Session Initiation Protocol Security Considerations

Sami Knuutinen
Helsinki University of Technology
Department of Computer Science and Engineering

May 28, 2003

Abstract

Session Initiation Protocol (SIP) is a protocol for signalling multimedia sessions with one or more participants. SIP is an application layer control protocol to initiate and control user sessions. It is used in call set-up signalling for IP telephony, instead of SS7 for circuit switching network. SIP is becoming popular in IP networking. This paper presents and analyses some threats and attacks that SIP is vulnerable to. These threats and attacks set the requirements for security mechanisms that are used to make SIP more secure. This paper examines some of these security mechanisms. In order to present and analyse the security threats and the security mechanisms they are divided into different aspects of security. Privacy protection issues of SIP are also discussed in this paper.

1 Introduction

Session Initiation Protocol (SIP) is a signalling protocol for IP-based communication services [1]. These services include for example Internet telephony, conferencing, presence, events notification and instant messaging. SIP is also the main candidate for signalling protocol in 3G “All-IP”-mobile networks [9].

SIP was developed by MMUSIC (Multiparty Multimedia Session Control), a working group inside the IETF (Internet Engineering Task Force). Since September 1999 the IETF SIP working group has continued the development of SIP.

Security and privacy are mandatory requirements for any network that people use for telephone communication or for any other communication. SIP has some additional security requirements when compared to Public Switched Telephone Network (PSTN) and its Signaling System 7 (SS7). Old PSTN is a closed system and it has a good level of security. Before SIP will be ready for large-scale deployment it must be able to guarantee high service availability, stable and error-free operation and protection of the user-to-network and user-to-user traffic for both control and data. SIP has to provide an adequate level of security running over the generally insecure, open and public Internet [9].

This paper presents and analyses a set of security threats that SIP has. This paper also presents some security mechanisms that are used to make SIP more secure. Communication is secure when data and services are properly secured with administrative and technical
procedures. Security is divided into the aspects of authentication, confidentiality, integrity and availability in this paper. In order to present and analyse the security threats and the security mechanisms they are divided into these different aspects of security. Privacy issues are nowadays a hot topic and should be noted whenever security is the subject of conversation. Privacy can be seen as a combination of all these aspects of security and we discuss privacy protection issues of SIP in this paper.

The following section gives a general and brief overview of the SIP. A set of security threats is presented in the third section of this paper. The fourth section of this paper presents some security mechanisms. The last chapter summarizes the paper and presents conclusions.

2 Session Initiation Protocol Overview

This section gives a general and brief overview of the Session Initiation protocol based on RFC 3261 [1].

Session Initiation Protocol is an application level signalling protocol for signalling multimedia sessions with one or more participants. Multimedia sessions can be for example Internet telephone calls.

SIP is a text-based protocol like for example HyperText Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). SIPs request and response structure is similar to HTTP, and its client-server model is also very much like in HTTP.

The responsibilities of the SIP (and in general any signalling protocol) are listed below.

- Locating a user
- Session establishment
- Negotiate session set-up parameters
- Modify a session
- Tear down a session

“The nature of the services provided make security particularly important[1].” Some security mechanisms are already part of SIP. These mechanisms include denial of service prevention, authentication, integrity protection, encryption and privacy services [1].

2.1 SIP entities

Table 1 presents the entities of the SIP. The role of UAC, UAS, proxy and redirect servers are defined on a transaction-by-transaction basis. UA that initiates a call acts as a UAC when sending the INVITE and as a UAS when receiving a BYE. The implementations of proxy, location service and registrar servers may combine them into a single application. [1]
<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User agent (UA)</td>
<td>A logical entity</td>
</tr>
<tr>
<td>User agent client (UAC)</td>
<td>UAC creates a new request and sends it</td>
</tr>
<tr>
<td>User agent server (UAS)</td>
<td>UAS creates a response</td>
</tr>
<tr>
<td>Proxy</td>
<td>Server and also a client that routes and relays requests</td>
</tr>
<tr>
<td>Redirect Server</td>
<td>UAS that generates 3xx responses</td>
</tr>
<tr>
<td>Registrar</td>
<td>A server that accepts and handles REGISTER requests</td>
</tr>
<tr>
<td>Location Service</td>
<td>Handles information about a callee’s location</td>
</tr>
</tbody>
</table>

Table 1: SIP entities

<table>
<thead>
<tr>
<th>Request</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>Invite the callee into a session</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Discover the capabilities of the receiver</td>
</tr>
<tr>
<td>BYE</td>
<td>Terminate a call or a call request</td>
</tr>
<tr>
<td>CANCEL</td>
<td>Terminate incomplete call requests</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledge a successful response</td>
</tr>
<tr>
<td>REGISTER</td>
<td>Register the current location of a user</td>
</tr>
</tbody>
</table>

Table 2: SIP request methods

2.2 SIP request and responses

Table 2 presents the request methods of the SIP. INVITE, ACK and CANCEL are for setting up sessions, BYE for terminating sessions and OPTIONS for querying the capabilities of the servers [1]. Table 3 presents the responses of the SIP. Figure 1 presents the flow of the request and response messages in the basic call.

2.3 SIP protocol stack

Figure 2 presents the SIP protocol stack. SIP can run over both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Session Description Protocol (SDP) is used to describe the media stream and the session for the purposes of session announcement, session invitation and session initiation [2]. Realtime Transport Protocol (RTP) is used to transport the media stream. Resource reSerVation Protocol (RSVP) is used to ensure Quality of Service (QoS) level for the media stream.

3 Security threats

Following subsections present some of the security threats that SIP has based on RFC 3261 [1] and on “On Applying SIP Security to Networked Appliances” by Tat Chan and Senthil Sengodan [10].

Communication is secure when data and services are properly secured with administrative and technical procedures. Security is divided into the aspects of authentication, confiden-
<table>
<thead>
<tr>
<th>Response</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1xx</td>
<td>Provisional</td>
</tr>
<tr>
<td>2xx</td>
<td>Success</td>
</tr>
<tr>
<td>3xx</td>
<td>Redirection</td>
</tr>
<tr>
<td>4xx</td>
<td>Client error</td>
</tr>
<tr>
<td>5xx</td>
<td>Server error</td>
</tr>
<tr>
<td>6xx</td>
<td>Global failure</td>
</tr>
</tbody>
</table>

Table 3: SIP responses

tiality, integrity and availability. Table 4 briefly introduces the aspects of security. In order to present and analyse the security threats they are divided into these different aspects of security. The summary of the aspects of security that the threat threatens is presented in the table 5.

<table>
<thead>
<tr>
<th>Aspect of security</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Access control, validity of the user is established</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data can be read only by authorized users</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data has not been altered or deleted in an unauthorized manner</td>
</tr>
<tr>
<td>Availability</td>
<td>Data or service is always available to authorized users</td>
</tr>
</tbody>
</table>

Table 4: Descriptions of the aspects of security

<table>
<thead>
<tr>
<th>Threat</th>
<th>Aspect of security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Hijacking</td>
<td>Availability</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Authentication, Confidentiality</td>
</tr>
<tr>
<td>Message tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td>Denial of Service attacks</td>
<td>Availability</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

Table 5: Threats divided into different aspects of security

### 3.1 Registration Hijacking

Registration hijacking means that the attacker may do malicious registrations to the registrar. Attacker may for example register his own device as the contact address of the victim and deregister all old contacts. After that all requests to victim direct to the device of the attacker.

Registration hijacking threatens the availability of the SIP services. The threat of registration hijacking sets the need for security mechanisms that enable SIP entities to authenticate the originators of requests [1].
3.2 Spoofing

The term 'spoofing' is used here to mean someone pretending to be someone else. Pretending to be someone other authorized user or impersonating a server are forms of spoofing.

Spoofing in SIP is pretty much the same as spoofing in SMTP. The attacker alters the headers and the body of the message so that the receiver thinks that someone else sends the message. The attacker may insert a fake source address to the 'From' field. The inserted fake address doesn’t even have to belong to anyone. Also the IP addresses can be spoofed so the reverse dns lookups don’t reveal the correct address.

Impersonating a server means that some malicious attacker pretends to be a server. UAs contact the server in the domain, specified in the Request-URI, directly in order to deliver a request [1]. If an attacker impersonates the server the attacker could intercept the request of the UA. “This family of threats has a vast membership, many of which are critical.”[1]
Authentication can be used to prevent spoofing. Authentication between call participants prevents, or at least makes it harder, pretending to be someone else. Possible countermeasure to impersonating a server is that UAs can authenticate the servers [1].

3.3 Message tampering

Message tampering means that the integrity of a message is violated. If an attacker manages to tamper messages, the message received may not be the same as the message that was sent.

With message tampering, “attackers might attempt to modify SDP bodies, for example, in order to point RTP media streams to a wiretapping device in order to eavesdrop on subsequent voice communications”[1]. The message tampering threat applies to all forms of content that could be delivered in SIP messages, for example to session encryption keys for a media session.

The countermeasures to message tampering are that UAs secure SIP messages end to end independently of the intermediaries such as proxies.[1] One way to ensure the message integrity is the authentication of messages.[10]

3.4 Denial of Service attacks

Denial of Service (DoS) attack is an attack that focuses on making a server, network element or in general a computer or a machine unusable. There are many kinds of denial of service attacks. One type of DoS attack is Distributed Denial of Service (DDoS) attack that directs huge amount of traffic to the network interface of the target host from multiple network hosts.

SIP proxies accept requests from Internet and so they are potential targets of a DoS at-
“SIP creates a number of potential opportunities for distributed denial-of-service attacks that must be recognized and addressed by the implementers and operators of SIP systems.”[1]

Attackers usually create bogus requests that contain fake IP addresses. Attackers can also modify the requests in a way that they can use UAs or proxies to generate DoS attack by counterfeiting the header field values of the SIP message or IP packet.[1]

If the REGISTER requests are not properly authenticated and authorized by registrars, attackers could de-register users in an administrative domain and so prevent the users from being invited to new sessions. Attackers can also try to make the registrar unusable by trying to waste its memory or disk space. One way to exhaust memory of the registrar is by registering huge amount of fake bindings. [1]

Denial of Service attacks are common in public Internet network environment. A script kid who has found a DoS tool and wants to test it causes often DoS attacks. A script kid is a young computer vandal who attempts to hack into internet sites, using scripts downloaded from the web. To the annoyance of security experts the number of script kiddies is growing.

Occasionally a DoS attack is used to draw the attention of the administrators and network operators and at the same time do some other malicious acts. DoS problems “demonstrate a general need to define architectures that minimize the risks of denial-of-service”[1]. Other possible countermeasure to DoS is using access controls [10].

3.5 Eavesdropping

Eavesdropping media stream or SIP messages is a threat to confidentiality and also to privacy [10]. Eavesdropping means here interception of media stream and signalling messages.

If hosts in the local Ethernet network are connected via a hub, the traffic in the network is pretty easy to monitor and intercept by setting the network interface in a promiscuous mode. When the network interface is in promiscuous mode, host receives also the messages that are addressed to other hosts. If the local network is switched or the malicious party wants to eavesdrop messages outside his local network the attacker can try Address Resolution Protocol (ARP) or Internet Control Message Protocol (ICMP) spoofing or implanting a Trojan horse in the target host.

When an attacker manages to intercept the media stream and decode the signalling messages, the communication content and other sensitive and private information are exposed [10]. In the traditional closed PSTN network eavesdropping has been a privilege of a police, certain authorities, phone companies and only the most skillful hackers. In the IP network there exists a risk that some very talented hacker releases a toolkit that automatically eavesdrops anyone. At least in the IP network it is easier for anyone to try the eavesdropping.

Encryption can be used as a countermeasure to eavesdropping [10]. Using for example Secure Realtime Transport Protocol (SRTP) can encrypt the media stream. SIP message can’t be completely encrypted. “SIP requests and responses cannot be naively encrypted end-to-end in their entirety because message fields such as the Request-URI, Route and
Via need to be visible to proxies in most network architectures so that SIP requests are routed correctly.”[1]

3.6 Analysis

SIP has threats in each aspect of security. Before SIP is ready for large-scale deployment it has to guarantee high availability, stable operation and protection of the traffic for both control and data. The presented Registration Hijacking and Denial of Service attacks are threats to the availability of the SIP service. The lack of service availability can be a major issue costing thousands of euros of lost revenue and potential business for both SIP operators and customers. Spoofing is a threat to the confidentiality and authentication of the SIP. Spoofing in SIP is pretty much the same as spoofing in SMTP. By spoofing it is possible to cause same kind of annoying problems than what the junk mail or so called spam causes in SMTP. Message tampering is a threat to message integrity. When the integrity of a message is violated received message may not be the same as the message that was sent. Eavesdropping is a threat to confidentiality. When the confidentiality is violated sensitive and private information can be exposed to the attacker.

4 Security mechanisms

SIP doesn’t have security mechanisms that are specific to it only. Security mechanisms of the SIP are used in HTTP and SMTP protocols. This section presents a set of security mechanisms and describes how they are used in SIP or could be used with SIP.

A secure method to choose the used security mechanisms and their parameters is described in RFC 3329. Secure way to choose the mechanisms is important because otherwise “it is hard or sometimes even impossible to know whether a specific security mechanism is truly unavailable to a SIP peer entity, or if in fact a man in the middle attack is in action.”[4]

Following subsections are based on RFC 3261 [1] and on “SIP Security Issues: The SIP Authentication Procedure and its Processing Load” by Stefano Salsano and Luca Veltri [9].

In order to present and analyse the security mechanisms they are divided into the different aspects of security. Table 4 briefly introduces the aspects of security. The summary of the aspects of security that the security mechanisms try to improve is presented in the table 6.

<table>
<thead>
<tr>
<th>Security mechanism</th>
<th>Aspect of security</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Digest Authentication</td>
<td>Authentication</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Confidentiality, Integrity</td>
</tr>
<tr>
<td>IPSec and TLS</td>
<td>see table 7</td>
</tr>
<tr>
<td>DoS Protection</td>
<td>Availability</td>
</tr>
<tr>
<td>Privacy Protection</td>
<td>Confidentiality, Integrity</td>
</tr>
</tbody>
</table>

Table 6: Security mechanisms divided into different aspects of security
4.1 HTTP Digest Authentication

Authentication means that the identification of the identified object is ensured, and so authenticated, by challenging the object in a way, with some request, that only the correct identified object could know the correct response. In short authentication means that the identification of an object is ensured by eg. a request to which only the identified object could know the correct response. For example normal operating systems authenticate users by first identifying the users by their user id and then challenging the users to answer their correct password.

The SIP authentication mechanism comes from HTTP Digest authentication. The HTTP Authentication procedure is explained in detail in RFC 2617 [5] and the usage of Digest authentication in SIP is explained in section 22 of the RFC 3261 [1]. Briefly the SIP authentication mechanism is stateless challenge based mechanism where the password is never sent in clear text. By modern security standards the authentication mechanism used in SIP doesn’t provide high level of security, because it is based on a shared secret rather than a public key mechanism [9].

The authentication mechanism may be used anytime when a proxy or UA receives a request. User to user and proxy to user authentication can be used. The Authentication mechanism could be used to provide message authentication and replay protection. Authentication doesn’t prove anything about message integrity or confidentiality. Authentication ensures that claimed source has created and sent a message. Authentication doesn’t ensure that the message is the same that was sent or that nobody else has seen it. [1]

4.2 Data encryption

Data encryption ensures the confidentiality of a message. Confidentiality means that messages are only revealed to those parties that should be able to see them and the messages or even their existence is not revealed to anyone else.

As it was said in 3.5 the SIP message can’t be encrypted completely. The encrypted message body can include header fields of the SIP message. Header fields To, From, Call-ID, CSeq and Contact are required in requests and responses and must be plaintext. These header fields can be included in encrypted body and the header could have plaintext version of these fields that differs from the encrypted version.

Data encryption can also ensure the message integrity. Integrity means that the message received is the same as the message that was sent. In general integrity also ensures that the message can’t be deleted illegally but the data encryption doesn’t ensure this. Ensuring that the message can’t be deleted illegally is pretty difficult in a public Internet network.

4.3 IPSec and TLS

IPSec improves the security of the network layer. IPSec is a set of tools that can be used to secure the Internet Protocol (IP). With IPSec one can create secure tunnels through untrustworthy networks. [7]
Transport Layer Security (TLS) provides transport-layer security over TCP. TLS provides privacy and data integrity and is most suited to architectures in which hop by hop security is required between hosts with no previous trust association. [8] “TLS must be tightly coupled with a SIP application.”[1]

The fields of security that IPSec and TLS are designed to improve are presented in the table 7. The table also shows the methods that are used. Availability field of security is excluded from the table because IPSec and TLS are not primarily designed to improve availability. However the use of IPSec and TLS also improves availability because they improve the overall level of security of the network and the transport layer. Whenever using IPSec it should be noted that “the security afforded by the use of IPSec is critically dependent on many aspects of the operating environment in which the IPSec implementation executes.”[7] TLS can be used to prevent eavesdropping SIP messages and to prevent tampering SIP messages.

<table>
<thead>
<tr>
<th>Field of security</th>
<th>IPSec</th>
<th>TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Internet Key Exchange (IKE)</td>
<td>TLS Handshake Protocol</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Authentication Header (AH)</td>
<td>Symmetric cryptography</td>
</tr>
<tr>
<td>Integrity</td>
<td>Encapsulating Security Payload (ESP)</td>
<td>Symmetric cryptography</td>
</tr>
</tbody>
</table>

Table 7: Methods that IPSec and TLS use to improve different fields of security

4.4 DoS Protection

DoS protection ensures the availability of the service. Availability means that services are available to the usage of their users when needed. Availability also ensures that the service operates effectively.

In public Internet network protection from DoS is difficult. Even the core of the Internet, the root nameservers of the Domain Name System (DNS), was troubled by a massive DDoS attack on 21 October 2002. SIP protocol does not have any special mechanism for protection from DoS. Good way to guard also the SIP from DoS is to protect the SIP entities from DoS. DoS protection of the SIP entities is similar to DoS protection of any other network components. Packet filtering and denying ICMP messages to broadcast addresses are common ways to protect from DoS attacks.

4.5 Privacy protection

Privacy is somehow a combination of all the aspects of the security and privacy issues are nowadays a hot topic. Privacy protection means that any sort of user’s private information is not available to any parties that don’t need to know it. Private information could be for example name of the caller or recipient, when the communication happens and how long, callers location or any other kind of sensitive information. SIP messages contain this kind of sensitive information. Implementation of the location service should be able to restrict, on a per-user basis, what kind of location and availability information is given out. [1],[9]

One may think that the session description information by Session Description Protocol
contains sensitive and private information. The following list includes an example of the information that the SDP conveys. With Session Description Protocol it is possible to create a private session. In the private session the session description is encrypted before distribution so the privacy is better protected. [2]

- Session name and purpose
- Time
- Information to receive media (addresses, ports and formats)
- Information about the bandwidth to be used
- Contact information for the person responsible for the session

Protecting privacy in a SIP network is complex because even the IP addresses of the session participants may reveal private information. When one knows the IP address it is possible, for example, to draw conclusions whether the person is at home or at work. A general purpose privacy requirements and privacy protection mechanisms in a SIP network is discussed in RFC 3323 [3]. RFC 3325 presents privacy protection extensions to Session Initiation Protocol that could be used inside an administrative domain [6].

### 4.6 Analysis

There exist mechanisms to improve SIP security in every aspect of security. SIP has additional security requirements when compared to PSTN and its SS7. In public Internet network security and privacy are harder to guarantee than in the closed PSTN network. SIP doesn’t have security mechanisms that are specific to it only. SIP is still rather new protocol and the most focus has been paid to provide new services. During the development of SIP many of the security and privacy issues are recognized. Recognizing the issues is a foundation for the security and privacy to be at a good level within time. In the end the implementation of the SIP protocol and the implementations of the security mechanisms define the security level of the SIP service. Many of the security issues are often due to poor implementations. For example the buffer overflow exploits are a good example of poor implementations. Also for example if the implementation of the random number generator in some security mechanism is not random enough it makes the whole security mechanism insecure.

### 5 Summary and Conclusions

This paper considers the security of the Session Initiation Protocol. At first paper studies the SIP by brief and general overview. Then paper presents and analyses some threats that could be used to exploit the SIP by means of exploiting the authentication, confidentiality, integrity or availability aspect of security. Then paper presents and analyses security mechanisms that can be used with SIP by means of ensuring the authentication, confidentiality, integrity or availability aspect of security.
SIP is used to signal IP network telephone communication and may be used also to signal the communication in 3G mobile networks. Security and privacy are mandatory requirements for this kind of protocol. Towards IP networking, SIP is becoming popular. Before SIP is ready for large-scale deployment it has to guarantee high availability, stable operation and protection of the traffic for both control and data. SIP has additional security requirements when compared to PSTN and its SS7. In public Internet network security and privacy are harder to guarantee than in the closed PSTN network.

Communication is secure when data and services are properly secured with administrative and technical procedures. Security is divided into the aspects of authentication, confidentiality, integrity and availability. SIP has threats in each of these aspects. Fortunately there exist also mechanisms to improve SIP security in every aspect of security. Privacy is somehow a combination of all these aspects of the security and privacy issues are nowadays a hot topic. Privacy protection is hard but a decent level of privacy is possible to achieve when using SIP and its security mechanisms.

SIP is still rather new protocol and the most focus has been paid to provide new services. During the development of SIP security and privacy issues have been dealt with decent effort. At least many of these security and privacy issues are recognized. Recognizing the issues is a foundation for the security and privacy to be at a good level within time.

References


