SIP
Internet-Draft
Intended status: Standards Track
Expires: August 22, 2007

M. Munakata
S. Schubert
T. Ohba
NTT

February 18, 2008

UA-Driven Privacy Mechanism for SIP
draft-ietf-sip-ua-privacy-01

Status of this Memo

Copyright Notice

Abstract

To withhold a user's identity and related information, RFC 3323 defines a Privacy mechanism for SIP, which requires the use of an privacy service. This document proposes a new privacy mechanism that a user agent can facilitate to conceal privacy-sensitive information without the need for aid from a privacy service.

Table of Contents

1. Introduction

Privacy is defined in [RFC3323] as the withholding of the identity of a person (and related personal information) from destination(s) of messages and/or intermediaries handling these messages in an exchange of SIP (Session Initiation Protocol) [RFC3261] communications.

In SIP, identity is most commonly carried in the form of a SIP URI and an optional display-name, which commonly appear in the To, From and other header fields of SIP requests and responses.

There are numerous other places in SIP messages in which identity-related information can be revealed. For example, the Contact header field contains a SIP URI. Moreover, information in the Record-Route and Via headers could inadvertently reveal something about the originator of a message.

RFC 3323 defines privacy mechanisms for SIP, based on techniques available at the time of publication. Some of these mechanisms rely on the use of a separate privacy service to remove sensitive information from messages sent by a user agent before forwarding those messages to the final destination. Since then, numerous SIP extensions have been proposed and standardized. Some of those seem to enable a user agent to withhold its user's identity and related information without dependency on privacy services, which was not possible when RFC 3323 was defined.

A number of issues have been identified with the mechanisms defined in RFC 3323, especially with mechanisms that depend on a privacy service.

1. There is no assurance that a privacy service exists in the signaling path.

2. There is no way that the user requesting the privacy can figure out that the privacy function was properly executed.

3. A privacy service that modifies a Call-ID must be present in the signaling path of any subsequent requests that carry that Call-ID. For requests within the same dialog this can be achieved using the record-route mechanism. For requests outside the dialog that carry the Call-ID in a Replaces, Join or Target-Dialog header field, for example, there is no defined mechanism.

4. To map the referenced dialog to a dialog attempt invoked by REFER, for example, the privacy service needs to retain the correspondence relation between original information and modified information beyond the actual dialog duration of the referenced

dialog.

To solve the problems, this document proposes a new privacy mechanism in which a user agent controls all the privacy functions on its own utilizing SIP extensions such as GRUU (Globally Routable User Agent URIs)[I-D.ietf-sip-gruu] and TURN (Traversal Using Relay NAT)[I-D.ietf-behave-turn].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

privacy-sensitive information:
: The information that identifies a user who sends the SIP message, as well as the supplementary information that can be used to guess the user's identity.

3. Concept of Privacy

The concept of privacy in this document means the concealing of the identity of a user and supplementary information. The scope of this document is to withhold the privacy-sensitive information of the user who sends the SIP message from other users and intermediaries handling the message. The protection of network privacy (e.g., topology hiding) is outside the scope of this document.

Privacy-sensitive information includes display-name and URI in a From header that can reveal the user's name and affiliation (e.g., company name), contact information in a Contact header that is used to communicate with the user's UA, an IP address in an SDP (Session Description Protocol)[RFC4566] that tells the location of a user's UA and can be used to establish a connection. A host name in Call-ID is also regarded as privacy-sensitive information because it may reveal the user's domain name.

Privacy-sensitive information is divided into two types, information inserted by the user's UA and information inserted by other SIP entities (e.g., proxies, B2BUAs). A user agent can maintain privacy of the UA-inserted information by itself. On the other hand, regarding the information inserted by other entities, a user agent can insert a privacy flag and request intermediaries not to add the privacy-sensitve information.

4. Requirements

The requirements for the UA-driven privacy mechanism are as follows:

Req 1: A user agent MUST be able to send a SIP request that is fully anonymized. This is, any headers and body inserted by the user agent does not jeopardize user privacy.

Req 2: It MUST be possible for a user agent to indicate to downstream entities that a user is requesting privacy.

Req 3: When privacy is requested, a proxy SHOULD honor the request and only add information necessary to route the call while withholding any sensitive information that may reveal anything about the user if possible.

Req 4: Mechanism defined here MUST be backward compatible with the pre-existing privacy mechanism already in place.

5. Treatment of Privacy-Sensitive Information

Except by means of a privacy service, RFC 3323 does not provide means to obscure two important pieces of information about the user agent, which are a URI used to exchange signaling (Contact, From, for example), and IP address(es) used to exchange media.

RFC 3323 recommends to set sip:anonymous@anonymous.invalid as a SIP URI in a From header when user privacy is required. Although, the From header field URI may need to be an anonymous but functional URI. For example, a mechanism of SIP-Identity [RFC4474] requires a functional From header even if it is anonymous.

With the use of GRUU [I-D.ietf-sip-gruu] and TURN [I-D.ietf-behave-turn], a user agent can now obtain URI(s) and IP address(es) for media that are functional yet anonymous, in that they do not identify the user agent.

5.1. Anonymous URI and Display-Name

A user agent wanting to obtain functional anonymous URI SHOULD support and SHOULD utilize the GRUU mechanism. By sending a REGISTER request requesting GRUU, the UA can obtain an anonymous URI, which can later be used for Contact header.

The detailed process on how a user agent obtains a GRUU is described in [I-D.ietf-sip-gruu]. If the Registrar supports GRUU and returns a REGISTER response, the user agent SHOULD search within the REGISTER

response for a "temp-gruu" URI parameter, which provides the desired privacy property.

If the "temp-gruu" URI parameter and value exist within the REGISTER response, the user agent SHOULD use the value of the "temp-gruu" as an anonymous URI representing the user agent. This URI SHOULD be used for Contact header.

The user agent using the "temp-gruu" as a contact URI is RECOMMENDED to set "Anonymous" as a display-name in any header where the display-name of the originator is set. That indicates the anonymity of the request to intermediaries that may invoke some services based on the anonymity of the call. The temp-gruu alone is not sufficient to invoke such service because GRUU is merely a URI that is a sequence of strings and digits with no explicit semantics to indicate that it

is an anonymous URI.

If there is no "temp-gruu" URI parameter in the 200 response to the REGISTER request, a user agent SHOULD NOT proceed with its anonymization process, unless something equivalent to "temp-gruu" is provided through some administrative means.

Note: How to obtain an anonymous URI for From and any headers other than the Contact is FFS.

It is RECOMMENDED that user agent consult the user before sending a request without a functional anonymous URI when privacy is request from the user.

5.2. Anonymous IP Address

It is assumed that a user agent is either manually or automatically configured through means such as a configuration framework [I-D.ietf-sipping-config-framework] with the address of one or more STUN relay servers.

Two IP addresses are needed to maintain privacy, one to be used in signaling such as in a Via header, another to be used in SDP for media.

A user agent that is not provided with a functional anonymous IP address through some administrative means, SHOULD obtain a relayed address (IP address of the media relay) for use in SDP, derived from a STUN [I-D.ietf-behave-turn] relay server using the STUN relay usage, which allows a STUN server to act as a media relay.

Note: A relayed IP address may be used for a Via header, but some commented that is not an appropriate to be used for signaling. There was a comment about the IP address in Via being stripped by the proxy, but that would require that a proxy compliant to this specification is in the signaling path.

6. User Agent Behavior

A user agent fully compliant with this document SHOULD obscure or conceal all the UA-inserted privacy-sensitive information in SIP requests and responses when user privacy is requested. Section 6.1 describes how to generate an anonymous message at a user agent.

When a user agent generates an anonymous message based on this specification, it SHOULD set an indication to tell intermediaries not to add privacy-sensitive information. Section 6.2 describes more about this.

6.1. Generating Anonymous Message

The two pieces of information that a user agent needs to obscure while sustaining its purpose and functionality are the URI and IP address used for establishing a media/signaling session. Instructions on how to obtain an functional anonymous URI and IP address are given in Section 5.1 and 5.2, respectively.

For anonymizing any headers and information in a SIP message, the user agent SHOULD follow the instructions in this document.

Note: Instructions to treat each SIP header/parameter in generating an anonymous SIP message will be given in a future version of this draft.

6.2. Indication to Maintain Privacy

This document defines a privacy flag, which indicates that the user requires privacy for the SIP message. Without a privacy flag, intermediaries might add some privacy-sensitive information in the message, even if a user agent had anonymized the message as perfectly as possible.

When a user agent generates an anonymous message by itself according to the guidelines in Section 6.1, it SHOULD set a flag to request intermediaries not to add privacy-sensitive information.

Note: The mechanism of the flag is FFS.

7. Proxy Behavior

When a proxy receives a SIP message containing a privacy flag, the proxy compliant with this specification MUST NOT add any information that may reveal something about the sender that is irrelevant to routing unless the proxy knows that such information will be deleted before it leaves the boundary of the Trust Domain[RFC3324].

A proxy MUST NOT modify the privacy flag, if present.

8. Security Considerations

TBD

9. IANA Considerations

TBD

10. References

10.1. Normative References

[I-D.ietf-behave-turn]
Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", draft-ietf-behave-turn-06 (work in progress), January 2008.

[I-D.ietf-sip-gruu]
Rosenberg, J., "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", draft-ietf-sip-gruu-15 (work in progress), October 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

10.2. Informative References

[I-D.ietf-sipping-config-framework]
Channabasappa, S., "A Framework for Session Initiation Protocol User Agent Profile Delivery", draft-ietf-sipping-config-framework-15 (work in progress), February 2008.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[RFC3324] Watson, M., "Short Term Requirements for Network Asserted Identity", RFC 3324, November 2002.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

Authors' Addresses

Mayumi Munakata
NTT Corporation

Phone: +81 422 36 7565
Email: munakata.mayumi@lab.ntt.co.jp

Shida Schubert
NTT Corporation

Phone: +1 604 762 5606
Email: shida@ntt-at.com

Takumi Ohba
NTT Corporation
9-11, Midori-cho 3-Chome
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 7748
Email: ohba.takumi@lab.ntt.co.jp

URI: http://www.ntt.co.jp

Full Copyright Statement

Intellectual Property

ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).