A Survey of Security Weakness of Session Initiation Protocol (SIP)

Ihsan Ilahi Jan, Prof. Adeel, Shahzad Rizwan, Waseem Khan, Junaid Khan, Qazi Ahmad Faraz, Fayyaz Gul, Rashid Zubair, Abdul-Sattar, Usman and Shahzad hameed

Gandhara University of Sciences, Peshawar, Pakistan

Abstract– **SIP stands for session initiation protocol and it is a signaling protocol bring into play for scheming communication session. For example for video calls and voice calls on internet protocol and because of the open/unlock organization the Internet and the exercise of open/unlock standards such as Session Initiation Protocol embody the stipulation of services similar to file relocation, incidence information, instant messaging are unprotected to recognized Internet thumps and assaults and at the comparable position commencing fresh safety measures troubles found on such standards cannot been fit into place in with nearby security/defense methods. The portion of scripting distinguishes and elucidates fortification destructions in the Session Initiation Protocol that may possibly guide towards negative response/rejection of services. Such like sanctuary impairments hold parser implementation, security vulnerabilities/weakness, flooding assaults and assail exploiting weakness at the signaling application level. A concise scrutiny of such security deficiency and theirs effects on Session Initiation Protocol systems are presented.**

Keywords– Survey, Security, SIP and Issues

I. INTRODUCTION

At present we have countless applications of the Internet that entails the conception and supervision of a session, however a session is well thought-out a switch over of data among associations of participants. The accomplishment of such sort of applications is problematical by the practices of contributors: customers may possibly be in motion among endpoints, they may be addressable by manifold/multiple names, and they may possibly communicate in several dissimilar media - frequently simultaneously.

Numerous protocols have been authored that bear various forms of real-time multimedia session data such as voice, video, or text messages. The Session Initiation Protocol (SIP) takes part in concert with these protocols by facilitating Internet endpoints (called user/client negotiator/agents) to find out one another and to consent on a categorization of a session they would love to share. For tracing forthcoming session contestants, and for other tasks, session initiation protocol permits the formation of an infrastructure of network hosts called proxy servers through which client/user agents or negotiators are able to transmit registrations, invitations to sessions, and some other additional requests. SIP is an agile, general purpose tool for constructing, altering, and ceasing sessions that toils autonomously of fundamental transport protocols and without enslavement on the type of session that is being established. [1]. Voice over Internet Protocol (VoIP) has been hastily employed in topical years, just because of its minor cost and superior suppleness comparing to Public Switched Telephone Networks. Before a VoIP call can take place, signaling protocols ought to be employed to ascertain a session, and to uphold and conclude the established session. Currently a dominant VoIP signaling protocol is the Session Initiation Protocol (SIP) developed by the Internet Engineering Task Force, and the arrangement of Session Initiation Protocol is therefore available in Request for Comments 3261. Besides its increasing popularity in VoIP, the SIP has been approved by the third Generation corporation mission/project as a signaling protocol and permanent element of the IP Multimedia Subsystem architecture (Sparks 2007). Multimedia information tends to attract more attentions and raise curiosities from intruders as people are keen on viewing and hearing communications. More importantly, VoIP protocols, including SIP, were designed without serious security concerns in mind, and the unlock/open structural design of the Internet crafts assaults easier. Consequently, alongside with the prevalent exploitation of VoIP, its security flaws have emerged and become a problem being addressed, in the exploitation of Voice over IP systems, and in the research and development of VoIP techniques. Safety measures of SIP Protocol have been scrutinized with an immense pact recently. Many intrusion detection methods and security countermeasures have been proposed most articles discuss or identify SIP security holes through critical reviews or experiments of typical SIP application scenarios. Evaluations of proposed detection methods and countermeasures largely rely on experimenting with real VoIP networks or test beds. Some of the intrusion detection systems make use of formal methods, such as communication state machines. However, to our best knowledge, little work has been done on using formal methods to systematically and comprehensively analyze security vulnerabilities of the SIP specification in RFC 3261. Although SIP has been widely deployed, its cram/study safekeeping/defense is yet unripe. So it is important to not only look into security problems and solutions for SIP-based networks, but in addition to carry out ceremonial sanctuary examination of SIP design. Further prominently security scrutiny based on research only are not all-inclusive, as we cannot test each and every possible scenario, unlike machinist/operator networks may possibly have diverse settings, and the implementations of SIP may not be the same. On the other hand, formal methods, such as Coloured Petri Nets (CPNs) (Jensen 1997, Jensen et al 2007), allow more complete analysis results and us to obtain rigorous. Coloured Petri Nets have been thereby functionalized extensively in substantiating communication protocols, business processes, and some other systems. In this paper, we apply and further develop the basic idea in (Nieh and Tavares 1993) for verifying cryptographic protocols, for security examination of SIP. The slant shaped in this paper, and our prospect work, are endeavored at all-inclusive and ceremonial sanctuary/security investigation of its design, to provide theoretical prop up to acknowledged security hazards, and to ascertain innovative protection fissures of SIP. Another goal of our work is to use the CPN models for SIP and the intruders as a platform to evaluate security countermeasures of SIP [2].

II. SIP ARCHITECTURE

SIP concern architecture is delineated in Request for Comments 3261 and has resemblance with two additional Internet application protocols, SMTP and HTTP. It utilizes the TCP/IP & UDP for the fundamental network infrastructure, just like SMTP and HTTP. It can, however, exploit any further transport too, Transport Layer Security (TLS) for the SIP system, for example. From an architecture standpoint, SIP network physical components can be clustered into two classes: one is client and the other is server. The figure underneath exemplifies the concern architecture of Sip's network.

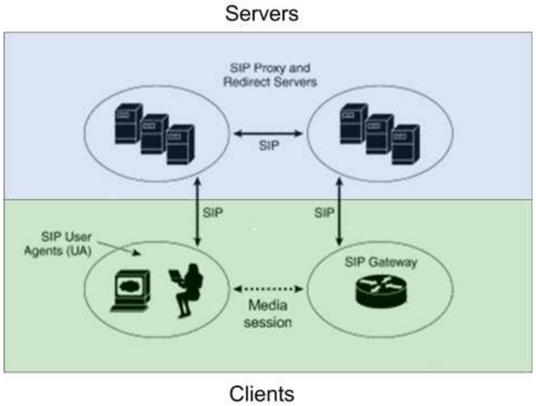

Fig. 1: SIP Architecture

- ***SIP clients***

Phones, which can act as either a user agent server (UAS) or user agent client (UAC). Softphones (PCs that have phone capabilities installed) and SIP IP phones can initiate SIP requests and respond to requests. Gateways, that endows by means of call control. Gateways provide many services, the mainly familiar being a transformation function among Sip's conferencing endpoints and some other terminal sorts. This function consists of translation among different communication/transmission formats and communications procedures. In addition, the gateway carries out call setup and defrayal on both the Local Area Network side and the circuit switching networks.

- ***SIP servers***

Redirect Server: Redirect server's purpose is to convey the request back to the customer, which points out that the customer, requires attempting a diverse direction to acquire to the recipient. It only occurs when a receiver has moved about from its unique location.

Proxy Server: When a request is produced/generated, the recipient literal address is not acknowledged in advance, which leads the user to propel the request to the concern proxy server. The server then promotes the request to an additional proxy server from the side of the user or either by the recipient itself.

Registrar: Its principal function is to sense the position of a customer in that particular network. This spot/location is identified by customers having to index their concern locations to this Registrar server. Customers invigorate their positions from time to time by indexing (by means of transmitting a unique message) to a Registrar server.

Location Server: Accumulates those addresses which have been employed by the Registrar server [3].

III. SIP SECURITY MECHANISMS ANALYSIS

As stated above, the HTTP digest authentication algorithm is currently the most frequently deployed security mechanism with SIP. This authentication scheme can offer one-way message authentication and replay protection but cannot support message integrity and confidentiality. According to RFC 3261[4], it is promising for a spiteful customer to consign Spam calls. Moreover, this method is vulnerable due to the use of plaintext, which facilitates MITM assaults, as both the plaintext (challenge) and the cipher text can be easily captured by a potential aggressor simply by sniffing the network traffic. Digest authentication also requires some sort of prearranged trusted environment for password distribution. Passwords may be Stored either in plaintext or cipher text form at the server side. However, cipher text is not capable of providing an enhance level of sanctuary level, since it is feasible to compute the message credentials by launching a brute force attack on the encrypted password. Besides, due to the absence of any correlation between the user name and the SIP URIs, a malicious user may masquerade itself as a legitimate user. Recently, an assortment of solutions has been recommended [5], [6] to recover of such limitations found in the HTTP Digest mechanism. Nevertheless, it is stressed that such solutions require modifications in the SIP user agent, which of course is not always easy to implement. Furthermore, considering that there is no authorization model, it is possible for an attacker to gain access to services that are normally available to legitimate users only. Another important issue is that the intermediate SIP proxies cannot be certain that the SIP UA has been authenticated. It has already been suggested in [7] that SIP messages must include a cryptographic token to confirm that the originating user's identity has been verified by the corresponding network. Performance issues are also reported for authentication procedures. Simulations showed that they highly strain SIP servers' performance [8].

In relation to authentication issues, it is of equal importance to protect the user's personal information and his real identity providing anonymity, privacy, and location privacy. SIP UAs can support anonymity by obscuring the From: head-er contained in SIP requests. However, not all headers can be obscured. For instance, the Contact: header is required for request routing and cannot be protected. Consequently, a satisfying level of privacy is not possible without adequate support from the SIP proxy infrastructure. As suggested in [9], the privacy service can be implemented in a proxy server that can also act as a back-to-back UA and proxy media streams. As mentioned above, the protection offered by Ipsec assumes pre-established trust among the communicating par ties and it can only be utilized in a hop-by-hop fashion. Since IPsec is implemented at the operating-system level, most SIP clients do not implement this protocol yet. For this reason, IPsec can only protect the traffic between the corresponding network servers. Moreover, SIP specifications do not suggest any framework for key administration, which is required by the Internet Key Exchange (IKE) part of the IPsec protocol. However, recently has been suggested a draft describing the corresponding requirements for IPSec negotiation in SIP [12]. In contrast to IPsec, TLS does not assume any trust relation among communicating parties. TLS can be utilized either for one-way or mutual authentication schemes and maybe it is the Internet Key Exchange (IKE) part of the IPsec protocol. However, recently has been suggested a draft describing the corresponding requirements for IPSec negotiation in SIP [12].

In contrast to IPsec, Transport Layer Security does not presuppose any sort of confident relation among communicating/exchanging parties/groups. TLS can be utilized either for one-way or mutual authentication schemes and maybe it is more suitable for inter domain authentication. Of course, there is always the risk that the message can be intercepted inside the recipient's network assuming that the last hop is not encrypted. Additionally, TLS is utilized by the Sip's system or plan to put forward an end-to-end protection. However, TLS fails to deliver end-to-end security as, at least until now, no mechanism exist to ensure that along the whole path from the source to the destination in a hop-by-hop fashion TLS is utilized by all the involved parties. Recently, some security requirements and directions for providing such a mechanism have been suggested [10]. Moreover, TLS protects only connection-oriented protocols. To put it simply, the lack of PKI in VoIP does not offer the appropriate environment for the utilization of TLS. S/MIME is exercised to hold up either or moreover reliability or privacy/confidentionality in an end-to-end approach.

It should be noted that S/MIME adds considerable overhead in SIP messages. More importantly, the integrity and confidentiality of the entire SIP message cannot be protected due to the existing restriction of header modification as the intermediate nodes ought to have entrée to the Session Initiation Protocol header to practice/process and route or direct the SIP message to the suitable and concern destination. Finally, as in the TLS case, the absence of PKI is an additional restriction for the operation of S/MIME in SIP. Apart from the abovementioned restrictions, in some cases, security services may require the combination of TLS and S/MIME. This includes the usage of TLS to support integrity and authentication, while S/MIME is used to provide mainly privacy for some parts of the transmitted data. However, some SIP intermediaries (e.g., servers) may require reading these data. This state/condition entails to have a protection mechanism/method to make safe message bodies and/or headers between proxy servers and the User Agents, while at the same time revealing information to those that actually need it. This is called an "end-to middle security." Security requirements for "end-to-middle" security" can be found in [11].

IV. QUALITATIVE ANALYSIS

The potential threats and attacks that a SIP-based network is facing can be divided into various known security categories:

• *Passive versus active attacks:* Passive attacks include the passive monitoring of packets exchanged among the SIP elements. On the other hand, in the active attacks the attacker may disrupt the normal operation of the network by altering, deleting, or retransmitting packets.

• *Internal versus external attacks:* The external Attacks regard attacks that stem from nodes, which do not belong to the SIP network. On the other hand, internal attacks regard malicious nodes belonging to the network as legitimate entities.

• *Single versus multisource(s):* Single-source attacks involve one malicious host (the attacker). On the other hand, multi sources involve numerous of possible innocent Internet hosts that have been exploited by the attacker.

• Vulnerability: Before launching an attack, attackers will try to discover possible vulnerabilities that can be exploited to gain access or cause a security problem in the target system.

• *Affected security issues:* Whenever an attack is launched, the affected security mechanisms are the following: (C)onfidetiality, (I)ntegrity, (Av)ailability, (R)eliability, (Au)thentication.

• *Consequences:* This category differentiates the attacks based on the intentions of the intruder:

–DoS attacks intend to make servers unavailable to accomplish their tasks.

–Unauthorized Access (UnA) as its name implies, intends to give access in the provided service to non-authorized users.

• *Attack class:* This category classifies attacks based on the different sort of the attack which is utilized in order to cause a security problem. We distinguish the aforementioned attacks in the following three general classes:

–Flooding attacks
*Registrar, proxy, end-user
–Parser attacks
–Application-level attacks
*Signaling-based attacks
(Route, record route, bye, cancel)
*SQL Injection

This categorization figures out the main security problems for the presented attacks that an attacker can exploit. In contrast to PSTN, an attacker may easily access SIP sub-systems and alter/deteriorate its operations. Thus, he can easily discover any appropriate parameters needed to launch an active or passive attack supposing that no underlying security mechanism is in place. For example, the aggressor may utilize well-known network tools, like ethereal, to eavesdrop on the required information. With some exceptions, most described attacks are active ones. More specifically, in signaling attacks (except the REFER one) the attacker is bound to act in passive mode, at least during the first steps of the attack, in order to eavesdrop the required information. Although it is difficult to launch such attacks from an external network, such a situation is not entirely improbable. On the other hand, in the case of the REFER attack, the impostor acts as man in the middle to be able to forge the response and transfer the caller in a malicious source. Regarding the SQL injection attack, the attacker is required to know only the user name which simply is public information. At the same time, concerning flooding attacks the attacker has a variety of alternatives to trigger a DoS. Some of the main components (presented above) that are vulnerable to this kind of attack are:

- Registrar
- Proxy
- End-user terminal

Furthermore, depending on the corresponding network bandwidth and other processing limitations as the case may be, this attack can be launched either from an internal or external network by utilizing one or more attackers acting as reflectors. Such attacks can cause a DoS to any of the aforementioned network element in just a few seconds [13]. In this context, parser attacks give the opportunity to adversaries either originating from an external or internal network to make an attempt to cause delays to the provided service or even at worst paralyze them by creating different malevolent messages as described previously). This situation is described in [14]. One of the main security vulnerabilities that attackers will possibly exploit is the lack of a complete authentication scheme, which can protect the SIP infrastructure against unauthorized access. One possible solution to this problem has been suggested in [7] for the utilization of cryptographic tokens. This solution can be also applied in hop-by-hop fashioned messages such as CANCEL (which cannot be challenged) and utilize HTTP Digest authentication. The second major problem is the lack of integrity mechanisms.

This problem can be fixed with the use of the appropriate integrity schemas (e.g., S/MIME, TLS, etc.). Moreover, the utilization of such mechanisms can assist the protection of signaling against eavesdropping attacks. However, the hop-by-hop nature of TLS and (partially) IPsec still remains as a major drawback, given that in every hop deciphering and reciphering is required. Moreover, the middle-to-end problem still remains. Another possible solution regarding the BYE signaling attack has been suggested in [15]. However such a solution is not entirely generic and thus it cannot be applied in any of the presented signaling attacks. To the best of our knowledge, no any other general solution has been suggested towards these problems.

Clearly, parser attacks utilizing malformed messages are very difficult to defeat by normal parsers as they are might lack sophisticated detection algorithms to identify and promptly discard such messages. A feasible and practical solution to this problem can be found in [14]. This solution has the advantage that it can also be applied to detect SQL injection attack as it is recommended in [16]. Another approach to circumvent the problem is the introduction of the aforementioned mechanism in the Middle Box Communication approach.

In addition, mechanisms like TLS, IPsec, and S/MIME are only able to protect against outsiders and not against insiders, who are normally legitimate users. Considering this situation, an outsider will endeavor to employ his SIP proxy in order to amplify the DoS effects of specially fabricated malformed, invalid, or nonstandard SIP messages towards the corresponding SIP target. Even more, a malicious insider may craft a SIP malformed message and then sign it with his private key. There is no doubt that such attack can be hardly defeated by utilizing only TLS, IPsec, S/MIME, or any other similar security mechanism.

V. CONCLUSION

In this survey we recognized and group a variety of SIP oriented intimidation, include flooding attacks Vulnerability in parser implemented, and attack Exploiting on signaling application level signaling- nevertheless, these sort of hit can also survive or be apply in other signaling protocols, such as h.323, MEGACO and so on. It is anxious that, no issue how well built the presented safety anticipation technique exist in present sip based VoIP services, their will forever the opportunity for a malevolent client to supervise to avoid them. Moreover, sip has evolved beyond VoIP. It is the accepted standard by both 3gpp and the next generation networks throughout the implementation of IP multimedia subsystem (IMS). The IMS manage design is presently implement SIP to manage extra sort of multimedia services e.g., video conferencing. Consequently, techniques are essential to make sure privacy, reliability, confidentiality, and legal interrupt in both 3G and NGN environment.

REFRENCES

[1] http://www.ietf.org/rfc/rfc3261.txt

[2] http://ro.ecu.edu.au/icr/8

[3] Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010.

[4] M. Garcia-Martin, "Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP)," May 2005, RFC 4083.

[5] C.-C. Chang et al., "Design and Implementation of SIP Security,"

[6] C.-C. Yanga, R.-C. Wangb, and W.-T. Liuc, "Secure Authentication Scheme for Session Initiation Protocol," Computers & Security (2005), vol. 24, pp. 381–86.

[7] J. Peterson, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol," Internet-Draft, Feb. 2003

[8] S. Salsano, L. Veltri, and D. Papalilo, "SIP Security Issues: The SIP Authentication Procedure and Its Processing Load," IEEE Network, vol. 16, Nov. 2002.

[9] J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)," RFC 3323, Nov. 2002

[10] J. Polk, "Requirements for Assured End-to-End Signaling Security within the Session Initiation Protocol," Internet Draft, July 2005.

[11] K. Ono and S. Tachimoto, "Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP)," RFC 4189, Oct. 2005.

[12] M. Saito and S. Fujimoto, "Requirements for IPsec Negotia- tion in SIP," Internet Draft, Oct. 2005.

[13] G. D. Kambourakis et al., "A Framework for Detecting Mal-formed Messages in SIP Networks," Proc. 14th IEEE Wksp. Local and Metropolitan Area Networks (LANMAN), ChaniaCrete, Greece, Sept. 2005.

[14] Y.-S. Wu et al., "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," Proc. 2004 Int'l. Conf. Dependable Systems and Networks (DSN'04).

[15] D. Geneiatakis et al., "SIP Message Tampering: THE SQL Code INJECTION Attack," Proc. 13th Int'l. Conf. Software, Telecomm. and Computer Networks (SoftCOM 2005) IEEE, Split, Croatia, Sept. 2005.

[16] P. Srisuresh et al., "Middlebox Communication Architecture and framework," IETF, RFC 3303, Aug. 2002.