Journal of Computer Science 8 (3): 348-357, 2012
ISSN 1549-3636


# Session Initiation Protocol Security: A Brief Review

Aws Naser Jaber, Chen-Wei Tan,
Selvakumar Manickam and Ali Abdulrazzaq Khudher
National Advanced IPv6 Centre,
University Sains Malaysia, 11800 USM, Penang, Malaysia

**Abstract: Problem statement:** This study aims to discuss several issues on session initiation protocol security and threats. An in-depth investigation related to SIP with the intention to categorize the wide variety of SIP security issues. **Approach:** Related papers to the infrastructure of SIP security were analyzed. Some of the identified issues are: Social threats, eavesdropping, delaying, modification of media session, service abuse threats, physical access threats and denied services threats. **Results and Conclusion:** A useful categorization of SIP security issues has been done. The vulnerabilities of existing SIP infrastructure and possible remedies are discussed. It is confirmed that, message attacks are the most dominant category of SIP attacks.

**Key words:** Session Initiation Protocol (SIP), Voice over IP (VoIP), Denial of Service Attacks (DoS), authentication test, IP Multimedia Subsystem (IMS)

## INTRODUCTION

The Session Initiation Protocol (SIP) is an application layer used for signaling protocols specified by the Internet Engineering Task Force (IETF) (Schulzrinne and Rosenberg, 2000). SIP has recently become the main signaling protocol for Internet applications, thus allowing the implementation of a number of features using SIP, such as video conferencing, online gaming, peer-to-peer application, instant messaging, presence services and voicemail. Hotline services for emergency calls and online flight booking also use SIP. SIP also supports mobile applications, which are more flexible applications than others. SIP is implemented in different wired and wireless networks, which has security issues.

VoIP has gained a large number of users in the past 10 years with the rise of VoIP-oriented businesses. So, SIP can be used as an integrated protocol to manage a specific multimedia service, including several aspects of configuration, coordination and adaptation logic to response a session negotiation control of user sessions (Akbar and Farooq, 2009).

The IP Multimedia Core Network Subsystem (IMS) also uses SIP (Stefanec and Skuliber, 2011). SIP servers and proxies combined in IMS and named Call Service Control Functions (Femminella *et al*., 2009). A review of SIP security case studies was conducted to evaluate previous vulnerability studies. Thus, rapidity of development and deployment and the numerous vulnerabilities of VoIP together with products were discovered.

While vulnerabilities inherited from IP are varied and they affect the consumer privacy and system failure, these failures are defined as system vulnerabilities. User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) floods are highly favoured by attackers that can be used in SIP servers or end point users, for example, caller ID spoofing, phone impersonation, media eavesdropping, call and redirection, VoIP spam, Denial of Service (DoS) and Distributed Denial of Service Attacks (DDos).

**Background of the SIP protocol:** SIP is an application-layer dominated protocol that establishes, modifies and ends multimedia sessions such as conferences. SIP is designed for signaling Multicast call flow.

The IETF defined a protocol designed specifically for the control of real-time multimedia communications (Aslam *et al*., 2004). The intention is not to limit the requirements to support voice, but to create a specific session control protocol capable of supporting all forms of communications.

VoIP protocol deployment has several versions. SIP is one of the most studied protocols because of its ability to support multiple media types. Figure 1 illustrates SIP location at application layer of Open Systems Interconnection (OSI).

**Corresponding Author:** Aws Naser Jaber, National Advanced IPv6 Centre, University Sains Malaysia, 11800 USM, Penang, Malaysia

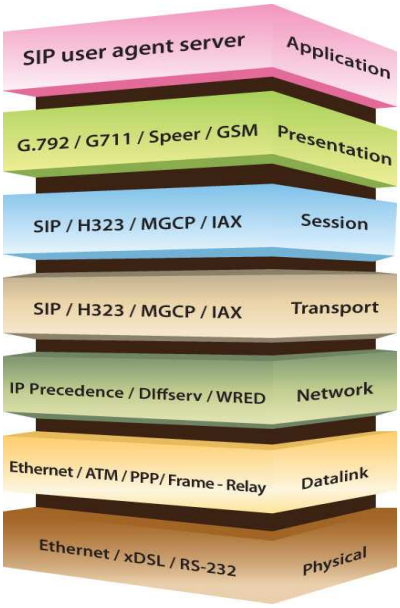


Fig. 1: SIP location within seven layer Open Systems Interconnection model

Table 1: Overview of SIP 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 |

The protocol was derived from the Hypertext Transfer Protocol (HTTP); several aspects of SIP protocol resemble HTTP. SIP is also implemented in web services and e-mail. A full SIP URI (Uniform Resource Identifier) is shown as: SIP URI = SIP username@ (IP or domain).

SIP is text-based, which makes it simpler to understand than most bit-oriented protocols, where knowledge of the significance of each bit position according to the rules and syntax of the defined protocol is required. The Transport of SIP messages can be carried by transport-layer over IP protocols, such as SIP over UDP or TCP.

SIP uses six requests Table 1: "REGISTER, INVITE, ACK, CANCEL, BYE and OPTION". The REGISTER request is used by a user agent to shows its present IP address. Nevertheless, it's not only the URLs must be IP, but also it can be canonical telephony number. So, it can manage with PSTN. In fact, SIP is a smooth protocol for managing with other networks.

Each one of SIP request has got 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

Moreover, it supports the header field and gathering information about the user agent before ringing.

Apart from SIP responses, there are three-digit codes. Due to the fact of the similarity between SIP and HTTP, the first digit refers to category of the response (for example, 481 Call/Transaction Does Not Exist and 200 OK).

There are six categories, namely: Informational response (1xx), Success; where the information was already delivered and request was passed successfully (2xx), Redirection; if the address has moved permanently, temporarily and using proxy the user can find alternative service (3xx), Client error; the request must proceed through proxy (4xx), Server error; server failures (5xx), Global failure; topical reqest cant response in server (6xx).

Nonetheless, SIP contains a dozen of response messages and Table 1 describes a few widely common SIP responses.

**SIP process:** The SIP operation is introduced as a specific example. Communication between Alice and Bob is used to explain SIP operation.

Besides, their end to end controls. An initial request starts from SIP server. It may be used as a user agent server. Otherwise, it will act as proxy server. The SIP proxy server was considered as the example here, for SIP signaling it should pass through SIP proxy server. When Alice log on to her SIP soft phone or hard-phone first step will be to register to the server sending invite messages, the server will response to Alice by informational trying, then proxy server will forward a second trying which will be received by Bob's telephony device.

Bob will ring his phone. The assumption is that Bob will pick up his incoming call, the message will be send for both SIP proxy server and Alice. When the SIP messages request succeeds, Final response to the INVITE "ACK" will be sent from Alice to Bob as illustrated in Fig. 2.

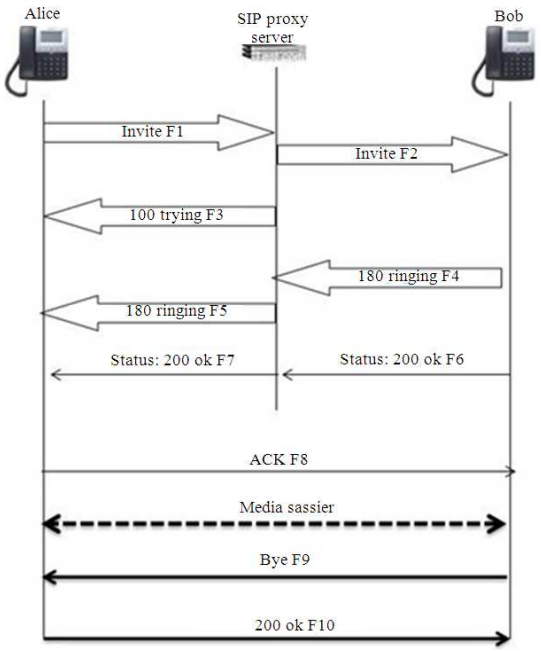


Fig. 2: SIP process

Table 2: SIP threat classification

| Threat | Definition |
|---|---|
| Eavesdropping | Attacker is able to capture the entire signaling and all data stream |
| Denial of Service (DoS) | causes loss of service to the users |
| Social threats | Misrepresentation of entities, |
| Interruption of services | loss of power, resource exhaustion, latency |

So, the media will start unless Bob ends the call. Thus, message from Bob will inform the server BYE and server will forward his request to Alice. After that, final agree message will be exchanged. RTP works point to point even if there are SIP proxy servers.

SIP normally uses Real Time Protocol (RTP) (Schulzrinne and Rosenberg, 2000). The purpose is to establish a media session.

**SIP attacks:** SIP proxies may suffer from unusual traffic (Keromytis, 2009), if there is not a third party solution to protect, monitor, prevent attacks. Concerns about instant messaging security through SIP has been discussed and explained in (Cui *et al*., 2010).

Most SIP servers build in optional Authentication procedures. However, it depends on the client's policy to enable or disable the security measure. SIP can operates over different transport protocols, which are simultaneously reliable and unreliable. Since Transport Layer Security (TLS) is a reliable transport protocol (Shen *et al.*, 2010), TLS evaluations use TCP transport. Generally, a TCP connection is established among end points. TLS and handshake occur to negotiate this connection. Thus, SIP signaling messages will be passed to the TLS layer for encryption. Large enterprise VoIP companies such as Skype suffer from attacks from time to time (Zhu and Fu, 2011). Meanwhile, a high traffic of Skype users have tempted attackers to target Skype. The attacks are mainly passive and based on Hidden Markov Model (HMM) (Srivastava, 2011; Murty and Devi, 2011; Ali *et al*., 2009; Charnsethikul, 2006; Ni *et al*., 2011), a great tool to model temporal data. A number of security modules have been created to solve this problem.

Voice over IP Security Alliance (VoIPSA) was created to address security and privacy threats for VoIP (Coulibaly and Liu, 2010). Within a short period of time since its inception, VoIPSA has more than doubled its membership. Before VoIPSA, no other group existed that could strongly help organizations in reducing VoIP security risks. The survey conducted a brief classification which is illustrated in Table 2.

This survey introduces brief study for SIP security researchers. Many other admirable surveys in the same field were published with high value of nobility, but this study gives a smooth refreshing knoweldge of SIP protocol and why hackers try hacking SIP servers and accounts.

The variety of SIP attacks starting with a leaked security threat and with Common Vulnerabilities and Exposures will be discussed.

**Survey of SIP security with different security threats: S**tudies on four taxonomy threats of SIP attacks were clarified to provide an overview and framework. Several Vulnerabilities, threat mechanism issues were also surveyed. Clues were formulated from high impact studies. The numbers of VoIP security works can be grouped into specific categories as described.

**Eavesdropping:** A professional VoIP programmer released several proof-of-concept programs to show how easily criminals eavesdrop on VoIP-based phone calls.

Karopoulos *et al*. (2011), described how to mitigate eavesdropping in exchanged SIP messages by presenting two types of solutions: PrivaSIP-1 and PrivaSIP-2. The proposed solution is suitable for mitigating SIP eavesdropping over heterogeneous networks contacted through SIP proxies. Previous research frameworks considered digest authentication weakness through indoor and outdoor SIP proxies. Therefore, the asymmetric cryptography can be

implemented in SIP headers. The main field SIP header "From" holds the privacy of the caller and the call recipient. The "From" header also carries sensitive information. Through social engineering the identity and home domain name of users are revealed.

Acute eavesdropping can either pass through as a recipient of the message between inbound and outbound or as a SIP proxy server. Therefore, the usefulness of the asymmetric cryptographic algorithm in a main branch can also be underlined. The use of asymmetric cryptography is obvious in caller IDs regardless of the SIP proxy location. The privacy method used to evaluate this effect was measured by time and client delay. The proposed SIP privacy scheme increases time delays before and after the implementation of asymmetric algorithm and cryptography. Previously published solutions failed to perceive time by keeping state data in "PrivaSIP-1" and "PrivaSIP-2" proxy models. Previous studies in SIP privacy against eavesdropping did not support this solution, which shows that in this work, privacy is more secured than that described in previous studies. Recent advances in research have the advantage of powerful user authentication with no trusted end-to-end proxies.

Yoon *et al*. (2009), studied the heterogeneous nature of VoIP and PSTN plus mobile networks and evaluated VoIP network security by three official security protocols. In addition, they explained end-to-end secure VoIP communication threats. Yoon proposed a possible solution limited to the SIP "option" which routes with a heterogeneous network. The result was that, it is not easy to provide a specific security design principle for VoIP communication in the backbone network; as development of heterogeneous networking structures continues. In this condition, testing of security protocols on test bed networks with TLS Secured Real Time Protocol (SRTP) and Multimedia Internet KEYing (MIKEY) were advised. This method is easier to fix than other protocols because of the implementation of MIKEY, which works between SIP-based VoIP and PSTN or SIP mobile user.

A security measure against VoIP eavesdropping for VoIP billing through hybrid network implemented just authentication server which is not enough against modern attack techniques.

Liu and Xu (2010), presented Peer-to-Peer SIP Authentication (P2P-SIP) scheme. The method was based on enhanced certification signatures, which can hold back fabricated identity, tampered and counterfeit messages during transmissions. They proposed that a unique node must first register to the Key Generation Centre (KGC) before joining the P2P overlay to verify its identity and obtain certificate authority for the next communication. The authors further made comparisons of security properties between related studies: one for streaming media in P2P networks and another for the P2P network authentication method based on Combined Public Key. The author framework shows the efficiency of preservation in P2P-SIP overlays.

Dawes (2011), proposed a mechanism to secure SIP media side, this RFC is strongly admired; the medication is SIP header that combine Datagram Transport Layer Security (DTLS) and Secure RTP (SRTP) named "DTLS-SRTP" in header through end-to-access-edge. While SIP transaction will pass through back-to-back SIP server, the session description will be secured in their proposed solution. As a result, the solution will secure media indeed and its already registerd in Internet Assigned Numbers Authority (Cerf, 1998).

**DoS attack:** Several components in a VoIP system, including media gateways, IP phones, IP PBX, VoIP firewalls and so on process signaling, causing DoS against the signaling interfaces to be a major issue (Liu *et al*., 2009).

Hussain and Nait-Abdesselam (2011), proposed a method to detect INVITE flooding on the SIP proxy server by a proxy model strategy that is based on a user-specified policy. The deployed module is based on type of SIP traffic message. Thus, the author's aim is to reduce the flooding attack to the normal SIP traffic and to identify the attacked traffic pattern.

Mehta *et al*. (2011), identified mitigation technique related for malformed messages. Their proposed intrusion detection is based on vulnerability exploits detection "xMiner". The process is structured from multi-order Markov process and Principal Component Analysis (PCA). These features gives a light weight design for fast, well maintained and high performance structure when SIP packet are active in the network . This means that, the detection procedure may provide effective defense against this type of attacks.

Taber *et al*. (2010), took a different method of testing the vulnerability that were caused by attacks. In the implemented fuzzer framework, two open source SIP-based soft-phones were tested and their various security vulnerabilities were identified. The number of vulnerabilities found showed that extensive security tests with additional scenarios and variations are required for soft-phone applications.

The current version of the implemented fuzzer framework produces several false-positive results. Improvement of the accuracy of the fuzzer test to reduce the time required for manual analysis is necessary for future versions.

The QoS is studied in (Liu and Li, 2010) using Network Simulator two (NS2). Packet loss and low-bandwidth lead the VoIP communication to low quality. This study shows the real-time occurrence by Botnet DDoS and shows also the observation of the packet loss rate and the calculation of the packet delay time using the experimental data. The Trojan and Social engineering Intrusion PC is used in this study highlighting the active threat which happened during the signaling session. The real-world Botnet, DDoS and the capacity for queue loading are simulated using NS2.

Sawda *et al.* (2010), described Data integrity and confidence deployed in SIP session management. They realized attacks are commonly executed through spoofing and hijacking, besides malicious SIP messages, which are also possible sources of unauthorized access or DoS. The authors also review the related study necessary for SIP security and concluded that IP traffics must be fixed within the enterprise to substitute for traditional PBX.

Liancheng and Ning (2009), clarified the necessity for sufficient SIP components to address common attacks on SIP, such as registration hijacking, proxy impersonation, DoS and spam. The authors believed that VoIP security involves several aspects of protocol, network equipment, code writing, operating system security, user security awareness and many other aspects. Their study presents a brief and useful reference for SIP attacks.

Zi-Fu *et al*. (2010), figure out a different approach in dealing with other SIP attacks.The authors used a unique approach to mitigate DoS flooding attacks, which depends on weighted fair queues. In brief, weighted fair queues use the min-max-fair-share algorithm to distribute packets, which means that the network OS will equally distribute minimum resources for each type of packet. The max fair-share means the network OS will provide more resources for packets that need to transfer large amount of data at that moment, but it will take the resource back after transfer. "Weighted" means that the scheduler will assign weight for each type of packet. The weight will determine how to queue and serve the packet. The classified SIP messages in Custom Weighted Fair Queue (CWFQ) are divided into INVITE SIP and non-INVITE SIP messages. Further, these SIP messages are put into different queues, so the CWFQ can classify the non-INVITE message established transactions (e.g., 100, 180, 200, ACK, BYE and so on) from the messages composed of proper SIP and INVITE flooding attack messages. Legal INVITE messages can be processed fast because the proportion of legal INVITE messages is usually smaller than that of illegal INVITE messages. Thus, because illegal INVITE messages are allocated to the low priority queue, illegal INVITE messages are likely to be discarded when the SIP server has higher usage of resources and outage overtime.

Liu and Li (2010), implement Network Simulator (NS2), this tool simulating the SIP Distributed Denial of Services (DDoS) attack. Further, on the network topology, the attack simulated over UDP and found that the rate of packet loss was 0%. After simulations with DDoS attacks were performed, the percentages for packet losses were obtained at 14.6 and 26.13%. This study analyzes a variety of DDoS attacks carried out by NS2 simulation.

Chen *et al*. (2009), described man-in-the middle (MitM) attacks through SIP by using the SIP VoIP communication model called triangle communication model. In particular, their study analyzed the relationship between the elements in the model. The entities were classified into two types: SIP user agent and SIP server. The model was also tested for MitM-DoS attacks to determine whether or not MitM can easily inject into the communication by tricking the SIP user agent into communicating with him rather than each other. Finally, the authors examined whether or not the formal model can cause man-in-the middle attacks using BYE and CANCEL options. The SIP VoIP triangle module can be widely used to reduce MitM attacks.

Takahara and Nakamura (2010), come out with a new mechanism for verification, called SIP Parameter for Verification Method (SPVM). It has extended from a combination between Proxy Authentication and SIP Identity to insure the integrity, where not much efforts are needed at the UA part. In addition, this mechanism is able to ensure an end-to-end integrity, within call flows bypassing a user-level Public Key Infrastructure (PKI). The normal secret session which it agrees at inter-domain using Secure Real-time Transport Protocol (SRTP) does ensure an integrity using fingerprint while a call flow at an intra-domain does not. Therefore, no MitM prevention will be occurring. In order to overcome the MitM attacks, the proposed mechanism ensure integrity in the intra-domain within a call flow. This mechanism was applied between UAC and the proxy within UAC part on one hand and between the UAC and UAS sides on the other hand. The SPVM can ensure an end-to-end media security thus can provide a VoIP service with high security.

**Social threat:** Ono and Schulzrinne (2009), describes a solution which is known as SPIT prevention. The authors addressed this issue by proposing two solutions. First, when the potential caller wants to call someone

from a contact list, the name list will appear as a suggestion to the caller. Organizations and companies that use SIP-supported lines are known to have their domain names in their extensions. The spammer can take the domain and send spam messages to the SIP server through his knowledge of the domain name. A solution can be found by using hashed contact addresses with Hypertext Transfer Protocol Security to prevent other suggested SIP contacts from appearing on the list. As a result, the routable contact address between caller and call recipient becomes more secure. The second involves the use of the technique called Weakly-Secret Information. A combination of these two techniques will produce significant results.

D'Heureuse *et al*. (2009), deployed anti-SPIT solution from one side to the other side on their prototype namely (Policy Decision Point). The solution can work with SIP-PBX. Their result shows mitigation of Spam over IP telephony.

**Interruption of service:** Description of other threats in VoIP.

Provides quality of VoIP service through a specific policy that reduce data trafic. Furthermore, they gave explanation of the variety of Highly unusual VoIP traffic caused from SIP attacks, several propsed in literature (Wu *et al*., 2009; Lee *et al*., 2011; Kyungtae *et al*., 2011; Sisalem, 2011; Kaarthick *et al*., 2011). Intrusion detection plays a good rule for monitoring and detecting threats that are not trivail (Asgharian *et al*., 2011). An extensive research for detection types must be provided to secure operation of dynamic VoIP applications, such as firewalls, NATs and VoIP traffic problems.

Thanthry *et al*. (2009), proposed a new encryption scheme, which however, use PKI architecture for both authentication and key exchange. In addition, it encrypts the real-time traffic by applying a unique key for packet using symmetric algorithm. The complexity of this algorithm is less than traditional algorithms such as SRTP and ZRTP. However, the first authentication and call setup delay are expected to be higher. The analyzed end-to-end call delay was studied, while the first call setup and network delays have not been calculated. Alternate Encryption scheme have relied on PKI architecture, also to be maintained. This study has been done using simulation with Advanced Encryption Standerd (AES). Furthermore, it can be analyzed by using Non-PKI architecture for exchanging first key and can be explored for fast authentication. Yoon *et al.* (2010) analyzes the security of VoIP communication on SIP-based environment by analyzing the RFC 4568 using SRTP with Key Management Protocol, also a novel scheme proposed to tighten security. TLS protocol applied to all routing between sender and receiver to find the baiting attack which occurs with RFC 4568. As a result, one needs to consider a new scheme for ensuring high levels of security.

**Miscellaneous issues:** Salgarelli *et al*. (2011), proposed a secure methodology between SIP proxies and their UAC through overlay networks. Several chain servers were secured through Distributed Hash Table (DHT), the servers are located on P2P-SIP. They secure media session in their solution. It was noticed that their proposal can offer availability and reduce the latency for P2P-SIP.

Matejka *et al*. (2004) described the prevention of attacks in VoIP architecture for the noticeable problem for TELECOM operators, when it migrated from telephony service to Voice over IP. This study described some techniques such as security architecture of VoIP related solution. This study aimed to list the current important projects involved in this area such as VoIP Honeypot Projects, Free SWITCH project and Session Border Controller (SBC) using OpenSBC project.

A SIP Service Monitoring Scheme (SSMS) has been designed and implemented in (Yang and Li, 2009), this scheme includes a Service Detection System (SDS) and Real-time Alert System (RAS). Increased credibility come from the quality testing of this service using (SDS). This scheme with a real-time alert system can produce information to the service provider to confirm the alarm message.

An advantage of this system is that, it has the ability to work with IPv4 and IPv6 networks, also able to know the status automatically by making simulated calls. In addition, the system can enable the administration to pinpoint the performance of the server and restart the server remotely. Finally, the SSMS provides a real-time SIP server performance status and is able to resolve some problem.

Carmo *et al*. (2011), provided an architectural design with an open-source implementation of a VoIP SIP-specific honeypot defined as Artemisa. The Honeypot software infrastructure has analysis tools, post-processing and SPIT call analysis. It is used for VoIP SPAM mitigation, signatures collection and Real-time closed-loop control of the domain security policy. As a result, the proposed testbed shows a impressive SIP security monitoring.

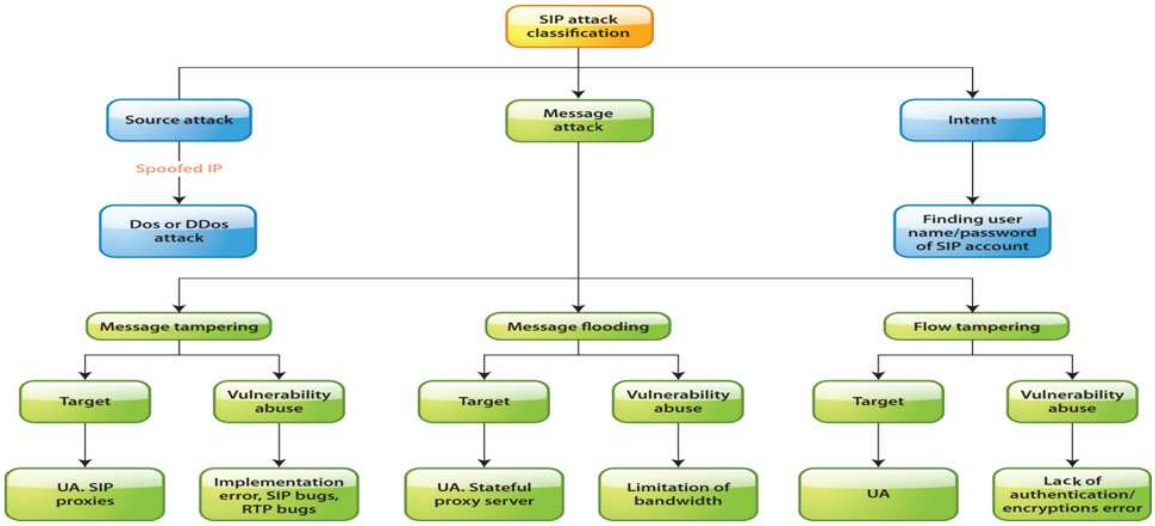


Fig. 3: SIP attack classification

It was proposed to build a security gateway in (Li *et al*., 2011). This gateway is used for enhancing UAs security and to set up secure sessions with the other SIP users. Result show that, the author prototype emphasizes on secure SIP mobility session, monitoring and prevents call interception. This is the concern of SIP privacy. Lin *et al*. (2011), introduced a privacy-aware SIP (PA-SIP) for enhancing VoIP communication security, PA-SIP is an extension for SIP used to detect and isolate the inner malicious nodes based on reputation mechanism.

In addition, the author analyze the performance of the security limits of PA-SIP. Due to the little effort that goes to VoIP over Wireless Mesh Networks (WMNs), the authors chose the WMN as a platform for this work. Network Simulator 2 (NS2) is used to test the performance of this study. This study shows the investigation on privacy security challenges with SIP for VoIP over WMN. Furthermore, the authors proposed a subjective logic based trust approach for SIP session privacy protection.

**Summary:** A brief investigation has been carried out on the SIP security issues. Through this study, a comprehensive classification of SIP attacks can be made. The classification has been depicted in Fig. 3. From this figure, it is clear that message attacks are the most dominant form of SIP attacks. Different types of message attacks are so common that, additional classification of such attacks can be carried out. It is strongly believed that, the discussion and classification presented here will give the security experts and researchers useful clues about implementing robust security architectures for SIP.

## CONCLUSION

IP is not an easy signaling protocol to secure. A discussion of some present solutions for SIP security malfunctions consisting of implementations and simulations is presented in this study. The SIP security solutions identified suggest that security mechanisms cannot provide 100% protection against SIP attacker, but threats can be mitigated significantly. A number of studies were reviewed and some common problems and their solutions were presented. Several SIP security solutions were found to be ultimately related to device security. The solutions presented here are not achieved by securing a single protocol but should involve the whole system.

## ACKNOWLEDGEMENT

We would like to express our gratitude to Prof. Dr. Sureswaran Ramadass, Director of National Advanced IPv6 Centre, Universiti Sains Malaysia for his kind support.

## REFERENCES

Akbar, M.A. and M. Farooq, 2009. Application of evolutionary algorithms in detection of SIP based flooding attacks. Proceedings of the 11th ANNUAL Conference on Genetic and Evolutionary Computation, July 08-12, ACM New York, N.Y. USA., pp: 1419-1426. DOI: 10.1145/1569901.1570092

Ali, S., S. Saharudin and M.R.B. Wahiddin, 2009. Quantum key distribution using decoy state protocol. Am. J. Eng. Applied Sci., 2: 694-698. DOI: 10.3844/ajeassp.2009.694.698

Asgharian, Z., H. Asgharian, A. Akbari and B. Raahemi, 2011. A framework for SIP intrusion detection and response systems. Proceedings of the International Symposium on Computer Networks and Distributed Systems, Feb. 23-24, IEEE Xplore Press, Tehran pp: 100-105. DOI: 10.1109/CNDS.2011.5764552

Aslam, J., S. Rafique and S. Tauseef-ur-Rehman, 2004. Analysis of real-time transport protocol security. Inform. Technol. J., 3: 311-314.

Carmo, R.D., M. Nassar and O. Festor, 2011. Artemisa: An open-source honeypot back-end to support security in VoIP domains. Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, May 23-27, IEEE Xplore Press, Dublin, pp: 361-368. DOI: 10.1109/INM.2011.5990712

Cerf, V.G., 1998. I remember IANA. Commun. ACM, 41: 27-28. DOI: 10.1145/290133.29014

Charnsethikul, P., 2006. Computational discrete time markov chain with correlated transition probabilities. J. Math. Stat., 2: 457-459. DOI: 10.3844/jmssp.2006.457.459

Chen, Z., S. Guo, K. Zheng and H. Li, 2009. Research on man-in-the-middle denial of service attack in SIP VoIP. Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, Apr. 25-26, IEEE Xplore Press, Wuhan, Hubei, pp: 263-266. DOI: 10.1109/NSWCTC.2009.326

Coulibaly, E. and L.H. Liu, 2010. Security of VoIP networks. Proceedings of the 2nd International Conference on Computer Engineering and Technology, Apr. 16-18, IEEE Xplore Pree, Chengdu, pp: V3104-V3108. DOI: 10.1109/ICCET.2010.5485790

Cui, X., Y. Zhang, W.J. Lee and S.J. Koh, 2010. SIP-based IM and its security solutions. Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing, Sep. 23-25, IEEE Xplore Press, Chengdu, pp: 1-4. DOI: 10.1109/WICOM.2010.5601309

D'Heureuse, N., J. Seedorf and S. Niccolini, 2009. A policy framework for personalized and role-based SPIT prevention. Proceedings of the 3rd International Conference on Principles, Systems and Applications of IP Telecommunications, Jul. 07-08, ACM, Atlanta, GA, USA. DOI: 10.1145/1595637.1595653

Dawes, P., 2011. Capability exchange for media plane security. IETF.

Femminella, M., R. Francescangeli, F. Giacinti, E. Maccherani and A. Parisi *et al*., 2009. Design, implementation and performance evaluation of an advanced SIP-based call control for VoIP services. Proceedings of the IEEE International Conference on Communications, Jun. 14-18, IEEE Xplore Press, Dresden, pp: 1-5. DOI: 10.1109/ICC.2009.5198905

Hussain, I. and F. Nait-Abdesselam, 2011. Strategy based proxy to secure user agent from flooding attack in SIP. Proceedings of the 7th International Conference Wireless Communications and Mobile Computing, Jul. 4-8, IEEE Xplore Pree, Istanbul, pp: 430-435. DOI: 10.1109/IWCMC.2011.5982572

Kaarthick, B., N. Nagarajan, E. Raguvaran and G. Saimethun, 2011. Subchannel allocation and mapping algorithms for improving the QOS of VoIP traffic in IEEE 802.16e networks. Comput. Netw., 55: 3672-3679. DOI: 10.1016/j.comnet.2011.04.022

Karopoulos, G., G. Kambourakis and S. Gritzalis, 2011. Privasip: Ad-hoc identity privacy in SIP. Comput. Stand. Int., 33: 301-314. DOI: 10.1016/j.csi.2010.07.002

Keromytis, A.D., 2009. A survey of voice over IP security research. Inform. Syst. Secu., 5905: 1-17. DOI: 10.1007/978-3-642-10772-6_1

Kyungtae, K., N. Drago and H. Sangjin, 2011. Gateway strategies for VoIP traffic over wireless multihop networks. KSII Trans. Internet Inform. Syst., 5: 24-51.

Lee, K.W., J.W. Ji, S.J. You and G. Lee, 2011. Abnormal traffic detection system of VoIP based on SIP. Conv. Hybrid Inform. Technol., 6935: 496-504. DOI: 10.1007/978-3-642-24082-9_61

Li, J.S., C.K. Kao and J.J. Tzeng, 2011. VoIP secure session assistance and call monitoring via building security gateway. Int. J. Commun. Syst., 24: 837-851. DOI: 10.1002/dac.1191

Liancheng, S. and J. Ning, 2009. Research on security mechanisms of SIP-based VoIP system. Proceedings of the 9th International Conference on Hybrid Intelligent Systems, Aug. 12-14, IEEE Xplore Press, Shenyang, pp: 408-410. DOI: 10.1109/HIS.2009.196

Lin, H., A. Ye and K. Yang, 2011. PA-SIP: A privacy-aware SIP for VoIP over wmns. Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing, Sep. 23-25, IEEE Xplore Pree, Wuhan, pp: 1-4. DOI: 10.1109/wicom.2011.6040159

Liu, Z.H., J.C. Chen and T.C. Chen, 2009. Design and analysis of SIP-based mobile VPN for real-time applications. IEEE Trans. Wireless Commun., 8: 5650-5661. DOI: 10.1109/TWC.2009.090076

Liu, C.H. and Y.S. Li, 2010. The study of botnet attack on VoIP. Proceedings of the 6th International Conference on Networked Computing and Advanced Information Management (NCM), Aug. 16-18, IEEE Xplore Press, Seoul, pp: 636-640.

Liu, X. and J. Xu, 2010. A mechanism of authentication for P2P-SIP overlays. Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing, Sep. 23-25, IEEE Xplore Press, Chengdu, pp: 1-4. DOI: 10.1109/WICOM.2010.5601329

Mehta, A., N. Hantehzadeh, V.K. Gurbani, T.H. Ho and J. Koshiko *et al*., 2011. On the inefficacy of euclidean classifiers for detecting self-similar Session Initiation Protocol (SIP) messages. Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, May 23-27, IEEE Xplore Press, Dublin, pp: 329-336. DOI: 10.1109/INM.2011.5990708

Murty, M.N. and V.S. Devi, 2011. Hidden markov models. Patt. Recog., 0: 103-122. DOI: 10.1007/978-0-85729-495-1_5

Matejka, L., A. Strachota, J. Plestil, P. Whelan and M. Steinhart *et al*., 2004. epoxy networks reinforced with Polyhedral Oligomeric Silsesquioxanes (POSS). Structure and morphology. Macromolecules, 37: 9449-9456. DOI: 10.1021/ma0484577

Ni, L., G. Chen and J. Li, 2011. A pairing-free identity-based authenticated key agreement mechanism for SIP. Proceedings of the International Conference Network Computing and Information Security, May 14-15, IEEE Xplore Press, Guilin, pp: 209-217. DOI: 10.1109/NCIS.2011.49

Ono, K. and H. Schulzrinne, 2009. Have I met you before?: Using cross-media relations to reduce SPIT. Proceedings of the 3rd International Conference on Principles, Systems and Applications of IP Telecommunications, Jul. 07-08, Atlanta, GA, USA., pp: 1-7. DOI: 10.1145/1595637.1595641

Salgarelli, L., G. Bianchi and N. Blefari-Melazzi, 2011. Trustworthy Internet. 1st Edn., Springer, London, ISBN: 884701817X, pp: 369.

Sawda, S.E., P. Urien and R.E. Sawda, 2010. A trust communication with SIP protocol. Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, May 16-19, IEEE Xplore Press, Hammamet, pp: 1-6. DOI: 10.1109/AICCSA.2010.5587028

Schulzrinne, H. and J. Rosenberg, 2000. The session initiation protocol: Internet-centric signaling. IEEE Commun. Mag., 38: 134-141. DOI: 10.1109/35.874980

Sisalem, D., 2011. SIP overload control: Where are we today? Trustworthy Internet. DOI: 10.1007/978-88-470-1818-1_21

Srivastava, S., 2011. Extensions to SIP signalling to indicate spam. FPO.

Stefanec, T. and I. Skuliber, 2011. Grammar-based SIP parser implementation with performance optimizations. Proceedings of the 11th International Conference on Telecommunications, Jun. 15-17, IEEE Xplore Press, Graz, pp: 81-86.

Shen, Y., Z. Wan, C. Coarfa, R. Drabek and L. Chen *et al*., 2010. A SNP discovery method to assess variant allele probability from next-generation resequencing data. Genome Res., 20: 273-280.

Taber, S., C. Schanes, C. Hlauschek, F. Fankhauser and T. Grechenig, 2010. Automated security test approach for SIP-based VoIP softphones. Proceedings of the 2nd International Conference on Advances in System Testing and Validation Lifecycle, Aug. 22-27, IEEE Xplore Press, Nice, pp: 114-119. DOI: 10.1109/VALID.2010.20

Takahara, H. and M. Nakamura, 2010. Enhancement of SIP signaling for integrity verification. Proceedings of the 10th IEEE/IPSJ International Symposium on Applications and the Internet, Jul. 19-23, IEEE Xplore Press, Seoul, pp: 289-292. DOI: 10.1109/SAINT.2010.33

Thanthry, N., G. Gopalakrishnan and R. Pendse, 2009. Alternate encryption scheme for VoIP traffic. Proceedings of the 43rd Annual International Carnahan Conference on Security Technology, Oct. 5-8, IEEE Xplore Press, Zurich, pp: 178-183. DOI: 10.1109/CCST.2009.5335543

Wu, L., Y. Zhang and F. Wang, 2009. A new provably secure authentication and key agreement protocol for SIP using ECC. Comput. Stand. Interfaces, 31: 286-291. DOI: 10.1016/j.csi.2008.01.002

Yang, X. and H. Li, 2009. Research of a service monitoring system based on SIP in hybrid network. Proceedings of the 9th International Conference on Hybrid Intelligent Systems, Aug. 12-14, IEEE Xplore Press, Shenyang, pp: 449-452. DOI: 10.1109/HIS.2009.206

Yoon, S., H. Jung and K.S. Lee, 2009. A study on the interworking for SIP-based secure VoIP communication with security protocols in the heterogeneous network. Security Technol., 58: 165-175. DOI: 10.1007/978-3-642-10847-1_21

Yoon, S., J. Jeong and H. Jeong, 2010. A study on the tightening the security of the key management protocol (RFC4568) for VoIP. Proceedings of the 4th International Conference on New Trends in Information Science and Service Science, May 11-13, IEEE Xplore Press, Gyeongju, pp: 638-641.

Zhu, Y. and H. Fu, 2011. Traffic analysis attacks on skype VoIP calls. Comput. Commun., 34: 1202-1212. DOI: 10.1016/j.comcom.2010.12.007

Zi-Fu, F., Y. Jun-Rong and W. Xiao-Yu, 2010. A SIP dos flooding attack defense mechanism based on custom weighted fair queue scheduling. Proceedings of the International Conference on Multimedia Technology, Oct. 29-31, IEEE Xplore Press, Ningbo, pp: 1-4. DOI: 10.1109/ICMULT.2010.5630386