SIP Security Mechanisms: A state-of-the-art review

Dimitris Geneiatakis, Georgios Kambourakis, Tasos Dagiuklas,
Costas Lambrinoudakis and Stefanos Gritzalis

Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, GR-83200 Samos, Greece
email: icsdm03001@icsd.aegean.gr

Abstract

The commercial deployment of VoIP necessitates the employment of security mechanisms that can assure availability, reliability, confidentiality and integrity. The Session Initiation Protocol (SIP) is considered as the dominant signalling protocol for calls over the Internet. SIP, like other Internet protocols, is vulnerable to known Internet attacks, while at the same time it introduces new security problems in the VoIP system. This paper lists the existing security problems in SIP and provides a brief description, followed by a critical analysis, of the security mechanisms it employs.

Keywords

Voice over Internet Protocol (VoIP), Session Initiation Protocol (SIP), Security Mechanisms.

1. Introduction

One of the main challenges that telecommunication providers are facing is the convergence of data and voice networks. The idea of utilizing data networks for transmitting voice was originally proposed in 1970 (Schulzrinne, 1999), while the Internet evolution has pressed telecommunications providers and Internet Service Providers (ISPs) to transmit Voice over the Internet Protocol (VoIP). VoIP has not only to provide similar to the PSTN services but also to achieve the same level of reliability, availability and security. As opposed to PSTN, VoIP utilizes one common network for signaling and voice and thus enjoys several advantages in relation to the telephony services that are offered (Varshney et al., 2002), albeit the fact that new network problems, like jitter, loss, and Quality of Services (QoS), are emerging. Moreover, signalling and voice are now exposed to various Internet known attacks.

Internet telephony uses a variety of signalling protocols, such as H.323, SIP, MGCP and MEGACO, for initiating VoIP calls. However, SIP seems to overwhelm all the others, mainly due to the fact that it has been adopted by various standardisation organisations (i.e. IETF, ETSI, 3GPP) as the protocol for both wireline and wireless world in the Next Generation Networks (NGN) era.

This paper introduces the VoIP related security problems, focusing on SIP security. The following section presents the general components of the SIP architecture. Section 3 addresses the security requirements and the possible threats and attacks in SIP, while it briefly

describes SIP's security mechanisms. Section 4 concludes the paper providing some pointers to future research work.

2. The SIP Architecture

2.1. The SIP protocol

SIP is an application-layer signalling protocol for creating, modifying, and terminating multimedia sessions with one or more participants (Rosenberg et al., 2002). A SIP message can either be a request or an acknowledgment to a request, consisting of the header fields and the message body. SIP messages are text-based and are similar to HTTP format. The message body is either used to describe session requirements or to encapsulate various types of signalling. SIP messages must also identify the requested resource, which corresponds to a unique address. SIP addresses follow the general form of HTTP addressing scheme; an example of a SIP address is *sip:dgen@aegean.gr*.

SIP REGISTER and INVITE messages are the pre-dominant messages used by the SIP protocol. SIP REGISTER (Figure 1a) is used for registering a user with a service, while SIP INVITE (Figure 1b) is used for inviting another user in a session. Like other similar Internet application protocols, SIP follows the Client-Server architecture. SIP Registrar and Proxy servers administrate SIP messages. The SIP Proxy server is responsible to routing all SIP messages to their destinations while SIP Registrar handles the registration service. It can be noticed that in Figure 1a the registration of user *'clam@sip.gr'* is successful, while the server rejects the SIP INVITE message in Figure 1b since prior to authenticate the client.

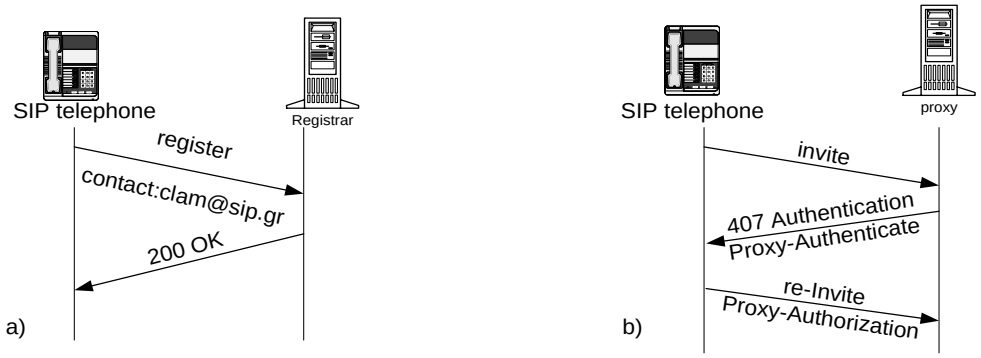

Figure 1: SIP message flows

Another important consideration concerning SIP methods is the SIP REFER one (Sparks, 2003). This extension provides a mechanism where one party (the referrer) provides a second party (the referee) with an arbitrary Uniform Resource Identifiers (URI) to reference. Assuming that this URI is a SIP URI, the referee will send a SIP request, often an SIP INVITE, to that URI (the refer target). As a result, SIP REFER can be used to enable many applications, including call Transfer. RFC 3892 [2] extends this method, allowing the referrer to provide information about the SIP REFER request to the refer target using the referee as an intermediary. The refer target can use this information to decide whether to accept the referenced request from the referee.

2.2. Supplementary SIP services

In the SIP architecture, there are several other components offering a number of complementary services. For instance, AAA services can be patronized by protocols such as RADIUS (Rigney et al., 2000) and DIAMETER (Calhoun et al., 2003) Furthermore, DNS and ENUM (Falstrom, 2000) can be utilized to resolve the mapping between the SIP URIs and E.164 telephone numbers to IP addresses. ENUM defines a method to convert an ordinary telephone number into a format that can be used on the Internet alias addressing information (such as, VoIP or e-mail addresses). The Internet addressing information of an ENUM number is stored within the DNS, providing instructions on how to reach a device associated with a particular ENUM number.

3. SIP Security

3.1. Security flaws in SIP

Security and privacy requirements in a VoIP environment are expected to be equivalent to those in PSTN, even though the provision of secure Internet services is much more complicated. SIP messages may contain information that a user or a server wishes to keep private. For example, the headers may reveal information about the communicating parties or other confidential information. The SIP message body may also contain user information (addresses, telephone number, etc) that must not be exposed. The open and distributed nature of the VoIP architectures, in conjunction with the variety of subsystems (ENUM, DNS, AAA) that the Internet telephony deploys, turns the establishment of a secure environment into an extremely difficult task.

The potential threats that a SIP-based network is facing can be divided into external and internal ones. External are the attacks launched by someone who does not participate in a SIP-based call and usually occur when signalling and data packets traverse untrustworthy network realms. For instance, VoIP suffers from all known attacks associated with any Internet application or subsystem. Table 1 illustrates some of the identified threats - attacks, their impact on the overall SIP security and a list of indicative solutions.

The most severe threat in a VoIP environment is probably the easy access to the communication channel. For instance, the existence of several Internet tools for analysing VoIP traffic, such as Ethereal (www.ethereal.com), makes eavesdropping a simple task for any potential perpetrator. Furthermore, the text-based nature of SIP messages gives more opportunities for attacks like spoofing, hijacking and message tampering (Rosenberg et al., 2002; Ofir, 2002a), as opposed to other VoIP protocols such as H.323 that follow ASN.1 syntax. The use of malicious SIP messages, is also a possibility and can cause unauthorized access or Denial of Service (DoS). Consider, for example, a malicious user who inserts a properly adapted SQL code in a SIP REGISTER message, inducing unauthorized changes in the location database (service). DoS is a major issue in SIP. For instance, forking proxies can amplify the traffic of an originator. This means that if this traffic is maliciously destined to a single machine, this machine will be easily become unavailable.

SIP protocol according to RFC 3261 utilizes transport protocols such as TCP, UDP, SCTP. As a result SIP inherits the vulnerabilities of these protocols. For instance, considering that

the TCP is vulnerable to attacks like SYN flood or TCP session hijacking (Noureldien, 1999), it is highly likely that SIP will be also vulnerable to similar attacks. Moreover, the interconnection of SIP with PSTN, introduces new single points of failure, such as VoIP gateways, which are susceptible to attacks like DoS or data tampering (i.e. creation of malicious ISUP/Q.931 messages). In particularly, all encrypted data must be decrypted for processing and then re-encrypted, offering the opportunity to a skilful malicious user to modify signalling or voice transport data.

Another potential source of SIP security problems is that of software bugs. It has been demonstrated (Wieser et al., 2003) that software problems can cause DoS or unauthorized access, while vulnerabilities in SIP telephone devices (Ofir, 2002b). On the other hand, Smart telephones (i.e. PC-based, PDAs, etc) are susceptible to virus programs. The first Smart-Phone virus named *Cabir* has been already released (Paulson, 2004).

Issues	Impact	Remedy
Eavesdropping: Unauthorized interception decoding of signaling messages	Loss of privacy and confidentiality	Encrypt transmitted data using encryption mechanisms like IPsec and/or TLS.
Viruses and Software bugs	DoS / Unauthorized access	Install antivirus applications / apply software patches.
Replay: Retransmission of genuine messages for reprocessing	DoS	Encrypt and sequence messages (Cseq and Call-ID headers).
Spoofing: Impersonation of a legitimate user	Unauthorized access	Send address authentication between call participants.
Message tampering/Integrity: The message received is the message that was send	Loss of integrity, DoS	Encrypt transmitted data using encryption mechanisms like IPsec, TLS and S/MIME.
Prevention of access to network services e.g. by flooding SIP proxy servers / registrars /.	DoS	Configure devices to prevent such attacks.
SIP-enabled IP phones: Trivial File Transfer Protocol (TFTP) Eavesdropping, Dynamic Host Configuration Protocol (DHCP) Spoofing, Telnet	Loss of confidentiality, Unauthorized access, DoS	SIP phones make TFTP requests to update configuration and firmware files. TFTP is insecure since files are sent unencrypted (disable TFPT). SIP phones make DHCP requests to get an IP address, gateway, etc. Disable Telnet in the phone configuration, allow only to administrators.

Table 1. Network and application security issues and solutions

Aside from IP Telephony based protocols, all the supplementary components of the SIP architecture impose new threats on VoIP (Ofir, 2002a). Attacks in ENUM or DNS are very simple to deploy. For example, if an attacker manages to corrupt a DNS server's cache, inserting a fake record set that effectively removes all Secure SIP (SIPS) records for a proxy server, then any SIPS requests that traverse this proxy server may fail or worse, redirected to another destination (Rosenberg et al., 2002). This sort of attack is known as DNS *cache poisoning*.

3.2. SIP security mechanisms

SIP specification does not include any specific security mechanisms. Instead, the utilisation of other well-known Internet security mechanisms is suggested. As highlighted in Figure 2, SIP security can be provided either in a *hop-by-hop* or *end-to-end* fashion. More specifically, the following security methods are described in (Rosenberg et al 2002): HTTP digest, Transport Secure Layer (TLS), SIPS, IP security (IPsec) and Secure MIME (S/MIME). An end-user has the ability to choose the most appropriate security mechanism using the security agreement described in (Arkko et al., 2003).

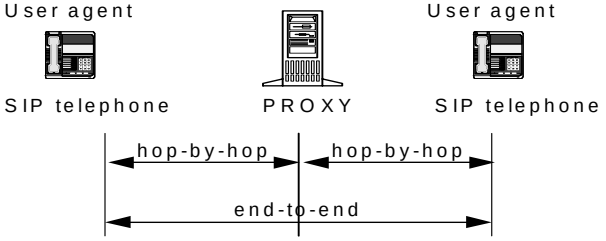

Figure 2 SIP security mechanisms

SIP authentication is inherited from HTTP Digest authentication (Franks et al., 1999), which is a challenge-response based authentication protocol. A SIP server (*registrar*, *proxy* or *redirect*) employs this mechanism for authenticating messages exchanged with a user or another server. The procedure, which is depicted in Figure 1b, is as follows:

- The client sends a SIP message (i.e. SIP INVITE), and the server, which requires authentication, is responding either with a *Proxy authentication require* (407) or *Unauthorized* (401) error.
- This message contains a WWW-Authenticate header including a challenge that will be used by the client to compute the necessary credentials.
- The client creates a new SIP message including an authorization header with the appropriate credentials. A detailed description for the computation of credentials can be found (Franks et al., 1999).

It is well known that IP, which is used to transport SIP messages, is vulnerable to attacks like spoofing, session hijacking etc. The IP security (IPsec) suite provides a set of services to protect IP packets from such attacks. IPsec can provide confidentiality, integrity, data origin authentication services as well as traffic analysis protection (Tiller, 2000). Introducing IPsec in Internet telephony can safeguard signalling and data from network vulnerabilities provided that some sort of trust (e.g. pre-shared keys, certificates) has been established *a-priori* between the communicating parties.

Another solution, to protect SIP communications is the use of SSL/TLS protocol (Rescorla, 2000). Authentication for the corresponding network elements during the handshake procedure is possible to be mutual and is performed by exchanging their certificates. SSL/TLS has many of the advantages of IPsec and the successful introduction of the protocol in the wired Internet has proved its usability and effectiveness. Likewise, SSL/TLS can be part of VoIP environment, as it runs above TCP/IP and below higher-level protocols such as HTTP or FTP and consequently the TCP header is not encrypted. On the other hand, the biggest difficulty with SSL/TLS is that it does not run over UDP. In addition, keeping up many TCP connections simultaneously may be too heavy for proxy servers.

SIP Secure (SIPS) (Rosenberg et al., 2002) is an end-to-end protection mechanism for a requested resource or service. It is considered equivalent to HTTPS and ensures *end-to-end* security. The SIPS addressing scheme has the same structure as SIP; the only difference is the change of the SIP to SIPS. An example of secure address in SIPS scheme is *sips:dgen@aegean.gr*.

SIP messages are capable of carrying MIME bodies, and the MIME standard includes mechanisms for securing MIME contents to ensure either integrity or confidentiality by means of the multipart/signed and application/pkcs7-mime MIME types (Rosenberg et al., 2002). S/MIME provides a set of functionalities and SIP utilizes two of them: *Integrity and authentication tunneling* and *Tunneling Encryption*. However, this solution mandates the deployment of a global S/MIME Public Key Infrastructure (PKI). Otherwise, the exchanged public keys would be self-signed, which makes the initial key exchange susceptible to man-in-the-middle attacks.

3.3. Analysis of SIP security mechanisms

HTTP Digest authentication scheme in SIP can offer one-way message authentication and replay protection but cannot support message integrity and confidentiality. According to RFC 3261, it is very possible for a malicious user to place spam calls. Moreover, this method is vulnerable to well known plaintext, and man-in-the-middle attacks (Ferguson and Schneier, 2003). This is due to the fact that both the plaintext (challenge) and the ciphertext can be easily captured by an aggressor. Additionally, some SIP messages (e.g. ACKs), may not respond with a response. Authentication for these messages is based on the credentials generated by previous requests. This implies that a malicious user may send a manipulated message to cause a DoS. Generally, to work out with DoS attacks, all requests must be authenticated and measures must be taken to prevent packet bombarding. Authentication challenge responses (401 & 407) must be allowed to be transmitted only once. Edge proxies, acting as single monitoring points, can also assist administrators to safeguard the proxy infrastructure from DoS, flooding and viruses.

Digest authentication also requires a pre-arranged trusted environment for password distribution. Passwords may be stored either in plaintext or ciphertext form in the server side. Ciphertext cannot offer an advanced security level since it is feasible to compute the message credentials by launching a brute force attack on the encrypted password. Besides that, the absence of any correlation between the user name and the SIP URIs gives the opportunity to a malicious user to masquerade as a legitimate user. Furthermore, considering that there is no authorisation model, it is possible for an attacker to gain access to services that are normally offered to legitimate users only. Another important issue is that intermediate SIP proxy cannot be certain that the SIP UA has been authenticated. Peterson (Peterson, 2003) suggests 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 server performance (Salsano et al., 2002).

In relation to authentication issues, it is of equal importance to protect user's personal information and his real identity (anonymity, privacy and location privacy). SIP UAs can

afford anonymity by obscuring the *From:* field of SIP requests. However, not all headers can be obscured. For instance, the *Contact:* header is required for request routing. Consequently, a satisfying level of privacy is not possible without support from the proxy infrastructure. As suggested by (Peterson, 2002) the privacy service can be implemented in a proxy server that can also act as a back-to-back user agent and proxy media streams.

Moreover, the SIP REFER method (see Section 2.1) enables the referee as an eavesdropper gives him the ability to launch man-in-the-middle attacks. For example, the referee can forge the Referred-By header or/and eavesdrop on the referred-by information. The referee may also copy – paste all the related information into future unrelated requests. Although, the specification uses an S/MIME based mechanism to enable the refer target to detect possible manipulation of the Referred-By header data, this protection is completely optional.

As already mentioned before, the protection offered by IPsec assumes pre-established trust among the communicating parties 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 IPsec.

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 more suitable for inter domain authentication. Of course, there is always the risk that the message can be intercepted inside the recipient's network if the last hop is not encrypted. Additionally, TLS is used by the SIPS scheme to offer an *end-to-end* security. However, TLS fails to deliver *end-to-end* security and protects only connection-oriented protocols. Currently, there are few SIP clients and network servers that implement TLS and SIPS respectively. On the other hand, the lack of PKI in VoIP does not offer the appropriate environment for the utilization of both SIPS and S/MIME.

S/MIME is used to support either integrity or confidentiality in an *end-to-end* fashion. It is worth noticing, that IPsec and S/MIME generate considerable overhead in SIP messages. More importantly they cannot protect the integrity and confidentiality of the entire SIP message due to existing restriction of header modification (Table 2), as intermediate nodes must have access to SIP header to process and route the SIP message to the appropriate destination. Finally, as in the SSL case, the absence of PKI is an additional restriction for the operation of S/MIME in SIP.

Header	Request URI	From	To	Via	Record Route	Record	Call Id	Cseq
Modification allowed	YES	NO	NO	YES	YES	YES	NO	NO

Table 2: Legal modifications in SIP messages

Regarding subsystems such as DNS and ENUM that must interwork with SIP, there is an on-going discussion on how data exchanged among the ENUM registrars can be protected. (Until now, no security framework for such services has been defined).

4. Conclusion and Future work

This paper has briefly described the SIP architecture and its security mechanisms, exposing the security shortcomings that this protocol is facing. The task of protecting SIP signalling is far more complicated than in PSTN due to the lack of central points for the design, implementation and monitoring of the corresponding traffic. The truth is that any *end-to-end* solution provided by SIP, is partially in the rough. Nevertheless, VoIP forms the driving force for the development of new security solutions being appropriate not only for the protection of voice data but also for numerous other Internet services. It is the authors' opinion that SIP can be considered as an effective solution for Internet telephony only if it offers secure services. The extensibility with additional capabilities helps the design and development of secure services in SIP. Also the development of a general framework for intrusion detection improves availability, reliability and security of SIP-based architectures.

Acknowledgments

This work has been performed in the framework of the IST-2004-005892 project SNOCER, which is funded by the European Union.

5. References

Arkko J et al (2003), Security Mechanism Agreement for the Session Initiation Protocol RFC 3329 IETF

Calhoun P et al, (2003), Diameter Base Protocol RFC 3588 IETF

Falstrom, P (2000), E.164 Number and DNS, RFC 2916, IETF

Ferguson Niels, Schneier Bruce, (2003), *Practical Cryptography*, Wiley Publications

Franks J, et al, (1999), HTTP Authentication RFC 2617 IETF

James S. Tiller (2000), A *technical guide to IPSec Virtual Private Networks* Auerbach publications.

Noureldien A. Noureldien (1999), Protecting Web Servers from DoS / DDoS Flooding Attacks A Technical Overview, www.diplomacy.edu/Conferences/WMIO/PAPERS_&_PRESENTATIONS/Noureldien/NOURELDIEN.pdf (Accessed 13/12/2004)

Ofir Arkin (2002 a), Security Risk Factors with IP Telephony based Networks http://www.sys-security.com/html/projects/VoIP.html (Accessed 13/12/2004)

Ofir Arkin (2002 b), The Trivial Cisco IP Phones Compromise Security analysis of the implications of deploying Cisco Systems' SIP-based IP Phones model 7960, http://www.sys-security.com/html/projects/VoIP.html (Accessed 13/12/2004)

Paulson Dailey Linda (2004), Smart Phone Virus is Discovered Linda Dailey Paulson August *IEEE internet Computing*

Peterson (2002), A Privacy Mechanism for the Session Initiation Protocol (SIP), RFC 3323, IETF.

Peterson (2003), Enhancements for authenticated identity management in the session initiation protocol (SIP), Internet-Draft

Rescorla Eric (2000), *SSL and TLS Designing and Building Secure Systems* . Addison Wesley.

Rigney C et al, (2000), Remote Authentication Dial In User Service (RADIUS) RFC 2865, IETF

Rosenberg J et al (2002), Session Initiation Protocol, RFC 3261 IETF

Salsano et al., (2002),. SIP Security Issues: The SIP authentication procedure and its processing load, IEEE Network

Schulzrinne Henning (1999), Converging on Internet Telephony *IEEE internet Computing*

Sparks, R. (2003), The Session Initiation Protocol (SIP) Refer Method, RFC 3515 IETF

Sparks, R. (2004), The Session Initiation Protocol (SIP) Referred-By Mechanism, RFC 3892, IETF

Stukas, M. and Sicker, C. D., (2004), An Evaluation of VoIP Traversal of Firewalls and NATs within an Enterprise Environment, *Information Systems Frontiers*, 6(3), 219-228, Kluwer Academic Publishers

Varshney Upkar, Snow Andy, McGivern Matt, and Christi Howard (2002), Voice Over IP *Communications of the ACM* Vol. 45, No. 1

Wieser Chirstian, Laakso Marko, Schulzrinne Henning (2003), Security testing of SIP implementations, http://compose.labri.fr/documentation/sip/Documentation/Papers/Security/Papers/462.pdf (Accessed 13/12/2004)