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/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 April 25, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

In some network configurations, it is desirable for the end system to be able to obtain its geodetic or civic location using an application-layer protocol. This document describes RELO; a simple, HTTP-based stateless protocol that fulfills this need.
1. Introduction

The RELO protocol allows end systems (devices) to obtain information about their current geodetic (longitude, latitude) or civic (jurisdictional or postal street address) location, based on their Internet Protocol address or possibly other identifiers. The protocol uses HTTP [3] to retrieve the information. The location information can be returned by value or by reference, either for retrieval or for event notification by subscription.

The protocol is motivated by the requirement that end user network-layer equipment, such as DSL modems, routers, NATs and wireless access points, cannot be modified. Hence, a DHCP or PPP based solution cannot be reused. A more detailed problem statement is provided in [12]. To reduce privacy risks, RELO is designed for "first-party" retrieval, i.e., the device obtains its own location or a reference thereto. It is not designed for a third party to retrieve location information about a device. However, RELO may retrieve a reference to location information that can be passed to third parties.

Like other HTTP-based protocols, RELO may fail to deliver the correct location information in some circumstances unless special care is taken. For example, if the ISP only allows HTTP connections that traverse an HTTP proxy, the LIS would return the location of the proxy, not that of the client. In this case, however, the ISP would likely know about the proxy and make appropriate arrangements, e.g., to allow non-proxied connections to the LIS only.

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 [1].

This document reuses terminology introduced by RFC 3693 [5] and [12].

3. Overview

This section describes the Location Information Server (LIS) discovery procedure (see Section 3.1), the query message (see Section 3.2) and the response message (see Section 3.3).
3.1. Discovery

The URI for the location server is conveyed via DHCP (not described here) or DNS (S-NAPTR) [7]. The domain is determined from the domain name of the end host, typically conveyed as part of the configuration information. In the example below, host dhcp-17.example.com would query the S-NAPTR record for that domain, obtaining the location server name relo.example.com.

```
dhcp-17.example.com.
 ; order pref flags service regexp
 IN NAPTR 50 50 "a" "Location.relo" ""
 ; replacement
 relo.example.com
```

If the host does not have a domain name or there is no suitable S-NAPTR record, the host checks whether the PTR record for the IP address exists and uses that domain, e.g., a host with the address 192.168.1.2 would query for the S-NAPTR record of 2.1.168.192.in-addr.arpa.

3.2. Query

The query is transmitted to the server in an HTTP GET request, using the media type application/relo+xml. The use of TLS [9] is RECOMMENDED.

The end system is identified by default by its IP address, contained in the IP packets carrying the HTTP request. If the querier is behind a NAT or firewall, the server will see the querier’s public IP address and use that address to identify the end system. In those cases, the location of the network termination equipment, such as the DSL modem or 802.11 access point, will be returned, not the actual location of the querier since the LIS generally has no way to estimate that location. Other identifiers, such as switch and port information, are for further study.

The format of the location information is contained in the <by> element of the query and can indicate that either civic or geo(spatial) information is desired and whether the client wishes to obtain the value ("value"), a reference to the current value ("reference"). If these parameters are omitted, the civic value is returned. It is possible to have an empty HTTP request, which defaults to retrieving the civic address value based on the IP address. A query example is shown below:
Query for location object containing civic location information

This protocol does not provide the ability for the end host to transmit a location estimate as, for example, obtained from a local GPS receiver, to the LIS.

By default, the protocol uses the querier IP address as identifier. However, other identifiers MAY be used. The type of identifier is described by the 'type' parameter in the optional <id> element. The value of the ID parameter is registered with IANA. The <id> element then contains the actual identifier value. All identifiers must follow the conventions for XML strings. A device SHOULD provide all available identifiers; the server chooses the most appropriate one. In the example below, we use the Cisco-proprietary Cisco Discovery Protocol (CDP) switch and port identifier as well as a MAC address.

Query for location object containing civic location information, using CDP and MAC address information

3.3. Response

A successful response contains the civic and or geospatial location information related to the identifier of the querier. Note that this proposal does not return a PIDF-LO [11] since most of the values carried by the PIDF-LO cannot be meaningfully instantiated by the network without the help of the end host. This proposal allows the end host to instantiate the values by itself without introducing security challenges and privacy risks. If the querier indicated a preference for location-by-reference, the answer simply contains a URI-list, i.e., media type text/uri-list [2].

Normal HTTP status responses are used to indicate failure conditions, e.g., when the information is unavailable.

The server indicates the validity period of the information using the HTTP Expires header field. If a reference is returned, the reference
URL itself is not guaranteed to be valid beyond the expiration time.

The server MAY provide one or more URLs in a new HTTP header field, Subscribe, that the client can subscribe to if it wants to receive updates for the object retrieved via HTTP. At least one of the URLs MUST be a SIP URL. For SIP, the event name to be used in the subscription can be encoded in the URL. (An HTTP header field was chosen since the subscription mechanism does not depend on the media type and is equally applicable to other media type. Puting the subscription URL in an HTTP header allows to subscribe to media types where it is difficult to embed SIP URLs, such as a JPEG image.) The server makes no guarantees that the client has the appropriate credentials to subscribe to the object. Clients MAY support this mechanism; all clients that do support subscriptions MUST support the SIP SUBSCRIBE and NOTIFY methods.

The field value consists of one or more absolute URIs:

\[
\text{Subscribe} = "\text{Subscribe} \ : \ #\text{absoluteURI}
\]

An example is:

\[
\text{Subscribe: } \text{sip:data@example.com?Event=location}
\]

[TBD: Since this mechanism is not limited to location delivery, this might be better separated into a stand-alone draft.]

The response containing the location information is not signed.

Response message examples are shown below starting with a response providing geospatial location information and followed by civic location information. Finally, we show an example with location-by-referency.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<returnlocation xmlns="urn:ietf:params:xml:ns:relo1"
    xmlns:gml="http://www.opengis.net/gml">
  <gml:location>
    <gml:Point gml:id="point1" srsName="epsg:4326">
    </gml:Point>
  </gml:location>
</returnlocation>
```

Geospatial location information response
<?xml version="1.0" encoding="UTF-8"?>
<returnlocation xmlns="urn:ietf:params:xml:ns:relo1"
  <civilAddress>
    <p2:country>Deutschland</p2:country>
    <p2:A1>Bayern</p2:A1>
    <p2:A3>Muenchen</p2:A3>
    <p2:A6>Neu Perlach</p2:A6>
    <p2:HNO>96</p2:HNO>
    <p2:PC>81675</p2:PC>
  </civilAddress>
</returnlocation>

Civic location information response

<?xml version="1.0" encoding="UTF-8"?>
<returnURI xmlns="urn:ietf:params:xml:ns:relo1">
  <URI>sip:15555551002adfkafjyonqoiyukjglky@example.com</URI>
</returnURI>

Response containing location-by-reference

4. CDP

The CDP identifier consists of the CDP device id, a colon and the port ID. An example is cepsr-7-1:FastEthernet6/6.

5. XML Schema Definition

This section provides the XML schema; it needs to be updated.

<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:ietf:params:xml:ns:relo1"
  xmlns:relo="urn:ietf:params:xml:ns:relo1"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">
  <!-- get-location -->
  <element name="get-location" type="relo:get-locationType"/>
  <complexType name="get-locationType"/>
</schema>
<complexType name="relo:byType">
  <restriction base="string">
    <enumeration value="value"/>
    <enumeration value="reference"/>
  </restriction>
</complexType>

<complexType name="relo:returnlocationType">
  <complexContent>
    <restriction base="anyType">
      <sequence>
        <element ref="gml:location" minOccurs="0" maxOccurs="1"/>
        <element name="civilAddress" type="civilLoc:civilAddress" minOccurs="0" maxOccurs="1"/>
      </sequence>
    </restriction>
  </complexContent>
</complexType>

<complexType name="relo:returnURIType">
  <sequence>
    <element name="URI" type="anyURI" minOccurs="1" maxOccurs="1"/>
  </sequence>
</complexType>

RELO XML Schema
6. IANA Considerations

6.1. S-NAPTR Application Service Tag

This document registers the label "RELO" as the S-NAPTR application service tag according to [7] for location lookup services and defines the intended usage, interoperability considerations and security considerations (Section 7).

6.2. HTTP Message Header ‘Subscribe’

This document requests the registration of a new message header field, ‘Subscribe’, according to RFC 3864 [6].

Header field name: Subscribe

6.3. MIME Type

This specification also requests the registration of a new MIME type according to the procedures of RFC 4288 [8] and guidelines in RFC 3023 [4].

MIME media type name: application

MIME subtype name: relo+xml

Mandatory parameters: none

Optional parameters: charset

Indicates the character encoding of enclosed XML.

Encoding considerations:

Uses XML, which can employ 8-bit characters, depending on the character encoding used. See RFC 3023 [4], Section 3.2.

Security considerations:

This content type is designed to carry authorization policies. Appropriate precautions should be adopted to limit disclosure of this information. Please refer to Section 7 of RFCXXXX [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number of this specification.] and to the security considerations described in Section 10 of RFC 3023 [4] for more information.
Interoperability considerations:  None

Published specification:  RFCXXX [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number of this specification.] this document

Applications which use this media type:
  Presence- and location-based systems

Additional information:
  Magic Number:  None
  File Extension:  .reloxml
  Macintosh file type code:  ’TEXT’

Personal and email address for further information:  Henning Schulzrinne, hgs@cs.columbia.edu

Intended usage:  LIMITED USE

Author/Change controller:
  This specification is a work item of the IETF GEOPRIV working group, with mailing list address <geopriv@ietf.org>.

6.4.  Registry for Node Identifiers

This document requests the creation of a registry for identifier types, contained in the ‘id’ parameter of the request. According to the processes outlined in [10], new identifiers require a ‘Standards Action’. Identifiers are XML tokens and case-sensitive. Registration includes the token, the RFC number and a brief description. The defining document MUST describe the privacy concerns of using the identifier, where the identifier type should and should not be used and how spoofing of the identifier can be prevented. This document registers the following entry:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>RFC XXXX</td>
<td>Cisco Discovery Protocol port</td>
</tr>
<tr>
<td>DCID</td>
<td>RFC XXXX</td>
<td>DHCP client identifier (RFC 4361)</td>
</tr>
</tbody>
</table>
7. Security Considerations

If IP addresses are used as identifiers, RELO relies on return routability to ensure that only the current owner of an IP address can obtain location information for that host, and assumes that an attacker cannot generate and intercept packets for a spoofed IP address. Note that TLS itself does not prevent client address spoofing if the attacker can intercept and generate IP packets with the victim’s IP address.

The victim can be protected against this privacy breach if the client and LIS share a secret, such as a username/password combination, and the LIS can associate an IP address with a particular user, e.g., based on PPP authentication. In that case, HTTP digest authentication can be used to prevent a third party from using a spoofed IP address to fraudulently obtain location information. Unfortunately, such authentication information is not generally available to wireless nodes in residential networks, for example.

To prevent others from accessing location information for a particular host, the reference to a Location Object MUST NOT be guessable. For example, it may contain a random component. It is RECOMMENDED to use TLS with confidentiality protection to prevent eavesdroppers to observe the protocol exchange between the end host and the LIS.

Other identifiers may have different privacy concerns. For example, switch port identifiers, such as those returned by CDP or LLDP, may not pose as grave a risk of disclosing private information by themselves unless they can be linked to an IP address. Thus, in this case, privacy-protecting the RELO query is particularly important. However, no special authorization is needed unless the ability to enumerate the locations of LAN jacks is considered sensitive.

Signing of location information is beyond the scope of this document [TBD; if desired, reference to other document, since this is not specific to obtaining location information]. Thus, colluding attackers may be able to obtain and replay location information that does not correspond to their true location.

8. Acknowledgments

This document is based on discussions with Hannes Tschofenig and inspired by protocols such as HELD. Andrew Newton provided helpful input.
9. References

9.1. Normative References


9.2. Informative References


Author’s Address

Henning Schulzrinne  
Columbia University  
Department of Computer Science  
450 Computer Science Building  
New York, NY  10027  
US  

Phone: +1 212 939 7004  
Email: hgs+geopriv@cs.columbia.edu  
URI:  http://www.cs.columbia.edu
Full Copyright Statement

Copyright (C) The Internet Society (2006).

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 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).