GeoPriv
Internet-Draft
Intended status: Informational
Expires: August 28, 2008

R. Marshall, Ed.
TCS

February 25, 2008

Requirements for a Location-by-Reference Mechanism
draft-ietf-geopriv-lbyr-requirements-02

Status of this Memo

Copyright Notice

Abstract

This document defines terminology and provides requirements relating to Location-by-Reference approach using a location URI to handle location information within signaling and other Internet messaging.

Table of Contents

1. Introduction 3
2. Terminology 5
3. Overview of Location-by-Reference 6
4. High-Level Requirements 9
4.1. Requirements for a Location Configuration Protocol . . . 9
4.2. Requirements for a Location Dereference Protocol 11
5. Security Considerations 14
6. IANA Considerations 15
7. Acknowledgements 16
8. References 17
8.1. Normative References 17
8.2. Informative References 17
Appendix A. Change log 18
Author's Address 19
Intellectual Property and Copyright Statements 20

1. Introduction

Location-based services rely on ready access to location information, which can be through a direct or indirect mechanism. While there are mechanisms for providing location directly, (e.g., as part of the SIP signaling protocol), an alternative mechanism has been developed for handling location indirectly, via a location reference, a pointer to the actual location information. This reference is called a location URI, and is used by the mechanism we generally call the Location-by-Reference mechanism, or simply, LbyR.

The use of a location URI is generally applied in one of the following ways:

1. Creation/allocation of a location URI, by a location server based on some request mechanism.

2. As part of a Location Configuration Protocol, between a target and location server*.

3. The location dereference process, (between a dereference client and dereference server).

4. Cancellation/expiration of a location URI, by a location server based on either a direct target request or some other action (e.g., timer).

*In this document, we make no differentiation between a LS, per RFC3693, and a LIS, but may refer to either of them as a location server interchangeably.

These four things fall under two general protocol mechanisms, location configuration protocols and location dereference protocols.

A fifth use of location URI is within the context of what is called location conveyance. Location conveyance is defined as part of the

SIP protocol, and is out of scope for this document. (see [I-D.ietf-sip-location-conveyance] for an explanation of conveyance of location using a location URI.

The issues around location configuration protocols have been documented in a location configuration protocol problem statement and requirements document [I-D.ietf-geopriv-l7-lcp-ps].

There are currently a several examples of a location configuration protocol. These include DHCP, LLDP-MED, and HELD [I-D.ietf-geopriv-http-location-delivery]) protocols.

The structure of this document includes terminology, Section 2, followed by a discussion of the basic elements that surround how a location URI is used. These elements, or actors, are discussed in an overview section, Section 3, accompanied by a graph and associated processing steps.

Requirements are outlined accordingly, separated as location configuration requirements, Section 4.1, and location dereference requirements, Section 4.2.

In contrast to using a location URI as the mechanism to support a Location-by-Reference model, it may be worth mentioning the common alternative model, that of Location-by-Value (LbyV), which provides location directly. LbyV uses a location object, (e.g., a PIDF-LO, [RFC4119]) within SIP signaling. Using the LbyV model for location configuration is considered out of scope for this document (see [I-D.ietf-sip-location-conveyance] for an explanation of location conveyance for either LbyR or LbyV scenarios.

Location determination, different than location configuration or dereferencing, often includes topics related to manual provisioning processes, automated measurements, and/or location transformations, (e.g., geo-coding), and are beyond the scope of this document.

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 RFC 2119 [RFC2119].

This document reuses the terminology of [RFC3693], such as Location Server (LS), Location Recipient (LR), Rule Maker (RM), Target, Location Generator (LG), Location Object (LO), and Using Protocol:

Location-by-Value (LbyV): The mechanism of representing location either in configuration or conveyance protocols, (i.e., the actual included location value).

Location-by-Reference (LbyR): The mechanism of representing location by means of a location URI for use in either a location configuration, conveyance, or dereferencing protocol, and which refers to a fully specified location.

Location Configuration Protocol: A protocol which is used by a client to acquire either location or a location URI from a location configuration server, based on information unique to the

client.

Location Dereference Protocol: A protocol which is used by a client to query a location dereference server, based on location URI input and which returns location information.

Location URI: An identifier which serves as a pointer to a location record on a remote host (e.g., LIS). Used within an Location-by-Reference mechanism, a location URI is provided by a location configuration server, and is used as input by a dereference protocol to retrieve location from a dereference server.

3. Overview of Location-by-Reference

In mobile wireless networks it is not efficient for the end host to periodically query the LIS for up-to-date location information. This is especially the case when power is a constraint or a location update is not immediately needed. Furthermore, the end host might want to delegate the task of retrieving and publishing location information to a third party, such as to a presence server. Finally, in some deployments, the network operator may not want to make location information widely available.

Different location scenarios, such as whether a Target is mobile and whether a mobile device needs to be located on demand or according to some pre-determined interval motivated the introduction of the LbyR concept. Depending on the type of reference, such as HTTP/HTTPS or

SIP Presence URI, different operations can be performed. While an HTTP/HTTPS URI can be resolved to location information, a SIP Presence URI provides further benefits from the SUBSCRIBE/NOTIFY concept that can additionally be combined with location filters [I-D.ietf-geopriv-loc-filters].

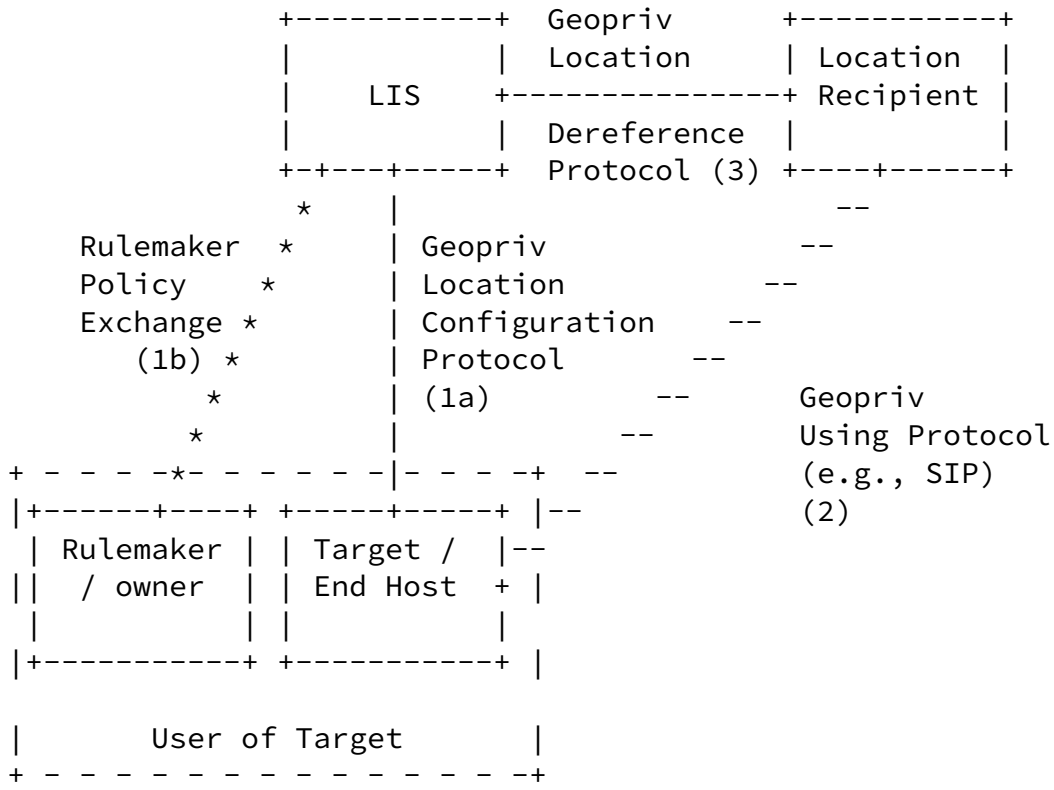

Figure 1: Shows the assumed communication model for both a layer 7 location configuration protocol and a dereference protocol:

Figure 1: Shows the assumed communication model for both a layer 7 location configuration protocol and a location dereference protocol.

(1a). Target requests reference from server; and receives back, a location URI in server response

(1b). Rulemaker policy is consulted (interface out of scope)

(2). Target conveys reference to recipient (out of scope)

(3). Recipient dereferences location URI, by a choice of methods, including a request/response (e.g., HTTP) or publish/subscription (e.g., SIP SUBSCRIBE/NOTIFY)

Note A. There is no requirement for using the same protocol in (1a) and (3).

Note B. Figure 1 includes the interaction between the owner of the Target and the LIS to establish Rulemaker policies. This is communications path (1b). This interaction needs to be done before the LIS will authorize anything of than default policies to a dereference request for location of the Target.

Note C. that the Target may take on the role of the Location Recipient whereby it would dereference the location URI to obtain its own location information.

An example scenario of how this might work, is where the Target obtains a location URI in the form of a subscription URI (e.g., a SIP URI) via HELD, (a Geopriv layer 7 location configuration protocol). Since, in this case the Target equals Recipient, then the Target can subscribe to the URI in order to be notified of its current location based on subscription parameters (see [I-D.ietf-geopriv-loc-filters]). Additionally, a geospatial boundary can be expressed (ref. [I-D.ietf-geopriv-policy]), so that the Target/Recipient will get its updated location notification once it crosses the specified boundary.

Location URIs may have an life expiration associated to them, so the LIS needs to be able to keep track of the location URIs that have been handed out, in addition, to also know about validity information for each location URI. Location URIs need to expire to prevent the recipient of such a URI from being able to (in some cases) permanently track a host. Another example of the usefulness of an expiration mechanism is to offer garbage collection capabilities to the LIS.

It is important to prevent adversaries from obtaining any information

about a Target through the location URI itself, or even a Target's

location if the owner of the Target wants to protect it. Therefore, each location URI must be constructed with security safeguards in mind. There are two general cases assumed, both having to do with the form of the location URI when it is created.

Case 1. Where access to the location URI is limited by policy: This is the case where the LIS applies authentication and access control at location configuration step and again at the dereference step. In this case, the URI can be of any form chosen by the LIS.

Case 2. Access limited by distribution: The LIS does not apply authentication and access control at the time that the location URI is dereferenced. In this case, the location URI must be difficult to guess (so that possession can be used to imply authorization).

4. High-Level Requirements

This document outlines the requirements for an Location by Reference mechanism which can be used by a number of underlying protocols. Requirements here address two general types of such protocols, a general location configuration protocol, and a general location dereferencing protocol. Given that either of these two general protocols can take the form of different protocols implementations for either location configuration vs. location dereference, (e.g., HELD/DHCP/LLDP-MED, vs. HTTP GET/SIP SUBSCRIBE/NOTIFY, respectively). Because each of these specific protocol implementations has its own unique client and server interactions, the requirements here are not intended to state what a client or server is expected to do, but rather which requirements must be met separately by either a location configuration protocol, or a location dereference protocol, for the purposes of using a location URI.

The requirements are broken into two sections.

4.1. Requirements for a Location Configuration Protocol

Below, we summarize high-level design requirements needed for a location-by-reference mechanism as used within the location configuration protocol.

C1. Location URI support: The configuration protocol MUST support a location reference in URI form.

Motivation: It is helpful to have a consistent form of key for the LbyR mechanism.

C2. Location URI expiration: When a location URI has a limited validity interval, its lifetime MUST be indicated.

Motivation: A location URI may not intend to represent a location forever, and the identifier eventually may need to be recycled, or may be subject to a specific window of validity, after which the location reference fails to yield a location, or the location is determined to be kept confidential.

C3. Location URI cancellation: The location configuration protocol SHOULD support the ability to request a cancellation of a specific location URI.

Motivation: If the client determines that in its best interest to destroy the ability for a location URI to effectively be used to

dereference a location, then there should be a way to nullify the location URI.

C4. [Deleted, replaced by C8,C9,C10]:

C5. User Identity Protection: The location URI MUST NOT contain any user identifying information that identifies the user, device or address of record, (e.g., which includes phone extensions, badge numbers, first or last names, etc.), within the URI form.

Motivation: It is important to protect caller identity or contact address from being included in the form of the location URI itself when it is generated.

C6. Reuse indicator: There SHOULD be a way to allow a client to control whether a location URI can be resolved once only, or multiple times.

Motivation: The client requesting a location URI may request a location URI which has a 'one-time-use' only characteristic, as opposed to a location URI having multiple reuse capability.

C7. Location URI Valid-for: A location URI validity interval, if used, MUST include the validity time, in seconds, as an indication of how long the client can consider a location URI to be valid.

Motivation: It is important to be able to determine how long a location URI is to remain useful for, and when it must be refreshed.

C8. Location URI Anonymous: The location URI MUST NOT reveal any information about the Target other than it's location.

Motivation: A user should have the option to control how much information is revealed about them. This provides that control by not forcing the inclusion of other information with location, (e.g., to not include any identification information in the location URI.)

C9. Location URI Not guessable: Location URIs that do not require authentication and authorization MUST NOT be guessable, based on the use of a cryptographically random sequence somewhere within

the URI. (Note that the number of bits depends to some extent on the number of active location URIs that might exist at the one time; 128-bit is most likely enough for the short term.)

Motivation: Location URIs without access control reveal private information, and a guessable location URI could be easily exploited to obtain private information.

C10. Location URI Optional: In the case of user-provided authorization policies, where anonymous or non-guessable location URIs are not warranted, the location configuration protocol MAY support optional location URI forms.

Motivation: Users don't always have such strict privacy requirements, but may opt to specify their own location URI, or components thereof.

4.2. Requirements for a Location Dereference Protocol

Below, we summarize high-level design requirements needed for a location-by-reference mechanism as used within the location dereference protocol.

D1. Location URI support: The location dereference protocol MUST support a location reference in URI form.

Motivation: It is required that there be consistency of use between location URI formats used in an configuration protocol and those used by a dereference protocol.

D2. Location URI expiration indicator: The location dereference protocol MUST support an indicator showing that, if it is the case, that a location URI is no longer valid due to expiration.

Motivation: Location URIs are expected to expire, based on location configuration protocol parameters, and it is therefore useful to convey the expired status of the location URI in the location dereference protocol.

D3. Authentication: The location dereference protocol MUST include

mechanisms to authenticate both the client and the server.

Motivation: Although the implementations must support authentication of both parties, any given transaction has the option not to authenticate one or both parties.

D4. Dereferenced Location Form: The value returned by the dereference protocol MUST contain a well-formed PIDF-LO document.

Motivation: This is in order to ensure that adequate privacy rules can be adhered to, since the PIDF-LO format comprises the necessary structures to maintain location privacy.

D5. Location URI Repeated Use: The location dereference protocol MUST support the ability for the same location URI to be resolved more than once, based on dereference server configuration.

Motivation: Through dereference server configuration, for example, it may be useful to not only allow more than one dereference request, but, in some cases, to also limit the number of dereferencing attempts by a client.

D6. Location URI Valid-for: A location URI validity interval, if used, MUST include the validity time, in seconds, as an indication of how long the client can consider a location URI to be valid.

Motivation: It is important to be able to determine how long a location URI is to remain useful when dereferencing a location URI.

D7. Location URI anonymized: Any location URI whose dereference will not be subject to authentication and access control MUST be anonymized.

Motivation: The dereference protocol must define an anonymized format for location URIs. This format must identify the desired location information via a random token with at least 128 bits of entropy (rather than some kind of explicit identifier, such as an

IP address).

D8. Location URI non-anonymized: The dereference protocol MAY define a more general, non-anonymized URI format.

Motivation: Only location URIs for which dereference is subject to access-control policy by the LIS may use this format.

D9. Location Privacy: The location dereference protocol MUST support the application of privacy rules to the dissemination of a requested location object.

Motivation: The dereference server must obey all provisioned privacy rules that apply to a requested location object.

D10. Location Confidentiality: The dereference protocol MUST support encryption of messages sent between the location dereference client and the location dereference server, and MAY alternatively provide messaging unencrypted.

Motivation: Environmental and local configuration policy will guide the requirement for encryption for certain transactions. In some cases, encryption may be the rule, in others, it may be acceptable to send and receive messages without encryption.

5. Security Considerations

The LbyR mechanism currently addresses security issues as follows.

A location URI, regardless of its construction, if public, implies no safeguard against anyone being able to dereference and get the location. The method of constructing a location URI in its naming does help prevent some potential guessing, according to some defined pattern. In the instance of one-time-use location URIs, which function similarly to a pawn ticket, the argument can be made that with a pawn ticket, possession implies permission, and

location URIs which are public are protected only by privacy rules enforced at the dereference server.

6. IANA Considerations

This document does not require actions by the IANA.

7. Acknowledgements

We would like to thank the IETF GEOPRIV working group chairs, Andy Newton, Allison Mankin and Randall Gellens, for creating the design team which initiated this requirements work. We'd also like to thank those design team participants for their inputs, comments, and reviews. The design team included the following folks: Richard Barnes; Martin Dawson; Keith Drage; Randall Gellens; Ted Hardie; Cullen Jennings; Marc Linsner; Rohan Mahy; Allison Mankin; Roger Marshall; Andrew Newton; Jon Peterson; James M. Polk; Brian Rosen; John Schnizlein; Henning Schulzrinne; Barbara Stark; Hannes Tschofenig; Martin Thomson; and James Winterbottom.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[I-D.ietf-geopriv-http-location-delivery]
Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-05 (work in progress), February 2008.

[I-D.ietf-geopriv-l7-lcp-ps]
Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-06 (work in progress), November 2007.

[I-D.ietf-geopriv-loc-filters]
Mahy, R., "A Document Format for Filtering and Reporting Location Notications in the Presence Information Document Format Location Object (PIDF-LO)", draft-ietf-geopriv-loc-filters-01 (work in progress), March 2007.

[I-D.ietf-geopriv-policy]
Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., and J. Polk, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", draft-ietf-geopriv-policy-14 (work in progress), February 2008.

[I-D.ietf-sip-location-conveyance]
Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sip-location-conveyance-09 (work in progress), November 2007.

[RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

Appendix A. Change log

Changes to this draft in comparison to the previous version (-02 vs. -01):

1. Reworded Introduction (Barnes 12/6 list comments).

2. Changed name of "Basic Actors" section to "Overview of Location by Reference" (Barnes).

3. Keeping the LCP term away (for now) since it is used as Link Control Protocol elsewhere (IETF).

4. Changed formatting of Terminology section (Barnes).

5. Requirement C2. changed to indicate that if the URI has a lifetime, it has to have an expiry (Barnes)

6. C7. Changed title and wording based on suggested text and dhcp-uri-option example (Polk).

7. The new C2 req. describing valid-for, was also added into the deref section, as D6

8. Changed C4 based on much list discussion - replaced by 3 new requirements...

9. Reworded C5 based on the follow-on C4 thread/discussion on list (~2/18).

10. Changed wording of D3 based on suggestion (Barnes).

11. Reworded D4 per suggestion (Barnes).

12. Changed D5 based on comment (Barnes), and additional title and text changes for clarity.

13. Added D9 and D10 per Richard Barnes suggestions - something needed in addition to his own security doc.

14. Deleted reference to individual Barnes-loc-sec draft per wg list suggestion (Barnes), but need more text for this draft's security section.

Author's Address

Roger Marshall (editor)
TeleCommunication Systems, Inc.
2401 Elliott Avenue
2nd Floor
Seattle, WA 98121
US

Phone: +1 206 792 2424
Email: rmarshall@telecomsys.com
URI: http://www.telecomsys.com

Full Copyright Statement

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).