Session Initiation Protocol Security, autumn 2002

JANNE KARIO
Helsinki University of Technology, Espoo

Session Initiation Protocol (SIP) is an application level protocol for initiating different kinds of sessions with one or more participants. Most common applications for SIP are in the field of IP telephony in which SIP is used to initiate telephony session or call. IP telephony over public Internet demands security. This document presents the different security features that are already part of Session Initiation Protocol as well as the ones that are planned to be added to Session Initiation Protocol. It makes assessments whether these extension are applicable and will be implemented in practice.

1. INTRODUCTION

This paper studies present and proposed security implementations in Session Initiation Protocol (SIP). Session Initiation Protocol request for comments [1] shows a set of security problems with SIP. Some of these problems may hinder the adoption of SIP as a basis for IP telephony over public Internet.

The basis of this study is the IETF's (Internet Engineering Task Force) Session Initiation Protocol request for comments (RFC) and a set of Internet drafts that propose different security enhancements to Session Initiation Protocol.

This first section was an introduction to this paper. The following second section gives a brief introduction to SIP. The third section introduces the present SIP security framework as well as proposed additions and extensions to this framework. Last section summarizes the paper.

2. INTRODUCTION TO SESSION INITIATION PROTOCOL

This section gives a brief introduction to Session Initiation Protocol.

2.1 Overview

Session Initiation Protocol [1] is a protocol for negotiating sessions between participants. Initiating a session using SIP is equivalent to initiating a call in the existing PSTN (Public Switched Telephony Network) infrastructure.

Session that SIP establishes can be anything ranging from a simple call to multi party call, conference or multimedia presentation. SIP offers such services as user discovery, user availability, user capabilities, session setup and session management.

Peer entities are identified using SIP identity which is a form of Uniform Resource Identifier (URI) or SIP URI. SIP identity has a counterpart in the PSTN world, namely phone number.

SIP was originally a component in the MBone multi cast network and became IETF standard in March 1999.

2.2 SIP entities

This section explains the different components of the SIP architecture.

2.2.1 *Softphone.* Softphone is a term for the SIP user agent.

2.2.2 *SIP User Agent Client.* SIP User Agent Client is a SIP entity which issues SIP request.

2.2.3 *SIP User Agent Server.* SIP User Agent Server is a SIP entity which responds to requests.

2.2.4 *Proxy Server.* Proxy server is an entity which relays SIP request forward according the header information that the SIP message has.

2.2.5 *Outbound Proxy.* Outbound proxy is a server which the SIP user agent connects to when making a call to recipient outside its own domain. Outbound proxy acts as relay between the user agent domain and rest of the Internet. Outbound proxy fills the function of PSTN telephone exchange.

2.2.6 *Location Service.* Location service keeps record of all registered SIP identities within its particular administrative domain.

2.3 SIP operations

SIP operations and transactions follow almost same analogy as in HTTP (Hypertext Transfer Protocol). It has a same kind of request/response transaction model. The

Author's contact information: jkario@cc.hut.fi

Published in *Internet Protocols for Mobile Computing - Seminar on Internetworking, Autumn 2002*, by Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory. The complete publication can be found at http://www.tml.hut.fi/Studies/T-110.551/2002/papers/December/index.html.
ISBN 951-22-6272-X - ISSN 1455-9749 - HUT - TML - TML-C9

following subsections introduce briefly the most commonly used SIP operations.

2.3.1 *INVITE.* INVITE method is used to initiate session.

2.3.2 *BYE.* BYE method is used to terminate session (ie. hang up).

2.3.3 *REGISTER.* REGISTER method is used among other things to register SIP user agent with the location service. Location service keeps the information about available SIP identities within its domain and their location.

2.3.4 *OPTIONS.* OPTIONS method is analogous to HTTP method with same name. It can be used to query capabilities of the remote peer.

2.4 SIP message format

SIP is a text-based protocol and the message form and syntax is almost identical to HTTP messages and responses. [1] has many examples of different SIP messages.

2.5 Relation with other protocols

SIP is an application-layer protocol which handles just the initiation of the multimedia sessions. It relies on other protocols to carry out transporting SIP messages, describing and transporting multimedia presentations and streams. Figure 1 contains a picture of the SIP protocol stack as well as the protocol stack for other protocols that are related to SIP.

2.5.1 *TCP (Transmission Control Protocol).* Main method for transporting SIP messages is TCP. TCP has an advantage that TLS (Transport Layer Security) can be used for transport level security.

2.5.2 *UDP (User Datagram Protocol).* Unlike with HTTP, SIP messages can also be transport over UDP. Using this method each SIP request or response is contained inside one UDP datagram.

2.5.3 *SDP (Session Description Protocol).* SDP is used to describe multimedia streams and presentations. SDP is transported in the payload part of the SIP messages. SDP describes such things as video and audio formats and port numbers for the communication. SDP is fully described in [2].

2.5.4 *RTP (Real-time Transport Protocol).* RTP is used to transfer the media stream as described in the SDP message.

2.5.5 *RSVP (Resource Reservation Protocol).* RSVP is used to reserve certain Quality of Service for the media stream.

2.6 Session Initiation Protocol Applications

SIP Forum is consortium of corporations and businesses whose mission is to "promote awareness and provide information about the benefits and capabilities that are enabled by SIP"[10]. SIP Forum is a great source for discovering what is going on behind the dull IETF papers.

Session Initiation Protocol real-life applications include SIP phonesets, SIP client software, SIP Instant Messaging software and SIP Telephony Gateways. SIP phones are ordinary looking phones except that they have an ethernet plug and the voice data is carried over IP. SIP client software include normal desktop applications that emulate phone functions. Nortel has a wide range of SIP based products including SIP phone [11] and SIP software phone [12].

SIP Telephony Gateways are server software which act as a bridge between IP networks and PSTN networks allowing these two to interact.

3. SESSION INITIATION PROTOCOL SECURITY

This section gives an introduction to the present state of the SIP security framework.

The problem with SIP when compared to existing PSTN solutions is that PSTN is closed system while SIP must generally run over public Internet. This sets some additional requirements for SIP security that have never been relevant for PSTN networks. [1] has a long list of different issues with SIP security as well as some threats that the present implementation brings forth.

SIP specification defines mechanisms for securing SIP. These solutions are based on existing technologies used with for example HTTP and SMTP. These four existing security mechanisms are *Transport and Network layer security, SIPS URI Scheme (Secure URI Scheme for SIP), HTTP Authentication (HTTP Digest scheme), S/MIME (Secure MIME)*[1]. Transport and Network layer security means that the communication is encrypted using TLS (Transport Layer Security) or IPSec. SIPS URI Scheme is method for identifying SIP entities that request secure communications, namely TLS. HTTP Authentication is a challenge response model for authenticating users. S/MIME is a method for securing MIME payload and secure SIP request tunneling.

In spite of these four security mechanisms SIP is still vulnerable to many threats.

The idea in following subsections is to present a set of enhancements to SIP security and comment whether they are applicable to reality and whether they will be implemented in real applications. The plan is also to try to evaluate them and find possible flaws in them. These enhancements are all IETF Internet drafts at the time of writing. They address subset of the security issues presented in [1].

3.1 User identity and authentication

As discussed in the previous sections, baseline SIP has user authentication mechanism which is based on the use of HTTP Digest[3]. The problem with this approach is that users are authenticated only within their own administrative domain and with the first outbound proxy. If the call was made to an entity outside this domain the callee has no access to the authentication information. User identity information can be used to implement such a service as for example caller id. User identity is also important in corporate communications where people generally want to be sure that the person they are talking to is not an outsider.

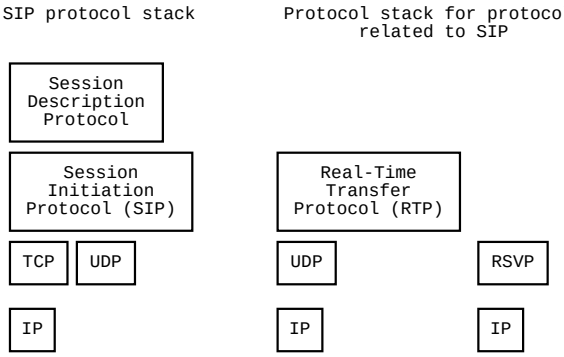

Fig. 1. SIP protocol stack

Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP) [6] is a proposal where SIP would be extended to support end to end authentication. After the outbound proxy has authenticated the caller it puts the authentication information in the SIP message payload for intermediate proxies and callee to see.

Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks [5] is a proposal that basically tries to do the same thing as [6] but within a trusted network.

These two proposals are competing solutions with slightly different focus. The first solution passes the cryptographically signed identity information in the SIP message payload using content type *message/sipfrag*. The second solution passes the identity information unsigned in an SIP *P-Asserted-Identity* extension header. The former is clearly to be used in an trusted environment and is to be a short term solution. The latter can be used in an untrusted network to provide end-to-end user identity authentication.

Because these two proposals have overlapping functions it would be nice to see them converge into one proposal[1]. The second solution can perform all of the operations that the first one does and provides end-to-end identity authentication as a bonus. However the first solutions is much more simple to implement in practice. Furthermore it is a joint IETF draft whereas the second is a personal proposal. The downside is that first does not provide end-to-end identity authentication. This has the power to demolish this draft if IETF is actually looking for a solution that can be deployed Internet wide. It seems however that the first solutions is much more likely to evolve into full RFC. [5] is at the time of this writing already in the RFC editors queue.

3.2 Privacy

SIP protocol has many headers that may unintentionally reveal identity information about the user. This information includes at least user's name, username, organization, network domain and subject. The information is available to all intermediate proxies as well as to the intended recipient.

A Privacy Mechanism for the Session Initiation Protocol (SIP) [8] discusses about requirements related to privacy in SIP. It also introduces a set of simple rules that enable user agents to minimize the private information sent. Finally, it presents a new "privacy service" role for the SIP proxy and a new "Privacy" header.

3.2.1 *User agent behavior.* The amount of private information can be diminished by configuring SIP user agent properly. [8] presents instructions for doing so. These guidelines work mostly within the existing SIP specification and do not require any extensions to SIP.

[8] suggests that user agent should avoid sending any optional headers that reveal identity information. Second suggested step is to try populate SIP URI and SIP headers in such way that they do not reveal sensitive information. Some of the headers identifying user can be filled with anonymous values without affecting the overall operation of the protocol.

3.2.2 *Privacy header.* Privacy header allows user agents to request certain level of privacy from the outbound proxy. The header is an extension to the existing SIP specification and requires an entity capable of handling it. This entity is called "privacy service" and it will be introduced in 3.2.3.

Privacy header is used in such circumstances where the user agent needs to obscure some header information but it cannot obscure headers itself. The header is a method for requesting the privacy service to do it for the user agent.

3.2.3 *Privacy Service.* [8] defines a new "privacy service" role. It is recommended that the new role would be implemented in the SIP outbound proxy. This service fulfills the session privacy parameters requested by the user agent.

The privacy service checks every message that passes through. If privacy is requested it conceals all appropriate headers and sends the message forward. Privacy

[1] In fact this happened October 28th when [13] was released. The purpose of the new draft is to find a common solution to the identity issues, one that is cryptographically secure enough that it can be deployed Internet wide. This new draft is beyond the scope of this paper because it was published so late.

service offers different levels of privacy. The levels are header, user and session.

When header level privacy is requested, privacy service obscures all header information that might contain identity information. When user level privacy is requested the privacy service replaces all information related to the end user with anonymous values. The privacy service must retain conversational state and act as a proxy between the intended recipient and sending user agent. The recipient receives messages that originate from the privacy service. The responses from the intended recipient are routed back to the original sender by the privacy service with appropriate headers converted back to their original form.

Session level privacy requests that the identity information related to the multimedia session traffic itself is obscured. For Internet telephone calls the session traffic means the audio media stream. Privacy information in session traffic generally means source IP address and domain of the actual media stream. Hiding identity in the multimedia session is beyond the scope of the SIP protocol.

3.2.4 *Privacy summary.* The good thing about [8] is that it can be used even without introducing new Privacy-header or the privacy service role for the outbound proxy. It serves as a general implementation guideline when implementing user agents that respect user privacy.

If the new privacy functionality is needed in full it is pretty straightforward to implement because the simplest case involves only rewriting a predefined set of SIP headers to conceal the identity of the sender. The problematic case is the session level privacy because it requires interaction with other network layers and protocols. The good news however is that it is not mandatory for the privacy service to implement any of the privacy levels. The only thing that is mandatory is that the privacy service understands the meaning of the Privacy-header.

3.3 Media authorization

SIP specification does not handle QoS (Quality of Service) in any way. The implication is that it is possible for more people to make calls than the bandwidth allows. This results in poor line quality. This section presents a SIP extension which adds QoS negotiation into SIP.

SIP Extensions for Media Authorization [7] proposes a QoS service mechanism which solves this problem stated above. The basic idea is to use an authorization token which the user agent receives from the first outbound proxy (QoS enabled proxy). The message flow is illustrated in Figure 2. The token or a set of tokens are used by the user agent when it opens the multimedia stream to reserve certain QoS for its transmission. In essence the user agent asks permission from the outbound proxy to open media stream. The QoS proxy can prevent the user agent from making the call by not sending any tokens or it can control the QoS of the call by returning different kinds and different number of tokens. QoS enabled proxy can inspect the SDP message and determine which kind of quality of service the specified media stream needs.

The SIP user agent can use the token or tokens that it receives from the QoS proxy to make a RSVP (Resource Reservation Protocol) PATH request to reserve the bandwidth for its media streams. The RSVP is provided in [7] just as example of the use of authorization token. The method for request QoS is not necessarily bound to be RSVP.

The QoS enabled proxy must cooperate with one additional network element, namely PDP (Policy Decision Point). QoS proxy supplies the PDP with authorization information and receives one or more authorization tokens. PDP stores the information in a database with authorization token as the key. The tokens are inserted into the response which goes back to the user agent.

The SIP user agent must interact with one additional network entity, ER (Edge Router), when it makes a decision based on the authorization token supplied by the user agent whether to allow bandwidth reservation. Edge router must contact Policy Decision Point and hand over the authorization token supplied by the user agent to check if it is valid.

This proposal is most welcome addition to SIP. However it is not necessarily easy to implement. The proposal introduces a new logical role for the outbound proxy (QoS service) and a totally new SIP entity Policy Decision Point. QoS proxy may need inspect all incoming message bodies to make decisions based on the SDP media descriptions they provide. The functionality of the QoS service overlaps two network layers.

4. SUMMARY

The section summarizes the present situation of the SIP security framework and future plans for the SIP security.

The present applications of are usually used in corporate intranets within trusted domain most common application being IP telephony in the corporate intranet. However there are security limitations in the present SIP specification. Some of these prevent wide range usage of SIP in public Internet environment. These limitations are related to privacy and user identity authentication.

IETF has made several Internet drafts that try to address some of these threats and limitations. These drafts are related to user personal identity information privacy, user authentication and quality of service negotiation within SIP.

Section 3.1 presented two competing solutions for identity management. The first solutions that uses *P-Asserted-Identity* header [5] works within trusted network of parties. The second solution [6] uses cryptographic signing and provides end-to-end authentication because it is able to transport the authenticated identity all the way to the recipient.

Privacy extensions presented in section 3.2 are valuable addition to Session Initiation Protocol. Not only is the extension easy to implement but also the proposed draft offers valuable implementation guidelines for SIP user agent implementer. Privacy is perhaps the most important issues when SIP moves from the trusted corporate intranets to the public Internet. People using Internet telephony do not want to start receiving calls from strangers who spy on peoples identity information. People do not also generally want their call behavior traced

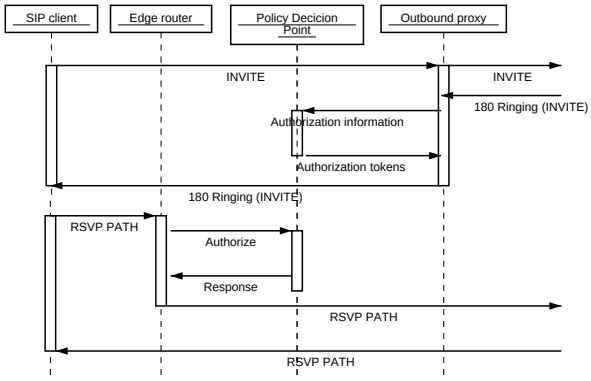

Fig. 2. Media authorization flow

and recorded by others than the authorities that provide the telephony service.

Section 3.3 presented a framework for adding QoS negotiation into SIP. The SIP user agent receives a token from the outbound proxy which the user agent uses when reserving bandwidth. The proposed features are needed in SIP but the implementation of this QoS framework requires interaction with other network layers. Furthermore the QoS architecture is not very commonly used in todays Internet. Very few Internet Service Providers offer quality of service functions. The prerequisite for this proposal to realize into practice is that QoS first becomes widely used in the public Internet and that the routers actually support it.

REFERENCES

[1] Rosenberg et all., SIP: Session Initiation Protocol, Online. June 2002, referred to September 24th 2002. URL: http://www.ietf.org/rfc/rfc3261.txt

[2] Handley, Jacobson, SDP: Session Description Protocol, Online. April 1998, referred to September 24th 2002. URL: http://www.ietf.org/rfc/rfc2327.txt

[3] Franks et all., HTTP Authentication: Basic and Digest Access Authentication, Online. June 1999, referred to September 24th 2002. URL: http://www.ietf.org/rfc/rfc2617.txt

[4] Arkko et all., Security Mechanism Agreement for SIP Sessions, Online. October 2002, referred to October 29th 2002. URL: http://www.ietf.org/internet-drafts/draft-ietf-sip-sec-agree-05.txt

[5] Jennings, Peterson, Watson, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, Online. June 2002, referred to September 24th 2002. URL: http://www.ietf.org/internet-drafts/draft-ietf-sip-asserted-identity-02.txt

[6] Peterson, Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), Online. July 2002, referred to September 24th 2002. URL: http://www.ietf.org/internet-drafts/draft-peterson-sip-identity-01.txt

[7] Marshall, Andreasen, Evans, SIP Extensions for Media Authorization, Online. May 2002, referred to September 24th 2002. URL: http://www.ietf.org/internet-drafts/draft-ietf-sip-call-auth-06.txt

[8] Peterson, A Privacy Mechanism for the Session Initiation Protocol (SIP), Online. June 2002, referred to September 24th 2002. URL: http://www.ietf.org/internet-drafts/draft-ietf-sip-privacy-general-01.txt

[9] Rosenberg, Schulzrinne, Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP), Online. November 2002, referred to November 4th 2002. URL: http://www.ietf.org/internet-drafts/draft-ietf-sip-guidelines-06.txt

[10] SIP Forum URL: http://www.sipforum.com

[11] i2004 Internet Telephone, referred to September 18th 2002. URL: http://www.nortelnetworks.com/products/01/succession/es/i2004/index.html

[12] i2050 Software Phone, referred to September 18th 2002. URL: http://www.nortelnetworks.com/products/01/succession/es/i2050/index.html

[13] Peterson Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), Online. October 28th 2002 referred to October 31st 2002 URL: http://www.ietf.org/internet-drafts/draft-ietf-sip-identity-00.txt