (MITM)	
	Replay Attack				
	RTP Reconstruction				
	Scan				
Vulnerabilities	Lack of Authentication and confidentiality	Illegal Invite Message	Lack of Mutual Authentication	Lack of Mutual Authentication	Unusual VoIP traffic
		Lack of Access Control in Architecture			
	Lack of Cryptographic Assurance	Social Engineering Intrusion			
		Softphone Vulnerability			
		Trojan			
Countermeasures	Asymmetric Cryptography	Digital Signature	Cryptographic Token/Ticket	Intrusion Detection System	Firewall
	Datagram Transport Layer Security (DTLS)	Firewall Policy	Identity based Authentication	Policy of Firewall	Real Time Alert System
	Multimedia Internet KEYing (MIKEY)	Intrusion Detection System	Policy Decision Point	Network Address Translation	Service Detection System
	Secure Real-time Transport Protocol (SRTP)	Proxy Model Strategy		Pair Based Cryptography (PBC)	Session Boarder Controller
	Transport Layer Security (TLS)	User Level PKI		PKI Authentication and Key exchange	

TABLE IV. ANALYSIS RESULTS OF AUTHENTICATION MECHANISM USED BY VOIP

Authentication Mechanisms: **PSK: Pre-shared key** **PKI: Public Key Infrastructure** **ID: Identity based Cryptography**	**Authentication**	**Data Integrity**	**Data Confidentiality**
HTTP Basic Authentication	PSK	No	No
HTTP Digest Authentication	PSK	No	No
Secure MIME (S/MIME)	PKI	Yes	Yes
DTLS	PKI	Yes	Yes
Proxy based Authentication	PKI	Yes	Yes
ID based Authentication	ID	Yes	Yes

According to [16], the existing mechanisms have its own flaws that make it more vulnerable to several other attacks. Therefore, we need to provide an efficient authentication mechanism that provides flexibility to the user in term of security and efficiency. We need to use the concept of *Single Sign-On* using cryptographic token for authentication in VoIP technology, which only required customizing of open source server and softphone clients in order to support the authentication mechanism. Initially the user's smartphone application required to register with the corresponding VoIP server. On the successful registration, server assigned a cryptographic token to registered users, which is valid for a specific time period depends upon admin requirement. The token is bind with the identity of user and there is no need to remember username and password for authentication. The smartphone application uses this token to avail different services as a voice call, video call, conference call, voicemail, instant message, or interactive-voice-response. This mechanism provides reliability and efficiency to the user in terms of strong authentication, also help to prevent against the examined attacks.

V. CONCLUSION AND FUTURE WORK

In this paper, we have analyzed the security weakness of Session Initiation Protocol (SIP) in VoIP architecture. We have performed a literature survey to analyze SIP theoretically and classified them in terms of attacks and defenses. From our theoretical analysis, we have concluded that most attacks on VoIP are due to some weakness of SIP. Also, we practically analyzed and pen-test the open source Asterisk in different attacking scenarios and identified the threats. From our theoretical and practical analysis studies, we have concluded that SIP is still vulnerable to several attacks such as eavesdropping, intentional interruption, social threats, interception and modification, and unintentional interruption. According to our analysis results, the major cause of these attacks is due to digest authentication mechanism used in the session establishment phase. In order to secure SIP we need to provide an efficient and strong authentication mechanism that helps to secure SIP from most of the attacks. We have suggested to use the concept of Single Sign-On using cryptographic token for authentication in VoIP technology. Where VoIP server assigns cryptographic token to authentic user. The token binds with the identity of the user. Whenever a user wants to avail any service the server will simply authenticate the user by its token and there is no need to remember or use the username and password to avail any VoIP services. This mechanism provides an efficient and strong authentication mechanism, also provide protection against the examine attacks.

REFERENCES

[1] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC3711: Internet Engineering Task Force (IETF), March 2004.

[2] F. Zi-Fu, Y. Jun-Rong, W. Xiao-Yu, "A SIP DoS Flooding Attack Defense Mechanism based on Custom Weighted Fair Queue Scheduling", International Conference on Multimedia Technology (ICMT), Ningbo, China, October 2010.

[3] Chia-Chen Chang, Yung-Feng Lu, Ai-Chung Pang, Tei-Wei Kuo, "Design and Implementation of SIP Security", International Conference On Information Networking (ICOIN), Jeju Island, Korea, February 2005.

[4] N. d'Heureuse, J. Seedorf, S. Niccolini, "A policy framework for personalized and role-based SPIT prevention", 3rd International Conference on Principles, Systems and Applications of IP Telecommunications, Georgia, July 2009.

[5] D. E. Denning, G. M. Sacco, "Timestamps in key distribution protocols", Comunications of the ACM, Vol. 24, No. 8, August 1981.

[6] A. M. Deusajute, P. S. L. M. Barreto, "The SIP Security Enhanced by using Pairing-assisted Massey-Omura Signcryption", International Association for Cryptologic Research, Eprint, February 2008

[7] Digium TDM410P Manual, "Digium The Asterisk Company". [Online] *Available at: http://www.digium.com/sites/digium/files/analog-telephony-card-4-port-user-manual.pdf* [Accessed: December 2013]

[8] A. Durlanik, I. Sogukpinar, "SIP Authentication Scheme using ECDH", International Journal of Computer, Information, Systems and Control Engineering, Vol. 1, No. 8, January 2007.

[9] Eun-Jun Yoon, Kee-Young Yoo, C. Kim, You-Sik Hong, M. Jo, Hsiao-Hwa Chen, "A secure and efficient SIP authentication Scheme for converged VoIP networks", ACM Computer Communications, Vol. 33, No. 14, September 2010.

[10] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, "Survey of Security Vulnerabilities In Session Initiation protocol", IEEE Communications Surveys & Tutorials, Vol. 8, No. 3, July 2006.

[11] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, S. Gritzalis, "SIP Message Tampering: THE SQL code INJECTION attack", 13th IEEE International Conference on Software, Telecommunications and Computer Networks, Split, Croatia, September 2005.

[12] M. B. Sayyad, A. Chatterjee, S. L. Nalbalwar, "Proposed Model for SIP Security Enhancement", Communication and Network, Vol. 2, No. 1, February 2010.

[13] M. Herculea, T. M. Blaga, V. Dobrota, "Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture", 7th International Conference RoEduNet, Cluj-Napoca, Romania, August 2008.

[14] I. Hussain, F. Nait-Abdesselam, "Strategy based proxy to Secure User Agent from Flooding Attack in SIP", 7th International Conference Wireless Communications and Mobile Computing, Istanbul, Turkey, July 2011.

[15] A. N. Jaber, K. D. Rajoo, S. Manickam, A. B. Osman, A. A. Khudher, Tan Chen-Wei, “Framework for Enhancing SIP Confidentiality to Prevent Unexpected High SIP Server Attacks by using Crypto-Gateway Sip Server (Cgs)”, 4th International Conference on Computer Research and Development, Kunming, China, February 2012.

[16] I. I. Jan, Adeel, S. Rizwan et al., “A Survey of Security Weakness of Session Initiation Protocol (SIP)”, International Journal of Multidisciplinary Sciences & Engineering, Vol. 3, No. 4, April 2012.

[17] Chou-Chen Yang, Ren-Chiun Wang, Wei-Ting Liu, “Secure Authentication Scheme for Session Initiation Protocol”, Computer and Security, Vol. 24, No. 5, October 2004.

[18] G. Karopoulos, G. Kambourakis, S. Gritzalis, “PrivaSIP: Ad-hoc identity privacy in SIP”, Computer Standards and Interfaces Vol. 33, No. 3, March 2011.

[19] A. D. Keromytis, “A Look at VoIP Vulnerabilites”, Usenix Security Article, Vol. 35, No. 1, February 2010.

[20] A. D. Keromytis, “A Comprehensive Survey of Voice over IP Security Research”, IEEE Communications Surveys & Tutorials Vol. 14, No.2, May 2012.

[21] L. Wu, Y. Zhang, F. Wang, “A new provably secure authentication and key agreement protocol for SIP using ECC”, ACM Computer Standards & Interfaces, Vol. 31, No. 2, February 2009.

[22] Y. M. Koh, K. H. Kwon, “A New Lightweight Protection Method against Impersonation Attack on SIP”, Advances in Computer Science and its Applications CSA 2013, Vol. 279, 2014.

[23] D. R. Kuhn, T. J. Walsh, S. Fries , “Security Considerations for Voice over IP Systems”, National Institute of Standards and Technology, SP800-58, January 2005.

[24] Chung-Li Lin, T. Hwang, “A Password Authentication Scheme with Secure Password Updating”, Computers and Security, Vol. 22, No.1, January 2003.

[25] R. Lu, Z. Cao, “Off-line Password Guessing Attack on An Efficient Key Agreement Protocol for Secure Authentication”, International Journal of Network Security, Vol. 3, No. 1, July 2006.

[26] R. Lu, Z. Cao, “Simple three-party key exchange protocol”, Computer & Security, Vol. 26, No. 1, February 2007.

[27] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, “Handbook of Applied Cryptograph”, 1st Edition, New York: CRC Press, October 1996.

[28] S. Niccolini, “SPIT prevention: state of the art and research challenges”, 3rd VoIP Security Workshop, Berlin, June 2006

[29] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, RFC3550: Internet Engineering Task Force (IETF), July 2003.

[30] K. Ono, H. Schulzrinne, “How I Met You Before? Using Cross-Media relations to reduce SPIT”, 3rd International Conference on Principles, Systems and Applications of IP Telecommunications, Georgia, July 2009.

[31] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “Sip: Session Initiation Protocol”, RFC3261: Internet Engineering Task Force (IETF), June 2002.

[32] J. Peterson, C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)”, RFC4474: Internet Engineering Task Force (IETF), August 2006.

[33] Q. Pu, S. Wu, “Secure and Efficient SIP authentication Scheme for Converged VoIP Networks”, International Arab Journal of Information Technology, Vol. 9, No. 6, November 2012.