Rationale for Location by Reference
draft-winterbottom-location-uri-00.txt

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 draft 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/1id-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 January 12, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document motivates the provisioning of location by-reference within the GEOPRIV architecture. Location by-reference takes the form of a URI in contrast to provisioning a static location.
Table of Contents

1. Introduction ................................................. 3
2. Definition of Terms ........................................... 4
3. Location By Reference ...................................... 5
4. Access Technology Agnostic ................................... 7
5. Access Topologies ............................................ 8
6. Location-Reference Benefits ................................. 9
7. Security Considerations ..................................... 10
8. References .................................................. 10
Authors’ Addresses ............................................. 10
Intellectual Property and Copyright Statements ................. 12
1. Introduction

Circumstances exist where pre-configuring an IP end-point with location and having the end-point communicate that location to other entities is undesirable and/or unsatisfactory. This document describes real network configurations that pose challenges to pre-configured location solutions, and suggests how a location by-reference can ubiquitously be used to overcome these circumstances and ensure that an end-point’s location is current, accurate, dependable and secure.
2. Definition of Terms

Location-Reference: A URI that when accessed by an authorized entity will yield the location of the end-point to which the reference is associated.

Location Dependability: refers to the level of confidence that consumers of the location can, or are prepared, to place in the location being accurate and attributable to an end-point.

Location Currency: refers to how applicable the provided location is when compared to where the end-device is as the time of a location request. That is, how current is the provided location.

Location-Key: mechanism used to provide a reference to a location. This may be a URI, a URL or some other kind of identifier.
3. Location By Reference

The concept of location by-reference, also referred to as a location-key, is to provide an end-point with a URI that when accessed will provide the location of the end-point. Such a mechanism provides a number of advantages that are not achievable through existing by-value location provisioning solutions. The advantages provided include location binding, location dependability, location currency, session decoupling and intransitive trust of location.

Location binding is achieved using location references by forcing the requesting node to ask the access network or other location provider about the location of a specified end-device. In this situation the location generator must be able to identify the end-device, based on the provided reference, and subsequently determine its location. This has the desired affect of ensuring that the location provided is for the end-device about which the request was made. Similarly a query response mechanism of this nature moves towards providing better location currency, and because the location is provided directly from the location generator the dependability of the location is of a higher degree also.

Location references support session decoupling by allowing the end-point to distribute the location reference to third parties so that they may obtain the end-point's location without the end-point needing to maintain a session with the third party. This may be realized through a SIP subscription or other mechanism, but is something that is not possible where location information may only be conveyed in-band between the end-point and the third party.

Location by-reference support intransitive trust because the consumer of location information forms a direct connection to the generators of location information without using the endpoint as an intermediary. Consumers of location information that have strong need to trust the veracity of location information are likelier to have stronger trust relationships with the generators of location information than they are with endpoints. Furthermore, some generators of location information might not want to disclose this information directly to endpoints for various business-model reasons, but might be perfectly willing to give this information to trusted requestors.
Unlike in-band location conveyance, where if one intermediary node is able to see the contents of a message then all may, a location reference may limit the disclosure of a user's location to a limited subset of network nodes, rather than all intermediary nodes, based on a authorization level. That is, location can be provided on a need to know basis. This has several key advantages particularly for SIP and similar session based protocols. Firstly, it allows specific intermediary nodes that require access to location in order to determine routes and so on to obtain the information, but it may restrict the final destination from obtaining the end-device's location if appropriate. Secondly, it allows an end-device the confidence to always send a location reference with all session initiations, so that if location is required by an authorized node it will have access to the information to complete the service. The converse to this would be that either the end-device must know in advance to provide this information, or it would need to be prompted during the session initiation to provide it. Providing this sort of selective disclosure with by-value provisioning of location information is extremely difficult (requiring separate encrypted bodies for separate anticipated recipients) and in some cases simply impossible (where recipients cannot be anticipated by endpoints).

The existing PIDF-LO structure is relatively large and can easily exceed several hundred bytes. A location reference on the other hand, being a URI, will likely be small enough to be accommodated in signalling message headers. Small structures are generally more easily processed by high capacity switching devices, leading to a more efficient message traversal through the network.
4. Access Technology Agnostic

The way in which an end-point accesses a network will have a direct impact on how the location of the end-point is determined, and on the level of precision shared with the network. The freedom of movement allowed to an Internet endpoint once it has connected to the network impacts the most appropriate time to determine its location. In networks where freedom of movement is tightly constrained, variations in location currency are less likely to be an issue than in highly mobile environments. In networks that allow large amounts of movement, for example WiMAX where freedom of movement can be measured in kilometers, it is far less easy to provide any assurances about the currency of location at any given point in time without re-measuring it. Coupling the provisioning of static location information with network-layer autoconfiguration (e.g., DHCP) is therefore applicable to only certain environments, and other environments require a different solution.

Maintaining accurate and current locations for highly mobile end-points in a network is challenging. Continually or periodically re-measuring the location of each end-point and then notifying or pushing this new location to the end-point is expensive and generally unnecessary. In such networks a location-reference can be used deferring location determination until the time that the location is actually required, when the reference is accessed. Such a mechanism reduces overall network load, and provides requestors and consumers of location information a more current location with greater assurances as to its authenticity. By contrast, by-value provisioning in these sorts of environments would result in continual and probably unnecessary updates to all endpoints for the benefits of the few that will ultimately require location-based services.
5. Access Topologies

In addition to access technologies having an impact on location, so too network topologies have an impact on location determination and acquisition. It is not uncommon for broadband services to be provided to end-consumers through infrastructure owned and operated by several different organizations. Such networks generally do not comprise of single DHCP servers, but rather use AAA and RADIUS devices, often in proxy configurations, to obtain and distribute configuration information. Modifying such systems to include native support for location acquisition proliferates a problem that is already starting to take hold in a number of layer 2 based protocols. An alternative approach is to provide a location reference mechanism that can be common across all access configuration protocols allowing simplification and solution consolidation.
6. Location-Reference Benefits

Location not explicitly included in provisioning messages, but available to authorized nodes (which may or may not include the provisioned endpoint).

Smaller messages traverse much of the network, larger location components only retrieved as required. Less load on access network elements as location is only generated and supplied as required.

End-devices do not need to maintain a trust relationship with the location recipient in order for the location recipient to obtain the end-device’s location.

Location consumers obtain location directly from the generator for a given end-point increasing location dependability and reducing unnecessary transitive trust (where recipients would have to trust the consumer "through" a user-controlled endpoint).

Location is determined at request time resulting in more current locations being returned, especially in dynamic environments where location might change over time.

Can be easily integrated into existing presence architectures to make use of existing privacy, authorization and authentication techniques.

Compensates well for network-layer tunnels etc as location-reference can be provided at the local level.
7. Security Considerations

There may be some concern about location-reference theft and subsequent replay attacks. Where they are used with protocols that have good support for identity and authentication management they are likely to be far more secure than currently proposed LCI and in-band location conveyance. In addition to protocol security mechanisms, additional precautions may be taken such as single usage, limited usage, and timed usage references being used.

8. References


Authors’ Addresses

James Winterbottom
Nortel
PO Box U87
University of Wollongong, NSW 2500
AU

Phone: +61 2 4223 3038
Email: winterb@nortel.com
URI: http://www.nortel.com/
Martin Thomson
Nortel
PO Box U87
University of Wollongong, NSW 2500
AU
Phone: +61 2 4254 7515
Email: martin.thomson@nortel.com
URI:  http://www.nortel.com/

Jon Peterson
NeuStar, Inc.
1800 Sutter St, Suite 570
Concord, CA 94520
US
Phone: +1 925/363-8720
Email: jon.peterson@neustar.biz
URI:  http://www.neustar.biz/
Intellectual Property Statement

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.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.
Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.