                 User-Agent-Driven Privacy Mechanism for SIP

Abstract

   This document defines a guideline for a User Agent (UA) to generate
   an anonymous Session Initiation Protocol (SIP) message by utilizing
   mechanisms such as Globally Routable User Agent URIs (GRUUs) and
   Traversal Using Relays around NAT (TURN) without the need for a
   privacy service defined in RFC 3323.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc5767.

Table of Contents

1. Introduction

   [RFC3323] defines a privacy mechanism for the Session Initiation
   Protocol (SIP) [RFC3261], based on techniques available at the time
   of its publication. This mechanism relies on the use of a separate
   privacy service to remove privacy-sensitive information from SIP
   messages sent by a User Agent (UA) before forwarding those messages
   to the final destination. Since then, numerous SIP extensions have
   been proposed and standardized. Some of those enable a UA to
   withhold its user's identity and related information without the need
   for privacy services, which was not possible when RFC 3323 was
   defined.

   The purpose of this document is not to obsolete RFC 3323, but to
   enhance the overall privacy mechanism in SIP by allowing a UA to take
   control of its privacy, rather than being completely dependent on an
   external privacy service.

   The UA-driven privacy mechanism defined in this document will not
   eliminate the need for the RFC 3323 usage defined in [RFC3325], which
   instructs a privacy service not to forward a P-Asserted-Identity
   header field outside the Trust Domain. In order to prevent
   forwarding a P-Asserted-Identity header field outside the Trust
   Domain, a UA needs to include the Privacy header field with value

'id' (Privacy:id) in the request, even when the UA is utilizing this
specification.

This document defines a guideline in which a UA controls all the
privacy functions on its own utilizing SIP extensions such as
Globally Routable User Agent URIs (GRUUs) [RFC5627] and Traversal
Using Relays around NAT (TURN) [RFC5766].

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 other information that can be
                              used to guess the user's identity.

3. Concept of Privacy

The concept of privacy in this document is the act of concealing
privacy-sensitive information. The protection of network privacy
(e.g., topology hiding) is outside the scope of this document.
Privacy-sensitive information includes display-name and Uniform
Resource Identifier (URI) in a From header field that can reveal the
user's name and affiliation (e.g., company name), and IP addresses or
host names in a Contact header field, a Via header field, a Call-ID
header field, or a Session Description Protocol (SDP) [RFC4566] body
that might reveal the location of a UA.

4. Treatment of Privacy-Sensitive Information

Some fields of a SIP message potentially contain privacy-sensitive
information but are not essential for achieving the intended purpose
of the message and can be omitted without any side effects. Other
fields are essential for achieving the intended purpose of the
message and need to contain anonymized values in order to avoid
disclosing privacy-sensitive information. Of the privacy-sensitive
information listed in Section 3, URIs, host names, and IP addresses
in Contact, Via, and SDP are required to be functional (i.e.,
suitable for purpose) even when they are anonymized.

With the use of GRUU [RFC5627] and TURN [RFC5766], a UA can obtain
URIs and IP addresses for media and signaling that are functional yet
anonymous, and do not identify either the UA or the user.

Instructions on how to obtain a functional anonymous URI and IP
address are given in Section 4.1 and 4.2, respectively.

Host names need to be concealed because the user's identity can be
guessed from them, but they are not always regarded as critical
privacy-sensitive information.

In addition, a UA needs to be careful not to include any information
that identifies the user in optional SIP header fields such as
Subject and User-Agent.

4.1. Obtaining a Functional Anonymous URI Using the GRUU Mechanism

A UA wanting to obtain a functional anonymous URI MUST support and
utilize the GRUU mechanism unless it is able to obtain a functional
anonymous URI through other means outside the scope for this
document. By sending a REGISTER request requesting GRUU, the UA can
obtain an anonymous URI, which can later be used for the Contact
header field.

The detailed process on how a UA obtains a GRUU is described in
[RFC5627].

In order to use the GRUU mechanism to obtain a functional anonymous
URI, the UA MUST request GRUU in the REGISTER request. If a "temp-
gruu" SIP URI parameter and value are present in the REGISTER
response, the user agent MUST use the value of the "temp-gruu" as an
anonymous URI representing the UA. This means that the UA MUST use
this URI as its local target and that the UA MUST place this URI in
the Contact header field of subsequent requests and responses that
require the local target to be sent.

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

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

Due to the nature of how GRUU works, the domain name is always
revealed when GRUU is used. If revealing the domain name in the
Contact header field is a concern, use of a third-party GRUU server
is a possible solution, but this is outside the scope of this
document. Refer to the Security Considerations section for details.

4.2. Obtaining a Functional Anonymous IP Address Using the TURN
      Mechanism

   A UA that is not provided with a functional anonymous IP address
   through some administrative means MUST obtain a relayed address (IP
   address of a relay) if anonymity is desired for use in SDP and in the
   Via header field. Such an IP address is to be derived from a Session
   Traversal Utilities of NAT (STUN) relay server through the TURN
   mechanism, which allows a STUN server to act as a relay.

   Anonymous IP addresses are needed for two purposes. The first is for
   use in the Via header field of a SIP request. By obtaining an IP
   address from a STUN relay server, using that address in the Via
   header field of the SIP request, and sending the SIP request to the
   STUN relay server, the IP address of the UA will not be revealed
   beyond the relay server.

   The second is for use in SDP as an address for receiving media. By
   obtaining an IP address from a STUN relay server and using that
   address in SDP, media will be received via the relay server. Also,
   media can be sent via the relay server. In this way, neither SDP nor
   media packets reveal the IP address of the UA.

   It is assumed that a UA is either manually or automatically
   configured through means such as the configuration framework
   [SIPPING-CONFIG] with the address of one or more STUN (Session
   Traversal Utilities for NAT) [RFC5766] relay servers to obtain
   anonymous IP address.

5. UA Behavior

   This section describes how to generate an anonymous SIP message at a
   UA.

   A UA fully compliant with this document MUST obscure or conceal all
   the critical UA-inserted privacy-sensitive information in SIP
   requests and responses as shown in Section 5.1 when user privacy is
   requested. In addition, the UA SHOULD conceal the non-critical
   privacy-sensitive information as shown in Section 5.2.

   Furthermore, when a UA uses a relay server to conceal its identity,
   the UA MUST send requests to the relay server to ensure request and
   response follow the same signaling path.

5.1. Critical Privacy-Sensitive Information

5.1.1. Contact Header Field

   When using this header field in a dialog-forming request or response
   or in a mid-dialog request or response, this field contains the local
   target, i.e., a URI used to reach the UA for mid-dialog requests and
   possibly out-of-dialog requests, such as a REFER request [RFC3515].
   The Contact header field can also contain a display-name. Since the
   Contact header field is used for routing further requests to the UA,
   the UA MUST include a functional URI even when it is anonymized.

   When using this header field in a dialog-forming request or response
   or in a mid-dialog request or response, the UA MUST anonymize the
   Contact header field using an anonymous URI ("temp-gruu") obtained
   through the GRUU mechanism, unless an equivalent functional anonymous
   URI is provided by some other means. For other requests and
   responses, with the exception of 3xx responses, REGISTER requests and
   200 (OK) responses to a REGISTER request, the UA MUST either omit the
   Contact header field or use an anonymous URI.

   Refer to Section 4.1 for details on how to obtain an anonymous URI
   through GRUU.

   The UA MUST omit the display-name in a Contact header field or set
   the display-name to "Anonymous".

5.1.2. From Header Field in Requests

   Without privacy considerations, this field contains the identity of
   the user, such as display-name and URI.

   RFCs 3261 and 3323 recommend setting
   "sip:anonymous@anonymous.invalid" as a SIP URI in a From header field
   when user privacy is requested. This raises an issue when the SIP-
   Identity mechanism [RFC4474] is applied to the message, because SIP-
   Identity requires an actual domain name in the From header field.

   A UA generating an anonymous SIP message supporting this
   specification MUST anonymize the From header field in one of the two
   ways described below.

   Option 1:

   A UA anonymizes a From header field using an anonymous display-name
   and an anonymous URI following the procedure noted in Section 4.1.1.3
   of RFC 3323.

The example form of the From header field of option 1 is as follows:

    From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=1928301774

Option 2:

A UA anonymizes a From header field using an anonymous display-name
and an anonymous URI with user's valid domain name instead of
"anonymous.invalid".

The example form of the From header field of option 2 is as follows:

    From: "Anonymous" <sip:anonymous@example.com>;tag=1928301774

A UA SHOULD go with option 1 to conceal its domain name in the From
header field. However, SIP-Identity cannot be used with a From
header field in accordance with option 1, because the SIP-Identity
mechanism uses authentication based on the domain name.

If a UA expects the SIP-Identity mechanism to be applied to the
request, it is RECOMMENDED to go with option 2. However, the user's
domain name will be revealed from the From header field of option 2.

If the user wants both anonymity and strong identity, a solution
would be to use a third-party anonymization service that issues an
Address of Record (AoR) for use in the From header field of a request
and that also provides a SIP-Identity Authentication Service. Third-
party anonymization service is out of scope for this document.

5.1.3. Via Header Field in Requests

Without privacy considerations, the bottommost Via header field added
to a request by a UA contains the IP address and port or hostname
that are used to reach the UA for responses.

A UA generating an anonymous SIP request supporting this
specification MUST anonymize the IP address in the Via header field
using an anonymous IP address obtained through the TURN mechanism,
unless an equivalent functional anonymous IP address is provided by
some other means.

The UA SHOULD NOT include a host name in a Via header field.

5.1.4. IP Addresses in SDP

   A UA generating an anonymous SIP message supporting this
   specification MUST anonymize IP addresses in SDP, if present, using
   an anonymous IP address obtained through the TURN mechanism, unless
   an equivalent functional anonymous IP address is provided by some
   other means.

   Refer to Section 4.2 for details on how to obtain an IP address
   through TURN.

5.2. Non-Critical Privacy-Sensitive Information

5.2.1. Host Names in Other SIP Header Fields

   A UA generating an anonymous SIP message supporting this
   specification SHOULD conceal host names in any SIP header fields,
   such as Call-ID and Warning header fields, if considered privacy-
   sensitive.

5.2.2. Optional SIP Header Fields

   Other optional SIP header fields (such as Call-Info, In-Reply-To,
   Organization, Referred-By, Reply-To, Server, Subject, User-Agent, and
   Warning) can contain privacy-sensitive information.

   A UA generating an anonymous SIP message supporting this
   specification SHOULD NOT include any information that identifies the
   user in such optional header fields.

6. Security Considerations

   This specification uses GRUU and TURN and inherits any security
   considerations described in these documents.

   Furthermore, if the provider of the caller intending to obscure its
   identity consists of a small number of people (e.g., small
   enterprise, Small Office, Home Office (SOHO)), the domain name alone
   can reveal the identity of the caller.

   The same can be true when the provider is large but the receiver of
   the call only knows a few people from the source of call.

   There are mainly two places in the message, the From header field and
   Contact header field, where the domain name is expected to be
   functional.

The domain name in the From header field can be obscured as described
in Section 5.1.2, whereas the Contact header field needs to contain a
valid domain name at all times in order to function properly.

Note: Generally, a device will not show the contact address to the
receiver, but this does not mean that one cannot find the domain name
in a message. In fact, as long as this specification is used to
obscure identity, the message will always contain a valid domain name
as it inherits key characteristics of GRUU.

Note: For UAs that use a temporary GRUU, confidentiality does not
extend to parties that are permitted to register to the same AoR or
are permitted to obtain temporary GRUUs when subscribed to the 'reg'
event package [RFC3680] for the AoR. To limit this, it is suggested
that the authorization policy for the 'reg' event package permit only
those subscribers authorized to register to the AoR to receive
temporary GRUUs. With this policy, the confidentiality of the
temporary GRUU will be the same whether or not the 'reg' event
package is used.

If one wants to assure anonymization, it is suggested that the user
seek and rely on a third-party anonymization service, which is
outside the scope of this document.

A third-party anonymization service provides registrar and TURN
service that have no affiliation with the caller's provider, allowing
caller to completely withhold its identity.

7. References

7.1. Normative References

   [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.

   [RFC5627]   Rosenberg, J., "Obtaining and Using Globally
                      Routable User Agent URIs (GRUUs) in the Session
                      Initiation Protocol (SIP)", RFC 5627, October 2009.

   [RFC5766]   Mahy, R., Matthews, P., and J. Rosenberg,
                        "Traversal Using Relays around NAT (TURN): Relay
                        Extensions to Session Traversal Utilities for NAT
                        (STUN)", RFC 5766, April 2010.

7.2. Informative References

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

   [RFC3325]   Jennings, C., Peterson, J., and M. Watson, "Private
                        Extensions to the Session Initiation Protocol (SIP)
                        for Asserted Identity within Trusted Networks",
                        RFC 3325, November 2002.

   [RFC3515]   Sparks, R., "The Session Initiation Protocol (SIP)
                        Refer Method", RFC 3515, April 2003.

   [RFC3680]   Rosenberg, J., "A Session Initiation Protocol (SIP)
                        Event Package for Registrations", RFC 3680,
                        March 2004.

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

   [SIPPING-CONFIG]   Channabasappa, S., "A Framework for Session
                        Initiation Protocol User Agent Profile Delivery",
                        Work in Progress, September 2009.

Authors' Addresses

   Mayumi Munakata
   NTT Corporation

   EMail: munakata.mayumi@lab.ntt.co.jp

   Shida Schubert
   NTT Corporation

   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