GeoPriv
Internet-Draft
Intended status: Informational
Expires: March 8, 2008

R. Marshall, Ed.
TCS

September 5, 2007

Requirements for a Location-by-Reference Mechanism
draft-ietf-geopriv-lbyr-requirements-00

Status of this Memo

Copyright Notice

Abstract

This document defines terminology and provides requirements relating to a Location-by-Reference approach to handling location information within SIP signaling and other Internet messaging. The key for a Location-by-Reference mechanism is the Location URI, which is a reference to a location, and is used by either an end-device or a middlebox to represent a location, and is used as a key by a dereferencing protocol to get a usable form of location. An example application for which the Location-by-Reference mechanism is used is emergency call routing with voice-over-IP (VoIP) and general Internet multimedia systems, where Internet protocols are used end-to-end.

Table of Contents

1. Introduction

Location-based services rely on ready access to location information, which can be through a direct, or indirect mechanism. While there is already a direct mechanism which exists to provide location as part of the SIP signaling protocol, an alternative mechanism has been developed for handling location indirectly, via a location reference, a reference which points to the actual location information. This reference is called the location URI, and is used by the Location-by-Reference mechanism.

Since possessing the location URI alone is insufficient to perform location-based routing, the location URI must be dereferenced. Once the actual location information is returned to a location recipient, it can then be used as input to some location-based service, such as in the case of routing a VoIP-based emergency call.

This document lists a set of requirements for a Location-by-Reference (LbyR) mechanism, using a location URI within the SIP protocol for the purpose of executing a location-based service routing request.

There are a variety of actions in which a location URI can be used. Included in this list is the action of 'location configuration', or the acquisition of the location into an end device or middlebox, 'location conveyance', which is the shuttling of location between SIP signaling nodes, and, 'location dereferencing', which we define as the action of exchanging a location URI for the actual location information it points to at a dereference server, which we call a Location Information Server, or LIS.

Each of these actions are represented by specific individual protocols. A Location Configuration Protocol (LCP), is used by a device or middlebox to acquire a location which already exists (examples of this protocol include DHCP, LLDP-MED, and HELD). By conveyance protocol, we mean a protocol which transports a location URI along from node to node according to specific rules (e.g., SIP).

A Location Dereferencing Protocol (LDP), is used by a client to resolve a location URI in exchange for location information at a LIS.

Though conveyance of a location URI may be discussed in general terms, any requirements for conveyance using LbyR are not included, and are considered out of scope.

In our SIP example, the LbyR is setup, instead of having a content identifier (cid:) pointing to a location object within a SIP body, to have a location URI carried in the SIP Geolocation header.

In constrast to LbyR, a direct access to location is equivalent to

having a location object included along with the signaling, (e.g., a PIDF-LO), is referred to as the Location-by-Value (LbyV) mechanism, and is treated as out of scope for this document. A separate draft document exists which describes, for both LbyR and LbyV scenarios, a way to convey location within SIP [I-D.ietf-sip-location-conveyance].

The structure of this document first defines terminology in Section 3. Then a short discussion on the basic elements which show LbyR. This section on actors, Section 4 includes a basic LbyR model, and describes the steps which the LbyR mechanism takes.

Requirements are outlined separately for the configuration step (LCP), (Section 5), followed by an additional list of requirements targeted toward the dereferencing step (LDP) (Section 6).

Location determination, which may include the processes of manual provisioning, automated measurements, or location transformations, (e.g., geo-coding), are beyond the scope of this document.

A detailed discussion of Identity information related to the caller, subscriber, or device, as associated to location or location URI, is also out of scope.

2. Requirements Terminology

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 RFC 2119 [RFC2119].

This document outlines only requirements for an LbyR mechanism which is used by two different protocols, a Location Configuration Protocol, and a Location Derferencing Protocol. Each of these protocols has its own unique client and server interactions, and the requirements here are not intended to state what either an LCP or LDP host client or server is expected to do, but rather which requirements must be met by both the LCP and LDP interface protocols.

3. Terminology

3.1. Definition of Terms

Several of the terms presented below are based on Geopriv Requirements [RFC3693], and in some cases, extended to include additional language to support the LbyR model.

Civic location: A described location based on some understood location reference system, such a jurisdictions or postal delivery grid. A street address valid within the USPS system is a common example.

Coordinate location: A reference to a geographic point which is able to be located as described by a set of defined coordinates within

a geographic coordinate system, such as latitude and longitude, within the WGS-84 datum. For example, 2-D geographic location is defined as an (x,y) coordinate value pair according to the distance north or south of the equator and east or west of the prime meridian. A coordinate location may be absolute, or may have associated uncertainty related to it's exact position, depending on how it is represented.

Location: Either a geographic coordinate or feature representation based on a specific coordinate reference system, or by other identifiable information such as a street number and street name within a civic, postal, or abstract location reference system.

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

Location-by-Reference: The mechanism of representing location either in configuration, conveyance, and dereferencing protocols as an identifier which refers to a fully specified location, (i.e., a pointer to the actual location value).

Location Configuration Protocol (LCP): A protocol which is used by a client to acquire location or a location URI from a location configuration server (e.g., (LIS)), based on information unique to the client.

Location Dereference Protocol (LDP): A protocol which is used by a client to query a location dereference server (e.g., (LIS)), based on location URI input and which returns location information (e.g., a PIDF-LO).

Location Information Server (LIS): The entity which receives a client request for either location or a location reference. In the latter case, also performs the dereference function for a Location Refernce Identifier, in the context of the Location-by-Reference model. May also be referred to as a Location Information Server (LIS). In the SIP Presence architecture, the LIS may be referred to as a Presence Server (PS). In this document the LIS is an instance of an LS.

Location Object (LO): An object conveying location information (and possibly privacy rules) to which Geopriv security mechanisms and privacy rules are to be applied.

Location Recipient (LR): The entity that receives location information. It may have asked for this location explicitly (by sending a query containing an location URI to a location configuration server), or it may receive this location asynchronously.

Location Server (LS): The entity to which a LG publishes location objects, the recipient of queries from location receivers, and the entity that applies rules designed by the rule maker.

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 (LbyR) mechanism. A location URI is provided by a location configuration server, based on a client request, and is the input used by the dereference protocol to retrieve the associated location from a dereference server. It is assumed that a LIS can function both as a configuration server and dereference server.

Rule Maker (RM): The authority that creates rules governing access to location information for a target (typically, this it the target themselves).

Target: A person, end device, or other entity whose location is communicated by a Geopriv Location Object.

Using Protocol: A protocol (e.g., SIP) which carries a Location Object or an Location Reference Identifier.

4. Basic Actors

LbyR with Location Subscription

The LbyR mechanism can be used via a normal query/response mode, or alternatively, by using a subscription model to get updated location.

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.

These use scenarios 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].

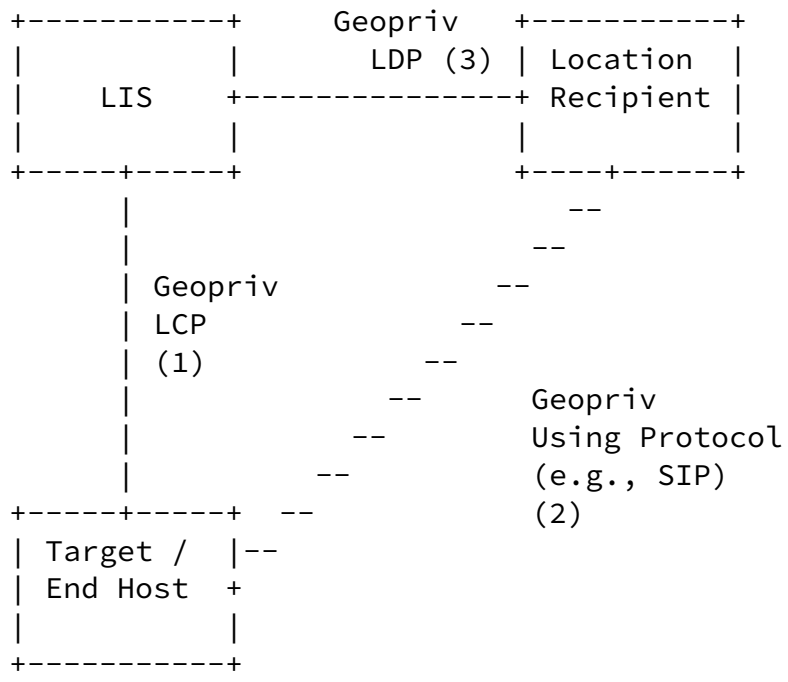

Figure 1: Shows the assumed communication model for a layer 7 (L7) LCP and LDP:

Note that there is no requirement for using the same protocol in (1)

and (3).

The following list describes the location subscription approach:

1. The end host discovers the LIS.

2. The target (end host) sends a request to the LIS asking for a location URI, as shown in (1) of Figure 1.

3. The LIS responds to the request and includes a location object along with a subscription URI.

4. The Target puts the subscription URI into a SIP message and forwards it to a Location Recipient via a using protocol, as shown in (2) of Figure 1. The Location Recipient subscribes to the obtained subscription URI (see (3) of Figure 1) and potentially uses a location filter (see [I-D.ietf-geopriv-loc-filters]) to limit the notification rate.

5. If the Target moves outside a certain area, indicated by a location filter, the Location Recipient will receive a notification.

Note that the Target may also act in the role of the Location Recipient whereby it would subscribe to its own location information. For example, the Target obtains a subscription URI from the Geopriv L7 LCP protocol. It subscribes to the URI in order to obtain its current location information. A service boundary indicates the bounded extent up to which the device can move without the need to have an updated location, since a re-query with any location within the boundary would result in the same answer returned from a location-based service.

For LbyR, the LIS needs to maintain a list of randomized location URIs for each host, timing out each of these URIs after the reference expires. Location URIs need to expire to prevent the recipient of such a URI from being able to (in some cases) permanently track a host. Furthermore, an expiration mechanism also offers garbage collection capability for the LIS.

Location URIs must be designed to prevent adversaries from obtaining a known Target's location. There are at least two approaches: The location URI contains a random component which helps obscure sequential updates to location, yet still allows any holder of the location URI to obtain location information. Alternatively, the location URI can remain public and the LIS performs access control via a separate authentication mechanism, such as HTTP digest or TLS

client side authentication, when resolving the reference to a location object.

5. High-Level Requirements for a Location Configuration Protocol

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

C1. Location URI support - LCP: 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: The LCP MUST support the ability to specify to the server, the length of time that a location URI will be valid.

Motivation: Location URIs are not intended 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. A configurable carried in the LCP for a location URI ensures that the location reference becomes invalid based on some internal LIS settings.

C3. Location URI cancellation: The LCP MUST 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 has to be a way to nullify the location URI. (This may be accomplished by setting the C2 configurable to 'expire=now', for example.)

C4. Random Generated: The location URI MUST be hard to guess, i.e., it MUST contain a cryptographically random component.

Motivation: There is some benefit to the client if the location URI is generated in an obscured manner so that its sequence, for example in the case of a client's location update, can't be easy guessed.

C5. Identity Protection - LCP : The location URI MUST NOT contain any information that identifies the user, device or address of record 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 flag default: The LCP MUST support the default condition of a requested location URI being repeatedly reused.

Motivation: The requestor of a location URI, shouldn't need to specify any special flag in order to receive a location URI which can later be used repeatedly, such as for an updated location.

C7. One-time-use: The LCP MUST support the ability for the client to request a 'one-time-use' location URI (e.g., via a reuse flag setting).

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.

6. High-Level Requirements for a Location Dereference Protocol

Below, we summarize high-level design requirements needed for a location-by-reference mechanism.

D1. Location URI support - LDP: The LDP 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 LCP and those used by a LDP.

D2. Location URI expiration status: The LDP MUST support a message indicating that for a location URI which is no longer valid, that the location URI has expired.

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

D3. Authentication: The LDP MUST support either client-side and server-side authentication between client and server.

Motivation: It is reasonable to expect implementations of authentication to vary. Some implementations may choose to

implement both client-side and server-side authentication, might implement one only, or may implement neither.

D4. Dereferenced Location Form: Location URI dereferencing MUST result in a well-formed PIDF-LO.

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

D5. Repeated use: The LDP MUST support the ability for the same location URI to be resolved more than once, based on server settings and LCP parameters.

Motivation: According to LCP parameters, there may or may not be a limit on the number of dereferencing actions at the dereference server.

D6. Updated location: The LDP MUST support the ability for the same location URI to be resolved into a continuum of location values (e.g., location updates).

Motivation: A location URI when reused may not always result in the same location value, but may be a mixture of unchanged and changed location values.

D7. Location form: The LDP MUST support dereferenced location in both coordinate and civic forms.

Motivation: It is important that the LDP not limit which type of location gets dereferenced, since it is assumed that some dereference servers may provide coordinate form of location only, others may provide civic only, while some may provide both forms of location.

7. Security Considerations

The LbyR mechanism currently addresses security issues as follows.

A location URI, regardless of its randomized construction, if public, implies no safeguard against anyone being able to dereference and get the location. The randomization of 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.

Additional security issues will be discussed in a separate geopriv document.

8. IANA Considerations

This document does not require actions by the IANA.

9. Acknowledgements

I 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.

I also would like to thank Andrew Newton; Martin Dawson; Henning Schulzrinne; Marc Linsner; Brian Rosen; Ted Hardie; James M. Polk; James Winterbottom; Martin Thomson; John Schnizlein; Barbara Stark; Jon Peterson; Allison Mankin; Randall Gellens; Cullen Jennings; Richard Barnes; Keith Drage; Rohan Mahy; and Hannes Tschofenig, for their individual contributions and comments.

10. References

10.1. Normative References

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

10.2. Informative References

[I-D.ietf-geopriv-http-location-delivery]
Barnes, M., "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-01 (work in progress), July 2007.

[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-04 (work in progress), August 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-sip-location-conveyance]
Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sip-location-conveyance-08 (work in progress), July 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.

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

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).