GEOPRIV
Internet-Draft
Intended status: Informational
Expires: April 20, 2007
H. Schulzrinne
Columbia U.
October 17, 2006

A Location Reference Event Package for the Session Initiation Protocol (SIP)
draft-schulzrinne-geopriv-locationref-00.txt

Status of this Memo

Copyright Notice

Abstract

Mobile devices sometimes want to give temporary access to their presence and location information to third parties that may not have a trust relationship with their presence server. Also, in addition to other mechanisms, application-layer location configuration protocols are helpful in building location-based systems. This document describes a Session Initiation Protocol (SIP) event package, locationref, that periodically delivers randomized presence URLs to

the target, which the target can then hand to call recipients and other parties.

Table of Contents

1. Terminology 3
2. Introduction 3
3. Assumptions 5
4. Goals 6
5. Finding the LIS 6
6. PIDF/PIDF-LO Parameter Setting 6
7. Event Package Formal Definition 7
7.1. Event Package Name 7
7.2. Event Package Parameters 7
7.3. SUBSCRIBE Bodies 8
7.4. Subscription Duration 8
7.5. NOTIFY Bodies 8
7.6. Notifier Processing of SUBSCRIBE Requests 9
7.7. Notifier Generation of NOTIFY Requests 9
7.8. Subscriber Processing of NOTIFY Requests 9
7.9. Handling of Forked Requests 9
7.10. Rate of Notifications 9
7.11. State Agents 9
8. Examples 10
9. Applicability Statement 12
10. Security Considerations 12
11. IANA Considerations 12
11.1. Registration of a new event package 12
11.2. Registration of event parameters 12
12. Acknowledgments 12
13. References 13
13.1. Normative References 13
13.2. Informative References 13
Author's Address 14
Intellectual Property and Copyright Statements 15

1. 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 RFC 2119 [1].

This document reuses terminology introduced by RFC 3693 [7] and [12]. We use the term Location Information Server (LIS) and Presence Server (PS) interchangable

2. Introduction

End systems need to be able to determine their geographic location, so that they can convey this information using SIP [2] or other protocols. Among many other possibilities, end systems can obtain location information from a location information server (LIS) via an application-layer protocol. The motivation and requirements for such a protocol are discussed in [12]. In particular, it is desirable that such a protocol work for mobile end systems, without requiring the end system to poll the LIS to find out if its location has changed. Thus, we need an event notification mechanism. Given the availability of SIP event notification [4] and the use of SIP for other purposes in many end systems, it makes sense to provide a SIP-based event notification for location-related events. This document defines the necessary event package.

Since the end system may move after sending location information in an INVITE request [13], for example, it is sometimes desirable to have the end system obtain a reference to a location object that can be converted into an event subscription by any recipient of such a reference, even if the LIS does not know the the location recipient and it has no way to verify the identity of the location recipient. For example, in emergency calling, the PSAP or first-responder may want to track the location of the caller during the emergency, but it is unlikely that a LIS can authenticate the PSAP or first responder.

Reflecting the needs of the end system and other system components, we define a new event package, locationref, that can be combined with the 'presence' event package [8] to support two operational modes. In both cases, the LIS, acting as a presence agent (PA), periodically delivers a new randomized SIP URL to the watcher via SIP NOTIFY requests. This randomized SIP URL can be used, without further authentication and authorization, to subscribe to presence information for the end system, typically including location information encoded as a PIDF-LO [10]. We refer to this SIP URL as a randomized presence retrieval URL, or an RPRU for short.

The RPRU has a finite, typically short, lifetime and becomes invalid after that time expires. For the applications envisioned, such as emergency calling or location-based delivery services, it appears sufficient for a URL to be valid for about one hour. Since the target to be located may distribute the URL just before the next one is delivered, the RPRU MUST be valid at least one hour beyond its replacement. Thus, the LIS must store randomized URLs with overlapping lifetime for each target and MUST provide a new URL one hour before the last one expires. For the default validity period of one hour, a new URL is delivered via NOTIFY once an hour, with the randomized URL having a validity period of two hours.

The system can operate in two modes:

Network-identifier-based location: In this mode, the end system subscribes to the locationref at the LIS, providing one or more node identifiers as event package parameters. Here, we define the IP address, MAC address and a switch-and-port identifier, but other node identifiers can be added in the future. The end system does not authenticate with the LIS and does not use its SIP address-of-record (AOR).

AOR-based location reference: Here, the end system subscribes to location references based on its AOR, rather than a network identifier. In particular, the UA may provide the location information to the PA via PUBLISH [5] requests. For example, a UA with a built-in GPS receiver could PUBLISH geolocation updates to the PA, and then hand out SIP URLs to callees that need to temporarily track or obtain its location.

TBD: It might be desirable to allow end systems to directly subscribe to presence information using the node identifiers, to avoid the duplicate notifications and subscriptions. This would require extending the presence event package [8] with additional parameters or creating a new 'location' event package parallel to the package defined here.

Figure 1 shows a protocol exchange that allows the UA to obtain a RPRU pointing to a PIDF-LO stored at the LIS in the access network. Note that the discovery exchange is not known in this figure and it it also not described in this document. First, the target sends a SUBSCRIBE with the event package 'locationref'. This message is protected using Transport Layer Security, which is also not shown in the figure. The LIS, for example, uses the IP address of the target (as carried in the SUBSCRIBE request) to determine its current location information and creates a RPRU. The RPRU is returned to the Target in a NOTIFY message (here, xu...56@lis for short). The subsequent exchange points to a potential usage case of conveying location information to a location recipient whereby the RPRU is then

carried in an INVITE message. A location recipient then uses the obtained reference to initiate a SUBSCRIBE followed by a NOTIFY message containing a PIDF-LO.

```
    +----------+      +-----------+                   +-----------+
    |          |      |           |                   | Location  |
    |   UA     |      |   LIS     |                   | Recipient |
    |          |      |           |                   |           |
    +-----+----+      +-----+-----+                   +-----+-----+
          |                 |                               |
          |                 |                               |
          |SUBSCRIBE        |                               |
          |---------------->|                               |
          |Event:locationref|                               |
          |                 |                               |
          |                 |                               |
          |NOTIFY           |                               |
          |<----------------|                               |
          |sip:xu...56@lis  |                               |
          |                 |                               |
          |                 |                               |
          |INVITE           |                               |
          |-----------------+------------------------------>+---------
          |Geolocation:     |                               |
          |xu...56@lis      |                               |
          |                 |   SUBSCRIBE xu...56@lis       |
          |                 |<------------------------------|
          |                 |   Event: presence             |
          |                 |                               |
          |                 |   NOTIFY sip:proxy.com        |
          |                 |------------------------------>|
          |                 |   PIDF-LO                     |
          |                 |                               |
```

Figure 1: Basic Message Exchange

3. Assumptions

This document makes the following assumptions:

- o The LIS is located in the access network and a corresponding LIS discovery mechanism is available, for example via a reverse DNS lookup or a DHCP option.
- o The LIS discovery procedure makes the domain name required for the SIP URI available to the target.

- The target is not assumed to share credentials with the LIS. The target does not authenticate to the LIS when creating the RPRU.
- This document only creates presence URIs that can be resolved into location objects by using the SIP presence mechanisms.
- The usage of authorization policies for controlling the access to PIDF-LOs are not envisioned or at least they are not provided by the target itself.

4. Goals

This document aims to provide a mechanism that offers the following functionality:

- It enables the end host to obtain a reference to a PIDF-LO from the LIS. The LIS is a SIP presence server. The reference is in the form of a a presence URI, the RPRU.
- The entity that knows the reference can subscribe to it in order to obtain the location object in the form of a PIDF-LO [10]. Every entity that is in possession of the RPRU can resolve it. There are no authorization policies that need to be uploaded from the target, or any other node, to the LIS for access control of a potential location recipient. Any node can play the role of a location recipient as long as it knows the RPRU (e.g., the Target, a Public Safety Answering Point (PSAP) or location/presence server).

5. Finding the LIS

The LIS can be discovered via DHCP, as described in [TBD]. If there is no such mechanism, the UA employs the normal SIP location mechanism [3], using its own domain name as the host name. The domain is determined from the domain name of the end host, typically conveyed as part of the configuration information or obtainable from the public IP address via DNS PTR records. (This mechanism works only if the end host is not designated as the SIP server for itself.)

6. PIDF/PIDF-LO Parameter Setting

To ensure the privacy of the target, the location object returned by the RPRU should observe certain conventions. Also, since the PIDF-LO itself is created by a node that does not know a number of parameters it needs to be constructed in a way that is privacy safe. The following PIDF-LO parameter usage is REQUIRED:

'usage-rules' Element:
retransmission-allowed: This element MUST be set to 'no'.
retention-expires: This field specifies an absolute date at which time the Recipient is no longer permitted to possess the location information and its encapsulating Location Object. The value of this field MUST be computed based on the lifetime of the presence URI, i.e., the Location Object and the presence URI MUST have the same lifetime.
ruleset-reference: This element SHOULD NOT contain a URI to an external set of privacy rules. Reason: The LIS is less likely in the position to know the reference to the ruleset.
note-well: This element SHOULD NOT contain a human readable privacy statement. Reason: The LIS does not know the human readable privacy statement of the user.
'method' Element: This element SHOULD contain information about the way how location information was derived or discovered.
'provided-by' Element: This element might SHOULD contain the entity or organization that supplied this location information. Since the PIDF-LO is not signed it is highly RECOMMMENDED to provide information within this element.
'entity' Attribute of the <presence> Element: The value of the 'entity' attribute (see [9]) MUST be set based on the RPRU.

7. Event Package Formal Definition

This section fills in the information required for all event packages by RFC 3265 [4].

7.1. Event Package Name

This document defines a SIP Event Package as defined in [4]. The event-package token name for this package is:

"locationref"

7.2. Event Package Parameters

This package defines an extensible set of event parameters that are used to identify the user agent as a network node. Currently, three identifiers are described; their tradeoffs are enumerated in the [12]. Additional parameters can be defined through an IANA registry.

ip The 'ip' parameter contains an IPv4 or IPv6 address, written in the format specified in [6], as either IP-literal or IPv4address. An example is ;ip="192.0.34.186". If this parameter is included, the SIP Contact header field MUST be identical to this value. (TBD: How to ensure that only the real owners of the IP address can usefully insert this address in the event parameter.)

mac The 'mac' parameter contains an IEEE MAC address written in IEEE EUI-64 or EUI-48 notation, with lower-case hexadecimal characters separated by colons. An example is ;mac="0:3:fc:0:ca:27".

msap The 'msap' parameter identifies a MAC service access point, typically a switch chassis and port. If derived from LLDP (IEEE 802.1ab), it is encoded in base64. (TBD: Should there be a separate identifier for CDP and other protocols that provide alphanumeric chassis and port information?)

End systems SHOULD provide all available identifiers. The PA can choose any one of the parameters, depending on its own internal database and possibly on which identifier is less subject to spoofing.

7.3. SUBSCRIBE Bodies

A SUBSCRIBE request body MAY contain a filter or policy document restricting access to the information accessible through the randomized URL. (TBD: This might allow the UA to upload information to the LIS that can then be placed in the PIDF-LO but introduces complexity and might raise a number of privacy concerns. Instead of sending the RPRU directly to location recipients the UA makes the RPRU available to its presence server and thereby ensures that authorization policies are applied in the classical fashion.)

7.4. Subscription Duration

Typically, an end system would either perform a one-time subscription with zero duration or continuously acquire new randomized location URLs. By default, NOTIFY requests will be delivered to the watcher at the rate of one per hour, so that a subscription duration of one day (86400 seconds) is chosen as a default to amortize the subscription overhead over a sufficient number of notifications. As per RFC 3265 [4], the subscriber MAY specify an alternate expiration in the Expires header field.

7.5. NOTIFY Bodies

Notifiers MAY send location information in any format acceptable to the subscriber, based on the information contained in the Accept header field in the SUBSCRIBE request. All implementations of this event package MUST support the text/uri-list content type and deliver

one or more randomized URLs to the watcher. All such URIs have the same functionality, but may use different schemes. The ordering of the URLs is immaterial. The username part of the presence URI MUST NOT contain any information that identifies the user, device or address of record. The username part of the presence URI MUST be hard to guess, i.e., it MUST contain a cryptographically random component of at least 128 bit length.

7.6. Notifier Processing of SUBSCRIBE Requests

SUBSCRIBE requests are addressed to the host name of the LIS, without a 'user' part in the request URI. For example, if the LIS resides at lis.example.com, the SUBSCRIBE request is directed to sip: lis.example.com.

When the notifier receives a SUBSCRIBE request, it attempts to verify that the event parameters indeed belong to the subscribing UAC.

7.7. Notifier Generation of NOTIFY Requests

Immediately after a subscription has been accepted, the notifier MUST send a NOTIFY with a new RPRU. One hour before the expiration of the last RPRU, the notifier sends a new RPRU.

7.8. Subscriber Processing of NOTIFY Requests

There are no special rules for locationref NOTIFY requests.

7.9. Handling of Forked Requests

This document follows the presence event package [8], Section 6.9, in handling forked SUBSCRIBE requests.

7.10. Rate of Notifications

By default, this event package will generate a new RPRU every hour. Shorter intervals are unlikely to be useful, given the need for the RPRU to be valid for a reasonable time period.

7.11. State Agents

This document does not preclude implementations from building state agents which support this event package. Likewise, this document does not preclude subscriptions to lists of resources using the event list extension [11].

8. Examples

In the examples below, we omit standard responses for brevity. We assume that the UA, located at host17.example.com (192.0.34.166), has determined the location of the LIS, e.g., via DHCP, here lis.example.com.

```
SUBSCRIBE sip:lis.example.com SIP/2.0
Via: SIP/2.0/TCP target.example.com;branch=z9hG4bKnashds7
To: &lt;sip:lis.example.com>
From: &lt;sip:target.example.com>;tag=xfg9
Call-ID: 2010@target.example.com
CSeq: 17866 SUBSCRIBE
Max-Forwards: 70
Event: locationref;ip="192.0.34.166";mac="0:3:fc:0:ca:27"
Accept: text/uri-list
Contact: &lt;sip:user@target.example.com>
Expires: 86400
Content-Length: 0
```

The NOTIFY returned by the LIS might look as follows:

```
NOTIFY sip:user@target.example.com SIP/2.0
Via: SIP/2.0/TCP server.example.com;branch=z9hG4bKna998sk
From: &lt;sip:lis.example.com>;tag=ffd2
To: &lt;sip:user@target.example.com>;tag=xfg9
Call-ID: 2010@target.example.com
Event: locationref
Subscription-State: active;expires=86399
Max-Forwards: 70
CSeq: 8775 NOTIFY
Contact: sip:lis.example.com
Content-Type: text/uri-list
Content-Length: ...

# your random presence retrieval URL, valid for two hours
sips:nt5n09r97952....816@lis.example.com
```

The UAC then inserts this URL into outgoing SIP requests, such as

```
INVITE urn:service:sos SIP/2.0
Geolocation: sips:nt5n09r97952....816@lis.example.com
```

```
SUBSCRIBE sip:nt5n09r97952x816@lis.example.com SIP/2.0
Via: SIP/2.0/TCP psap.example.net;branch=z9hG4bKxkuvads7
To: &lt;sip:nt5n09r97952x816@lis.example.com>
From: &lt;sip:alice@psap.example.net>;tag=xab1
Call-ID: 1234@psap.example.com
CSeq: 4986 SUBSCRIBE
Max-Forwards: 70
Event: presence
Accept: application/pidf+xml
Contact: &lt;sip:alice@psap.example.com>
Expires: 3600
Content-Length: 0
```

If the RPRU is still valid, the LIS will return

```
NOTIFY sip:alice@psap.example.com SIP/2.0
Via: SIP/2.0/TCP lis.example.com;branch=z9hG4bKna998sk
From: &lt;sip:nt5n09r97952x816@lis.example.com>;tag=ffd2
To: &lt;sip:user@example.com>;tag=xab1
Call-ID: 1234@psap.example.com
Event: presence
Subscription-State: active;expires=4200
Max-Forwards: 70
CSeq: 7812 NOTIFY
Contact: sip:lis.example.com
Content-Type: application/pidf+xml
Content-Length: ...
```

9. Applicability Statement

A future version of this document will provide information regarding its appliability.

10. Security Considerations

The security considerations in [12] apply here.

Without a cryptographic identifier for hosts, there are only two mechanisms for making it difficult for end systems to impersonate other devices. First, the LIS can enforce return routability, so that only the network-layer originator of the request can see a response or subsequent message. Secondly, another protocol can be used to deliver an 'identifier' to the end system that can only be seen by that end system and is used as a lookup key in the SUBSCRIBE request. For example, if the MSAP is sufficiently long and cryptographically random, a third party would not be able to guess the value and obtain the location keys of other nodes. The IP address and the MAC address obviously do not fulfill this requirement.

The security of the randomized URL depends on the channel security of the protocols used to carry it. For conveyance within SIP, use of SIPS is RECOMMENDED.

11. IANA Considerations

11.1. Registration of a new event package

Package name: locationref
Type: package
Contact: Schulzrinne
Published Specification: This document.

11.2. Registration of event parameters

This document requests that IANA establish a registry for event parameters for the locationref event package.

12. Acknowledgments

This document has been influenced by the earlier work by Rohan Mahy, in the expired Internet draft draft-mahy-geopriv-sip-loc-pkg. The notion of randomized URLs has been discussed under the label of "pawn

tickets" in the working group.

The authors would like to thank the Geopriv L7 design team (the members are listed in Section 11 of [12]) for motivating this document.

Jonathan Rosenberg, Brian Rosen, Marc Linsner, Hannes Tschofenig and Jon Peterson contributed to the design.

13. References

13.1. Normative References

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

[2] 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.

[3] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[4] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[5] Niemi, A., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, October 2004.

[6] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

13.2. Informative References

[7] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[8] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004.

[9] Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W., and J. Peterson, "Presence Information Data Format (PIDF)", RFC 3863, August 2004.

[10] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[11] Roach, A., Campbell, B., and J. Rosenberg, "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", RFC 4662, August 2006.

[12] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-tschofenig-geopriv-l7-lcp-ps-02 (work in progress), August 2006.

[13] Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", draft-ietf-sip-location-conveyance-04 (work in progress), August 2006.

Author's Address

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7004
Email: hgs+geopriv@cs.columbia.edu
URI: http://www.cs.columbia.edu

Full Copyright Statement

Intellectual Property

Acknowledgment

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