SIP
Internet-Draft
Intended status: Standards Track
Expires: January 10, 2008

M. Munakata
S. Schubert
T. Ohba
NTT

July 9, 2007

UA-Driven Privacy Mechanism for SIP
draft-munakata-sip-privacy-new-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 this document 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 a SIP (Session Initiation Protocol) [RFC3261] dialog.

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.

To provide privacy, [RFC3323] defines a privacy mechanism for SIP, which was then the best current practice to maintain privacy. 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 RFC3323 was defined.

Some aspect of RFC 3323, especially its dependency on a privacy service to provide privacy, seems to cause some issues, which we hope that we can resolve with this specification.

Some of the issues identified with the RFC 3323 are shown below.

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 in the establishment of the original dialog must be in the signaling path of the subsequent request such as REFER. If a privacy service anonymizes a Call-ID and the anonymized Call-ID is referenced in a subsequent SIP message for the purpose of a call-back or a call replacement, the privacy service needs to be in a signaling path to replace the anonymized Call-ID with the original Call-ID appropriately, regardless of being inside/outside the dialog.

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 executes 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.rosenberg-midcom-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].

3. Concept of Privacy

The concept of privacy in this document means the concealing of information that relates to a user, identifies a user, and belongs to a user, as well as the supplementary information that can be used to guess the user's identity. The scope of this document is to withhold the identity of a user and supplementary information from other users and intermediaries handling the message. The protection of network privacy (e.g., topology hiding) is outside the scope of this document.

User-privacy-related 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, an IP address in an SDP (Session Description Protocol)[RFC4566] that tells the location of a user's terminal and can be used to establish a connection. A host name in Call-ID is also regarded as user-privacy-related information because it may reveal the user's domain name.

Privacy-sensitive information is divided into two types, user-inserted information and network-inserted information. A user agent can maintain privacy of the user-inserted information by itself. On the other hand, regarding the network-inserted information, a user agent can insert a privacy flag and request intermediaries not to add the user-privacy-related information.

4. Use Cases

The following are the use cases from the viewpoint of privacy.

Case 1: User privacy is required and a user agent can anonymize all of the user-inserted privacy-related information by itself.

Case 2: User privacy is required but a user agent cannot anonymize the user-inserted privacy-related information all by itself.

Case 3: User privacy is not required. The user does not want privacy at all and would like to reveal his/her identity.

Note that Case 2 is based on the premise that the user agent has limited capabilities and it cannot find a GRUU or TURN server. Case 2 is outside the scope of this document.

5. Requirements

The following are requirements to cover the use cases in the previous section.

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 UA 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.

6. Treatment of User Privacy Related Information

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 an IP address used to exchange media.

With the use of GRUU [I-D.ietf-sip-gruu] and TURN [I-D.rosenberg-midcom-turn], UA can now obtain URI and IP address

that are functional, which are usable to exchange either signaling or media while providing privacy.

6.1. Anonymous URI

A user agent wanting to obtain functional anonymous URI SHOULD support and SHOULD utilize the Global Routable User Agent URI (GRUU) mechanism. By sending a REGISTER request requesting GRUU, the UA can obtain an anonymous URI, which can later be used for From, Contact and other headers where the URI of the originator is needed.

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 originator. This URI SHOULD be used for Contact and From, for example, wherever the originator of the URI is required.

The user agent setting the "temp-gruu" as a GRUU SHOULD 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.

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.

6.2. Anonymous IP Address

It is assumed that a user agent is either manually or automatically configured through means such as a configuration framework with 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 relay server using the STUN Relay Usage[I-D.rosenberg-midcom-turn], 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.

7. User Agent Behavior

A user agent fully compliant with this document SHOULD obscure or conceal all the user-inserted privacy-related information in SIP requests and responses when user privacy is requested. Section 7.1 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 or modify user-privacy-related information. Section 7.2 describes more about this.

7.1. 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 6.1 and 6.2, 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 SIP message will be given in a future.

7.2. 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 user-privacy-related 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 7.1, it SHOULD set a flag to request intermediaries not to add user-privacy-related information.

Note: The mechanism of the flag is FFS.

8. 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.

9. Security Considerations

TBD

10. IANA Considerations

TBD

11. References

11.1. Normative References

[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-14 (work in progress), June 2007.

[I-D.rosenberg-midcom-turn]
Rosenberg, J., "Traversal Using Relay NAT (TURN)", draft-rosenberg-midcom-turn-08 (work in progress), September 2005.

[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.

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

11.2. Informative References

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

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

Authors' Addresses

Mayumi Munakata
NTT Corporation

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

Shida Schubert
NTT Corporation

Phone: +1 604 762 5606
Email: shida at 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 at lab.ntt.co.jp
URI: http://www.ntt.co.jp

Full Copyright Statement

Intellectual Property

Acknowledgment

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