Internet Engineering Task Force
Internet Draft
Expiration: Aug 9th, 2004
File: draft-ietf-sipping-location-requirements-00.txt

James M. Polk
Cisco Systems
Brian Rosen
Marconi

Requirements for Session Initiation Protocol Location Conveyance

February 9th, 2003

Status of this Memo

Abstract

This document presents the framework and requirements for an

extension to the Session Initiation Protocol (SIP) [1] for conveyance of user location information from a Session Initiation Protocol (SIP) user agent to another SIP entity. We consider cases where location information is conveyed from end to end, as well as cases where message routing by intermediaries is influenced by the location of the session initiator.

Table of Contents

1. Introduction

This document presents the framework and requirements for an extension to the Session Initiation Protocol (SIP) [1] for conveyance of user location information object described by [7] from a SIP User Agent to another SIP entity.

There are several situations in which it is appropriate for SIP to be used to convey Location Information (LI) from one SIP entity to another. This document specifies requirements when a SIP UAC knows its location by some means not specified herein, and needs to inform another SIP entity. One example is to reach your nearest pizza parlor. A chain of pizza parlors may have a single well known uri (sip:pizzaparlor.com), that is forwarded to the closest franchise by the pizzaparlor.com proxy server. The receiving franchise UAS uses the location information of the UAC to schedule your delivery.

Another important example is emergency calling. A call to sip:sos@example.com is an emergency call as in [3]. The example.com proxy server must route the call to the correct emergency response center (ERC) determined by the location of the caller. At the ERC, the UAS must determine the correct police/fire/ambulance/... service, which is also based on your location. In many jurisdictions, accurate location information of the caller in distress is a required component of a call to an emergency center.

A third example is a direction service, which might give you verbal directions to a venue from your present position. This is a case where only the destination UAS needs to receive the location information.

This document does not discuss how the UAC discovers or is

configured with its location (either coordinate or civil based). It also does not discuss the contents of the Location Object (LO). It does specify the requirements for the "using protocol" in [7].

1.1 Conventions used in this document

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 [2].

1.2 Changes from Individual Submission Versions

This is a list of the changes that have been made from the -00 individual submission version of this ID:

- Brian Rosen was brought on as a co-author

- Requirements that a location header were negatively received in the previous version of this document. AD and chair advice was to move all location information into a message body (and stay away from headers)

- Added a section of "emergency call" specific requirements

- Added an Open Issues section to mention what hasn't been resolved yet in this effort

This is a list of the changes that have been made from the individual submission version -01

- Added the IPR Statement section

- Adjusted a few requirements based on suggestions from the Minneapolis meeting

- Added requirements that the UAC is to include from where it learned its location in any transmission of its LI

- Distinguished the facts (known to date) that certain jurisdictions relieve persons of their right to privacy when they call an ERC, while other jurisdictions maintain a person's right to privacy, while still others maintain a person's right to privacy - but only if they ask that their service be set up that way.

- Made the decision that TLS is the security mechanism for location conveyance in emergency communications (vs. S/MIME, which is still the mechanism for UA-to-UA non-emergency location conveyance cases).

- Added the Open Issue of whether a Proxy can insert location information into an emergency SIP INVITE message, and some of the open questions surrounding the implications of that action

- added a few names to the acknowledgements section

2. In the Body or in a Header

When one user agent wants to inform another user agent where they are, it seems reasonable to have this accomplished by placing the location information (coordinate or civil) in an S/MIME registered and encoded message body, and sending it as part of a SIP request or response. No routing of the request based on the location information is required in this case; therefore no SIP Proxies between these two UAs need to view the location information contained in the SIP messages.

Although SIP [1} does not permit a proxy server to modify or delete a body, there is no restriction on viewing bodies. However, S/MIME protection implemented on bodies is only specified between UAS and UAC, and if engaged, would render the location object opaque to a proxy server for any desired modification if it is not correct or precise enough from that proxy's point of view (were it to be able to view it). This problem is similar to that raised in Session Policy [8], where an intermediary may need information in a body, such as IP address of media streams or codec choices to route a call properly. Requirements in [8] are applicable to routing based on location, and are incorporated in these requirements by reference.

It is conceivable to create a new header for location information. However, [7] prefers S/MIME for security of Location Information, and indeed S/MIME is preferable in SIP for protecting one part of a message. Accordingly, these requirements specify location be carried in a body.

It is the use of S/MIME however, that limits routing based on location. Therefore, it seems appropriate to require that, where routing is dependent on location, protection of the location information object be accomplished by other mechanisms: here TLS ("sips:" from [1]). It is envisioned that S/MIME SHOULD be used when location information is not required by proxy servers, and TLS MUST be used when it is. The UAC will need to know the difference

in the call's intent as to which security mechanism to engage for LI conveyance.

This document does not address the behavior or configuration of SIP Proxy Servers in these cases in order to accomplish location-sensitive routing. That is out of scope, and left for further (complementary) efforts.

3. Scope of Location in a Message Body

As concluded from the previous section, location information is to be contained within a message body. If either another body (SDP for example) is also to be sent in the message, or the LI is to be protected with S/MIME, the rules stated in section 7 of [1] regarding multipart MIME bodies MUST be followed. The format and privacy/security rules of the location information SHOULD be defined within the Geopriv WG.

4. Requirements for UA-to-UA Location Conveyance

The following are the requirements for UA-to-UA Location Conveyance Situations where routing is not based on the LI of either UA:

U-U1 - MUST work with dialog-initiating SIP Requests and responses, as well as the SIP MESSAGE method[4], and SHOULD work with most SIP messages.

U-U2 - UAC Location information SHOULD remain confidential in route to the destination UA.

U-U3 - The privacy and security rules established within the Geopriv Working Group that would categorize SIP as a 'using protocol' MUST be met [7].

U-U4 - The UAC SHOULD indicate in the SIP message that includes location information where the LI came from (IANA registered codes for GPS, Cell Tower Triangulation, WiFi, DHCP, manual entry - as examples).

5. Requirements for UA-to-Proxy Server Location Conveyance

The following are the requirements for UA-to-Proxy Server Location Conveyance situations:

U-PS1 - MUST work with dialog-initiating SIP Requests and

responses, as well as the SIP MESSAGE method[4], and SHOULD work with most SIP messages.

U-PS2 - UAC location information SHOULD remain confidential with respect to entities to which the location information is not addressed, but MUST be useable by intermediary proxy servers.

U-PS3 - The privacy and security rules established within the Geopriv Working Group which would categorize SIP as a 'using protocol' MUST be met [7].

U-PS4 - Modification or removal of the LO by proxy servers MUST NOT be required (as [1] currently forbids this).

U-PS5 - any mechanism used to prevent unwanted observation of this Location Information CANNOT fail the SIP Request if not understood by intermediary SIP entities or the destination UAS.

U-PS6 - Proxy Servers that do not or cannot understand the Location Information in the message body for routing purposes MUST NOT fail the SIP Request.

U-PS7 ¡ It MUST be possible for a proxy server to assert the validity of the location information provided by the UA. Alternatively, it is acceptable for there to be a mechanism for a proxy server to assert a location object itself.

U-PS8 - The UAC SHOULD indicate in the SIP message that includes location information where the LI came from (IANA registered codes for GPS, Cell Tower Triangulation, WiFi, DHCP, manual entry - as examples).

6. Additional Requirements for Emergency Calls

Emergency calls have requirements that are not generally important to other uses for location in SIP:

Emergency calls presently have between 2 and 8-second call setup times. There is ample evidence that the longer call setup end of the range causes an unacceptable number of callers to abandon the call before it is completed. Two-second call completion time is a goal of many existing emergency call centers. Allocating 25% of the call set up for processing privacy concerns seems reasonable; 1 second would be 50% of the goal, which seems unacceptable; less than 0.5 second seems unachievable, therefore:

E-1 - Privacy mechanisms MUST add no more than 0.5 second of call setup time when implemented in present technology UAs and Proxy Servers.

It may be acceptable for full privacy mechanisms related to the location of the UAC (and it's user) to be tried on an initial attempt to place a call, as long as the call attempt may be retried without the mechanism if the first attempt fails. Abandoning privacy in cases of failure of the privacy mechanism might be subject to user preference, although such a feature would be within the domain of a UA implementation and thus not subject to standardization. It should be noted that some jurisdictions have laws that explicitly deny any expectation of location privacy when

making an emergency call, while others grant the user the ability to remain anonymous even when calling an ERC. So far, this has been offered in some jurisdictions, but the user within that jurisdiction must state this preference, as it is not the default configuration.

E-2 ¡ Privacy mechanisms MUST NOT be mandatory for successful conveyance of location during an (sos-type) emergency call.

E-3 - It MUST be possible to provide a privacy mechanism (that does not violate the other requirements within this document) to a user within a jurisdiction that gives that user the right to choose not to reveal their location even when contacting an ERC.

E-4 ¡ The retention and retransmission policy of the ERC MUST be able to be made available to the user, and override the user's normal policy when local regulation governs such retention and retransmission (but does not violate requirement E-3). As in E-2 above, requiring the use of the ERC's retention and/or retransmission policy may be subject to user preference although in most jurisdictions, local laws specify such policies and may not be overridden by user preference.

Location information is considered so important during emergency calls, that it is to be transmitted even when it is not considered reliable, or might even be wrong. For example, some application might know that the DHCP reply with location information was overwritten recently (or exactly) when a VPN connection was activated. This could, and likely will, provide any new location information to the UA from somewhere far away from the UA (perhaps the user's corporate facility).

E-5 Location information MUST be transmitted, if known to the UAC, in all calls to an ERC, even in the case it is not considered reliable.

E-6 The UAC SHOULD be able to inform the ERC that the location information provided in the SIP message might be wrong.

Requirements U-U4 and U-PS8 stipulate the inclusion of how the UAC learned its location. This can be especially useful to an ERC

operator attempting to learn all that is possible from this remote person in distress. With that in mind, it is important to distinguish the location information learned locally from LI learned over a VPN; which in itself is useful additional information to that ERC operator.

E-7 The UA MUST not provide the (overwritten?) location information provided by a VPN (in lieu of the LI from the local network).

E-8 The UA SHOULD include within the location conveyance to the ERC that it is (or recently was) connected to a VPN.

7. Current Known Open issues

This is a list of open issues that have not yet been addressed to conclusion:

1) Whether SIP Proxies SHOULD be able to insert location information into an emergency call set-up (the INVITE)?

1a) This has the additional implication of whether or not, or regardless of the fact the UAC already inserted location into the sos@localdomain INVITE.

1b) Should the Proxy somehow differentiate its location information from that provided by the UAC (with each LI having a SIP entity (type?) originator label?

1c) Should there be any behavior difference with respect to Open Issue #1b if the Proxy does not know or cannot tell if the UAC inserted location information (further emphasizing the need for some form of originator label)?

2) Whether SIP Proxies SHOULD be able to return location information in a Redirect message to the UAC making the emergency call?

3) If S/MIME is chosen as a SHOULD (in general, vs. TLS), this doc might consider stipulating a special purpose Proxy (an "emergency services" proxy) that can process location information (a Geopriv LO) and route the message directly to the appropriate ERC.

At Issue: plain "vanilla" proxies probably won't have the capabilities to route based on location information in the near future, but should that timing be considered here?

8. Security Considerations

Conveyance of geo-location of a UAC is problematic for many reasons. This document calls for that conveyance to normally be accomplished through secure message body means (like S/MIME or TLS). In cases where a session set-up is routed based on the location of the UAC initiating the session or SIP MESSAGE, securing the location with an end-to-end mechanism such as S/MIME is problematic.

9. IANA Considerations

There are no IANA considerations within this document at this time.

10. Acknowledgements

To Dave Oran for helping to shape this idea. To Jon Peterson and Dean Willis on guidance of the effort. To Henning Schulzrinne, Jonathan Rosenberg, Dick Knight, and Keith Drage for constructive feedback.

11. References - Normative

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

[2] S. Bradner, "Key words for use in RFCs to indicate requirement levels," RFC 2119, Mar. 1997.

[3] H. Schulzrinne, "draft-schulzrinne-sipping-sos-04.txt", Internet Draft, Jan 03, Work in progress

[4] B. Campbell, Ed., J. Rosenberg, H. Schulzrinne, C. Huitema, D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging" , RFC 3428, December 2002

[5] J. Polk, J. Schnizlein, M. Linsner, " draft-ietf-geopriv-dhcp-lci-option-03.txt", Internet Draft, Dec 2003, Work in progress

[6] H. Schulzrinne, "draft-schulzrinne-geopriv-dhcp-civil-01.txt", Internet Draft, Feb 03, Work in progress

[7] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk, "draft-ietf-geopriv-reqs-04.txt", Internet Draft, Oct 03, Work in progress

[8] J. Rosenberg, "Requirements for Session Policy for the Session Initiation Protocolö, draft-ietf-sipping-session-policy-req-00", Internet Draft, "work in progress" June, 2003

12. Author Information

James M. Polk
Cisco Systems
2200 East President George Bush Turnpike
Richardson, Texas 75082 USA
jmpolk@cisco.com

Brian Rosen
Marconi Communications, Inc.
2000 Marconi Drive
Warrendale, PA 15086
Brian.rosen@marconi.com

IPR Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

The Expiration date for this Internet Draft is:

August 9th, 2004