

Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 18, 2008

J. Peterson
NeuStar
T. Hardie
Qualcomm
J. Morris
CDT
February 15, 2008

Implications of <retransmission-allowed> for SIP Location Conveyance
draft-peterson-geopriv-retransmission-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 18, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document explores an ambiguity in the interpretation of the <retransmission-allowed> element of the Presence Information Data Format for Location Objects (PIDF-LO) in cases where PIDF-LO is conveyed by the Session Initiation Protocol (SIP). It provides recommendations for how the SIP location conveyance mechanism should

Internet-Draft

Retransmission

February 2008

adapt to these ambiguities.

Table of Contents

1.	Introduction	3
2.	Problem Statement	3
3.	Solution Space	5
3.1.	Indicating Permission	5
3.2.	Withholding Location	7
4.	Analysis	8
5.	Recommendation	10
6.	IANA Considerations	10
7.	Security Considerations	10
8.	Informational References	10
	Authors' Addresses	11
	Intellectual Property and Copyright Statements	12

Internet-Draft

Retransmission

February 2008

1. Introduction

The Presence Information Data Format for Location Objects (PIDF-LO [\[4\]](#)) carries both location information (LI) and policy information set by the Rule Maker, as is stipulated in [RFC3693](#) [\[3\]](#). The policy carried along with LI allows the Rule Maker to restrict, among other things, the duration for which LI will be retained by recipients and the redistribution of LI by recipients.

The Session Initiation Protocol ([RFC3261](#) [\[1\]](#)) is one proposed Using Protocol (see [RFC3693](#)) for PIDF-LO. The conveyance of PIDF-LO within SIP is specified in [\[5\]](#). The common motivation for providing LI in SIP is to allow location-based personal communications services. One example would be emergency services; another would be fast food delivery.

Some ambiguities have arisen in the interpretation of Rule Maker policy when PIDF-LO is conveyed by SIP. The following sections explore the problem and possible solutions before providing a recommendation.

2. Problem Statement

The <retransmission-allowed> element of [RFC4119](#) was designed for use in an environment like that of [Section 4 of RFC3693](#), in which Location Information (LI) propagates from a Location Generator through a Location Server to a Location Recipient. In this architecture, it is the responsibility of the Location Server to act on the rules (policy) governing access control to LI, which are in turn set by the Rule Maker. The most important of these responsibilities is delivering LI to authorized Location Recipients and denying it to others. Internal to [RFC4119](#)-compliant location objects (LOs) are additional privacy rules which are intended to constrain Location Recipients. These include the <retransmission-allowed> element. This element is intended to prevent a compromise

of privacy when an authorized recipient of LI shares that LI with third-party entities, principally those who are not authorized by the Rule Maker to receive LI. For example, a user might be willing to share their LI with a pizza shop, but they might not want that pizza shop to sell their LI to a targeted advertising company that will contact the user with coupons for a nearby hair salon.

Bear in mind, however, that <retransmission-allowed> is not intended to provide any protocol-level mechanism to prevent unauthorized parties from learning location through means like eavesdropping. It is merely a way to express the preferences of the Rule Maker to the LR. If the LR were, for example, legally bound to follow the privacy

preferences expressed by Rule Makers, then they might incur liability if they ignored the <retransmission-allowed> parameter. No further privacy protection is assumed to be provided by <retransmission-allowed>.

There is a use case for LI that involves embedding it in a SIP request that will potentially traverse multiple SIP intermediaries before arriving at a UAS. In this use case, one or more intermediaries may inspect the LI in order to make a SIP routing decision; we will hereafter refer to this as location-based routing. Common examples would include emergency services and other more mundane cases where the originator of a SIP request wants to reach a service in proximity to a particular geographic location, such as contacting a nearby pizza shop. In both such cases the UAC may intend for selected intermediaries and the UAS to have access to the LI. In the pizza case, for instance, the UAC shares an address both for location-based routing and additionally so that the pizza shop reached by that routing has the address to which a pizza should be sent.

This location-based routing use case for LI has a number of important disconnects from the [RFC3693](#) model. Unlike the [RFC3693](#) model, there is no LS designating to which specific entities LI will be sent. There may be multiple intermediaries between the UAC and UAS, some of which need or want to inspect LI (which would seem to qualify them as LRs) and some of them will not. While SIP proxy servers generally are not [RFC4119](#)-aware and do not need to inspect SIP request bodies in order to perform their function, nothing however precludes proxy servers inspecting or logging any SIP message bodies, including LI.

Furthermore, it is very difficult for the UAC to anticipate which intermediaries and which eventual UAS a SIP request might reach.

This architecture is further complicated by the possibility of sending location information by-reference, that is, placing a URL where LI can be retrieved in SIP requests instead of a by-value PIDF-LO body - depending on the qualities of a reference, further authorization checks may be performed before LI is retrieved, LI may be customized depending on who is asking, and so forth. The conveyance of a reference may have very different privacy properties than conveying a PIDF-LO body by-value in a SIP request.

In these location-based routing cases, a number of questions and concerns arise when <retransmission-allowed> is set to "no". The core concern is "to whom does <retransmission-allowed> apply in location-based routing?" More specifically:

Is any entity that reads LI bound by <retransmission-allowed> If so, does that mean a proxy that performs location-based routing is unable to forward a request and complete a SIP call if

<retransmission-allowed> is not to "no" unless they strip location out of the message? This interpretation is fairly problematic, and a solution is required to allow location-based routing to take place.

By forwarding a request at all, is a SIP proxy violating [RFC4119](#)? Of course, not all proxies understand [RFC4119](#), but is any entity that potentially could read LI under an obligation to read it if only to learn that it is not authorized to retransmit it? Is there a need for SIP-level indications regarding retransmission for the benefit of entities that do not understand 4119?

If the UAC cannot anticipate who may receive a SIP request, how do we understand who the intended LR is in the location-based routing case? Can a UAC intended for there to be multiple serial LRs in a transmission? If so, if one LR is authorized to retransmit to another LR, how will it know it is not also authorized to transmit LI to other third parties (i.e., how will the serial LRs know to whom they are authorized to retransmit)? How could all of this be designated?

[3.](#) Solution Space

At a high level, a solution for this problem would enable location-based routing to work even when the <retransmission-allowed> flag is set to "no". Ideally, it would give the Rule Maker responsible for L0 policy the ability to allow or forbid the use of LI for location-based routing, and similarly allow or forbid the use of LI for the consumption of the endpoint.

It is important to note that whatever the solution turns out to be, solving this problem does not obviate the need to explain the meaning of <retransmission-allowed> "no" in the absence of the solution. This work cannot be complete without an account of how <retransmission-allowed> is to be understood.

[3.1.](#) Indicating Permission

A SIP message conveying location information could contain some sort of indication that allows location-based routing, or more specifically specifies what entity or entities are intended to consume the LI. This admits of varying degrees of specificity: a binary indicator might say only whether or not routing is allowed, a more complex indicator might allow and/or disallow both routing and consumption by endpoints, or a very specific indicator might designate (by hostname, for example) a list of exactly which entities on the SIP signaling path are intended to inspect PIDF-L0.

In order for indicators with a great deal of specificity to serve

their purpose, the sender of SIP requests must be able to anticipate the path and ultimate destination of messages. In most operational environments this is a more complicated matter than one might think. The manner in which proxy servers make forwarding decisions is unpredictable to the originating UAC, as are any registrations that might be associated with the destination AoR, which might point to unexpected endpoints or new AoRs. Thus, solutions along the lines of specifying an exact list of hosts that a request will visit have very limited applicability.

It may even be difficult for the originator of a SIP request to anticipate whether an intermediary or endpoint will need to inspect LI to process a request. In sending a request to sip:orders@pizzahut.example.com, for instance, the UAC cannot anticipate whether pizzahut.example.com uses location-based routing

to direct requests to particular retail outlets, or whether the location information is consumed by a centralized monolithic endpoint that dispatches orders in some manner outside the scope of SIP and PIDF-LO. That much said, a binary indicator used to authorize location-based routing (something like "routing=yes") would at least serve to allow location-based routing to occur when <retransmission-allowed> is set to "no".

Placing the indicator in the Location header has the advantage that a recipient need not inspect the PIDF-LO body in order to learn whether or not they are supposed to inspect it. Parsing an XML body also entails a computational expense that may be burdensome for an intermediary processing large numbers of messages, especially in cases where the parsing yields nothing more than a stop sign.

Placing the indicator within the PIDF-LO object has the advantage of binding the indicator to the other policy elements in PIDF-LO. Were the indicator to appear in a SIP header, it would be unclear who set the indicator and what the relationship of that entity might be to the Rule Maker. Furthermore, were the PIDF-LO object in the course of its routing ever to leave the scope of SIP conveyance (say, hitting a gateway to another protocol like Jabber), the indicator would be retained without the need for any special intelligence on the part of the gateway.

Regardless of where the indicator is staged, it can do nothing but indicate - it will not prevent any entity from inspecting LI out of malice or incompetence. Of course, the same is true of the <retransmission-allowed> element itself. The indicator can serve no other purpose than to express the policy of the originator (hopefully the Rule Maker), and in turn to provide grounds for liability when these policies are violated.

[3.2.](#) Withholding Location

The originator of a SIP request can also withhold LI from particular elements in the signaling stream and reveal it to others. In this manner, the Rule Maker can guarantee that the LI will only be reveal to appropriate recipients, and all such recipients will be understood to be constrained by the <retransmission-allowed> of PIDF-LO. Since the Rule Maker specifically authorized each entity capable of

inspecting the LI, forwarding the SIP request in this case does not constitute "retransmission".

One manner of accomplishing this is to encrypt the PIDF-LO object in a SIP request. If the originator knows which specific entity on the path needs to inspect the LI, and knows a public key for that entity, this is a straightforward matter. It is even possible to encrypt multiple instance of PIDF-LO, containing different policies or levels of location granularity, in the same SIP request if multiple entities along the path need to inspect the location. However, for the much the same reason as the very specific (list of hosts) indicator above is problematic, this is also more or less useless in most practical deployments. Not only is anticipating the intermediaries or endpoints that a request will visit prohibitively difficult, but this approach also requires some sort of public key discovery system which compounds the operational complexity significantly. In some very specific environments this might have some applicability, but they would be rare.

Another, more feasible approach is leveraging location by reference. When a SIP request conveys a reference, it cannot be properly said to be conveying location; location is conveyed upon dereferencing the URI in the question, and the meaning of <retransmission-allowed> must be understood in the context of that conveyance, not the forwarding of the SIP request.

A recent study [Henning's types-of-LbyR] has pointed out that the properties of references, especially the security properties, vary significantly depending on the nature and disposition of the resource indicated. Clearly, if the referenced PIDF-LO is available, in the same form, to any entity along the SIP signaling path that requests it, then inserting a reference has no advantages over inserting LI by value (and introduces wasteful complexity). However, if the Rule Maker influences the results of the dereferencing process, including determining who can receive LI at what degree of granularity and what policies are bound with the LI,

It might superficially appear that this suffers from the same problems as the encryption approach, since the Rule Maker must anticipate a set of entities who are authorized to receive location

information. The difference is that this set does not need to be

communicated in the SIP request in order for authorization decisions to be made. There is a world of difference between managing a whitelist of a thousand parties that might ask for LI and sending a SIP request containing a thousand differently-encrypted adumbrations on LI – the former is commonplace and the latter is impossible. Additionally, some Rule Maker policies might not even require the establishment of an exhaustive whitelist. For example, it may be that there exists a finite set of commercial requestors that the Rule Maker would like to block, in a manner similar to the way ad-blockers operate in modern web browsers.

In any system where one makes an authorization decision, a certain cost in authentication must be paid – the greater the assurance the greater the cost. The precise cost will of course depend on the URI scheme of the reference. For SIP, Digest has a low computational cost but requires pre-established keys, which limits applicability. [RFC4474](#) Identity does not require any pre-association, but it does make signaling more heavyweight and requires the deployment of additional features in the network, including a web-like PKI.

But even if no authentication takes place, in the LbyR case the meaning of <retransmission-allowed> is unambiguous – each entity to which LI is conveyed in the dereference process is bound by the retransmission policy. The cost of the reference itself is of course the server that maintains the resource. While not every SIP client has access to an appropriate server for this purpose, the fact that PIDF-LO builds on the typical SIP presence service makes this less implausible than it might be. Moreover, the LbyR approach casts the conveyance architecture in a manner familiar from [RFC3693](#), with a Location Server receiving requests from Location Recipients which may be accepted or denied. This allows the preservation of the original semantics of <retransmission-allowed>.

[4.](#) Analysis

Regardless of how permission for location-based routing is granted, the meaning of <retransmission-allowed> with a value of "no" in a PIDF-LO body conveyed in a SIP request must be unambiguous for all endpoints and intermediaries that process the message. Since even location-aware intermediaries might perform a baseline SIP forwarding function without inspecting LI, and location-unaware intermediaries can do nothing but, it is clear that SIP messages with a flag of <retransmission-allowed> equal to "no" can and will be forwarded by SIP intermediaries.

Leaving aside for the moment the question of LI in particular, and

instead considering the matter purely from a SIP perspective, when a UAC sends a SIP request with a body, SIP permits any intermediaries and the eventual endpoint recipient to inspect the body, and places little constraints on how intermediaries arrive at a forwarding decision. In other words, when a UAC sends a request, it is implicitly allowing set of entities to receive that message body, a set whose contents the UAC cannot anticipate in typical SIP environments. Consequently, for the purposes of SIP as a conveyance protocol, it would not be unreasonable to proceed as if each location-aware entity in the routeset of a SIP request is an [RFC3693](#) Location Recipient, and as such each is bound by <retransmission-allowed> as if the LG had shared this information with them bilaterally, regardless of what actions they take as they process SIP requests.

This approach has the desirable property that it does not alter the [RFC4119](#) semantics of <retransmission-allowed>. It does however require some additional work to make this understanding of SIP location conveyance meet the privacy goals of [RFC3693](#). Consider, for example, that an unanticipated SIP intermediary which is not location-aware might log SIP requests, body and all, enabling parties interested in tracking location information to data mine its logs later. In any system of intermediaries whose behavior cannot be predicted, these sorts of scenarios are a potential downside.

The simplest way to mitigate this risk is by withholding LI. For the many reasons described in the previous section, encryption is not a feasible approach to this. However, a privacy-conscious UAC can send LI by-reference in SIP requests. The service that manages requests for LI (an [RFC3693](#) LS) can then use whatever access controls it sees fit to ensure that LI is only shared with appropriate parties. A SIP intermediary which logged all requests would in this instance merely log a URI rather than a copy of the LI.

These risks are not always a privacy concern for UACs, however, and when a UAC cannot or does not wish to publish its location to an LS, it can avail itself of the 'routing-permitted' indicator to express the intended usage of location information. If 'routing-permitted' is set to "yes", a location-aware intermediary knows that the LI so designated is likely to be useful for routing, and that it is worth the trouble to run any routing algorithm. If it is set to "no", then a location-aware intermediary knows not to invoke any routing algorithm - the LI might not be even be useful for making a routing decision in this case.

Where location by-reference is preferred, a location-aware

intermediary does not want to incur the costs of looking up the reference URI needlessly. If LI is not intended for use by

Internet-Draft

Retransmission

February 2008

intermediaries, and dereferencing a URI conveyed within SIP would only lead to the denial of the request, the UAC could set the 'routing-permitted' indicator in the SIP request to "no". This would let any location-aware intermediary know that it needn't even bother to try to dereference the URI. This use of the indicator argues strongly for making it a SIP-layer indicator (a part of the Location header) rather than a new element of PIDF-LO. Although in this case it is not possible to provide a common integrity protection over the 'routing-permitted' indicator and the remainder of policies set by the Rule Maker, the value of tampering with 'routing-permitted' seems low; it will not result in privacy leaks, in any event, since privacy can be managed with greater granularity by withholding LI.

In summary, both the strategies of indicating permission and withholding LI are viable, and in fact compatible.

[5.](#) Recommendation

This document recommends that the "recipient" parameter in the SIP location conveyance proposal ([\[5\]](#)) be replaced by a parameter called "routing-permitted". This parameter accepts only a binary value of "yes" or "no". The default value shall be "no".

The current text in the SIP location conveyance proposal on privacy, in the first paragraph of [Section 5](#), considers encryption as a means of providing access control for PIDF-LO. For the reasons mentioned in [Section 3](#), encryption is not an optimal means of withholding location information. The relevant text in [Section 4.2](#), 5 and 7 of the SIP location conveyance proposals should instead reference or include the discussion in this document.

[6.](#) IANA Considerations

This document contains no considerations for the IANA.

[7.](#) Security Considerations

The privacy and security implications of distributing location information are the fundamental subject of this document.

8. Informational References

- [1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP:

Peterson, et al.

Expires August 18, 2008

[Page 10]

Internet-Draft

Retransmission

February 2008

Session Initiation Protocol", [RFC 3261](#), June 2002.

- [2] Bradner, S., "Key words for use in RFCs to indicate requirement levels", [RFC 2119](#), March 1997.
- [3] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", [RFC 3693](#), February 2004.
- [4] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [RFC 4119](#), December 2005.
- [5] Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", [draft-ietf-sip-location-conveyance-09](#) (work in progress), November 2007.

Authors' Addresses

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
USA

Phone: +1 925/363-8720
Email: jon.peterson@neustar.biz
URI: <http://www.neustar.biz/>

Ted Hardie
Qualcomm, Inc.

Email: hardie@qualcomm.com

John B. Morris, Jr.
Center for Democracy and Technology
1634 I Street NW
Suite 1100
Washington, DC 20006
USA

Email: jmorris@cdt.org
URI: <http://www.cdt.org>

Peterson, et al.

Expires August 18, 2008

[Page 11]

Internet-Draft

Retransmission

February 2008

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat 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 on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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