Network Working Group
Internet-Draft
Expires: December 21, 2003

H. Schulzrinne
Columbia U.
June 22, 2003

Location Objects and Location Privacy Information for Presence Information
draft-schulzrinne-geopriv-presence-lo-00

Status of this Memo

This Internet-Draft will expire on December 21, 2003.

Copyright Notice

Abstract

Location information is a natural extension of presence information. This document describes how the Presence Information Data Format (PIDF) can be extended to deliver geospatial and civil location information, as well as privacy policy information. The privacy policy information can be used both within the presence agent (PA) as well as the presence document.

Table of Contents

1. Requirements notation

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 [RFC2119].

2. Introduction

The draft [I-D.morris-geopriv-core] describes a set of privacy protections and rules that a location object (LO) must contain. This document implements the notions set forth in the draft, albeit with differences in details.

The draft [I-D.peterson-geopriv-pres] makes the case that presence systems already offer many of the features required from a using protocol. Thus, this document extends presence information encoded in the CPIM-compliant PIDF format to express the location of tuples describing a presentity. Such tuples may represent a human being named by the 'entity' attribute in the 'presence' element of the presence document or it may describe the location of a communications device associated with the presentity. Presentities do not need to refer to humans, so the same mechanism is applicable to tracking the location of animals, vehicles or other assets.

3. Architecture

The LO described here is a small, but crucial, component in an overall location service. As motivated in the introduction, a location service based on presence can leverage a number of other existing and emerging pieces of the presence infrastructure. For example, location recipients (i.e., presence subscribers or watchers) need to satisfy the policy requirements before they are allowed to subscribe. The watcher information event package [I-D.ietf-simple-winfo-package] allows authorization agents to be notified when potential location recipients request subscriptions to presence information.

Filters [I-D.ietf-simple-pres-filter-reqs] can be used by subscribers to limit the amount of information that they receive, for example to avoid taxing limited subscriber bandwidth. Conceptually, the subscription filter is applied to the information after it has been tailored by the rules described in this specification, Section 4.

The geospatial and civil coordinates described in this document extend the RPIDS [I-D.schulzrinne-simple-rpids] presence using the RPIDS composition rules to merge tuples and to 'pivot' (i.e., to compose tuples along a certain attribute axis).

4. Privacy Rules

4.1 Introduction

Privacy rules describe how participants in a location system may access, distribute and retain location information. We also allow other components to use these privacy rules. For example, elements within Rich Presence Information (RPIDS) may be protected by these rules.

Privacy rules are found in two places: they are contained in location objects delivered as part of presence information and they are stored in presence agents. We believe that there is much to be gained by making these two the same. Among other advantages, a simple presence agent can just copy the rules into location objects that it delivers. However, this is not always advisable since the privacy rules may well reveal private information that is at least as sensitive as the location information itself, e.g., the target's list of friends and less-trusted acquaintances. The privacy rules defined here are capable of restricting the delivery of the privacy rules themselves, so that the presentity can achieve fine-grained control over its visibility. We also mitigate this exposure by introducing hashed versions of identifiers which are sufficient for the watcher to determine whether another entity may receive location information, but does not reveal the identity itself.

Privacy rules are uploaded and manipulated by the presentity, or an agent acting on its behalf, to the presence agent, e.g., using XCAP. They complement and refine the subscription rules. While subscription rules govern who can subscribe to the presentity, the privacy rules contained in this document restrict the information that is being delivered to the successful subscriber.

When a watcher receives presence information containing these privacy rules, it can propagate the presence object according to these rules and may itself include rules in the presence information it divulges to third parties. However, these rules MUST NOT be any less restrictive than the rules contained in the presence information received. This applies even if, for example, the accuracy of data is also degraded.

4.2 Area Description

The area description provides a labeled geographic area that can be referenced from other rules. It uses the same geospatial or civil coordinates defined in Sections Section 5.1, respectively.

4.3 Disclosure

An example of a disclosure description is shown in Figure 1.

```
<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:cpim-pidf"
   xmlns:p="urn:ietf:params:xml:ns:geo-privacy"
   entity="pres:alice@example.com">

...

<p:disclosure rule="http://example.com/disclosure.xml">
  <p:rule uri="sip:bob@example.com">
    <p:match>
      <p:area>home</p:area>
      <p:rrule freq="daily" until="20031224T000000Z" count="10"/>
    </p:match>
    <p:action>
      <p:include>a1</p:include>
      <p:include>a2</p:include>
      <p:exclude></exclude>
      <p:resolution latitude="9" longitude="10" altitude="3"/>
      <p:notify uri="mailto:alice@example.com"/>
    </p:action>
  </p:rule>
  <p:rule subject="C=US ST=Washington L=Seattle O=Amazon.com, Inc
    OU=Software CN=www.amazon.com"/>
  <p:rule hash-uri="6e8c81b2f0de5e5957871354761b56c5"/>
  <p:rule until="2004-05-31T13:20:00.000-05:00" duration="3600"/>
</p:disclosure>
```

Figure 1

A disclosure specification consists of any number of rules, where each rule consists of a 'match' description that determines when the rule applies and an 'action' element that enumerates which elements of the LO to include and exclude and whether the target needs to be notified.

While the disclosure information could be organized along any number of matching rules, this document chooses to make the recipient of the information the principal selection criteria. Among other reasons, it is easier to compare than the time and area selectors and seems most likely to be the most common criteria for allowing or disallowing disclosure. TBD: The destination could easily be made a peer of the other selection criteria.

A rule with no 'uri' attribute matches any destination. Like the 'default' tag in C switches, it is only used if no other rule matches according to the 'uri' tag.

Instead of a constant URI, simple 'glob' expressions can also be used for user@domain-style URIs such as SIP and mailto URIs. Only two wildcards are permitted: a '*' instead of the user name indicates that any user in the domain matches the rule, while a '*.' immediately following the '@' sign indicates that any subdomain within the domain matches. The '*' MUST NOT appear anywhere else. For example, 'alice@example.*.com' is invalid. (TBD: '*' is a legitimate user name, so an escaping rule is needed, strictly speaking.)

Instead of a literal URI, a rule can contain a hashed URI that is compared to the MD5 hash of the potential destination the holder of presence information wants to deliver data to. Hashed URIs can only be used for schemes that support a canonical form. Examples include SIP URIs [RFC3261]. Using hashed URIs avoids exposing the identity of favored or disfavored individuals to the watcher. Naturally, the watcher can still play a game of 'I wonder if the presentity likes Alice' by checking hashed URIs against a guessed list of friends and enemies.

As a third type of identifier, X.509 subject identities are supported, applicable when the location requestor can be verified using a X.509-using authentication protocol, such as CMS (S/MIME) or TLS.

Each 'to' element can specify a set of time restrictions during which disclosure is permitted.

The time recurrence rules are specified using the iCal notation in RFC 2445 [RFC2445], translated into XML schema format, roughly following the (expired) Internet draft draft-ietf-calsch-many-xcal-00. 'exdate' 4.8.5.2, 'rdate' 4.8.5.3, 'rrule', 4.8.5.4.0

The same 'uri' can appear multiple times. Disclosure is permitted if any of the matching rules allow disclosure. A rule matches if all elements of the rule match. If a rule contains an attribute that is unknown to the receiver, the rule does not match.

One or more 'include' elements enumerate, as XPath expressions, the elements that should be included in transmission, while the exclude explicitly removes elements from that list. If there is no 'include' element, all elements are included and need to be removed explicitly.

This mechanism is sufficient to limit the accuracy for civil

coordinates, but does not suffice for geospatial coordinates. The 'resolution' element restricts the resolution for geospatial coordinates and is measured in bits, similar to the LaRes, LoRes and AltRes parameters in draft-ietf-geopriv-dhcp-lo-option.

A target can request that all disclosures to a particular destination cause a notification to be sent to the target, using the 'uri' specified. The notification could be sent, for example, using instant messaging (im:), email (mailto:) or an HTTP request. This clearly has security implications, since a malicious target could use this mechanism to cause messages to be sent to third parties, introducing a new form of 'open proxy' spamming. Thus, such notification is only appropriate if the notifying party can convince itself that the address indeed belongs to the presentity. Unfortunately, there is no fool-proof way of ensuring that, but a recipient of this information may compare the non-schema part of the notification URI with the presentity and only allow notification on equality. Given these constraints and the inherent unreliability and delays in most current notification mechanisms, a target cannot rely on receiving notification.

4.4 Retention

```
<retention until="2004-05-31T13:20:00.000-05:00" duration="3600"/>
```

The 'until' attribute determines the absolute time until the recipient may retain this information. The 'duration' attribute determines the time duration, measured in seconds, counting from the time the location recipient has obtained the location object. [TBD: should this be a schema duration, in ISO 8601 format? Seconds seems easier and in line with other duration indications.]

Note that a location recipient that passes a LO to a third party MUST decrement the 'duration' attribute by the time it has held the location object.

If no attribute is specified, a default of one hour is assumed. If both 'until' and 'duration' attributes are specified, the shorter duration governs retention.

5. Location Information

Each tuple can have zero or more 'location' elements, each containing an alternate representation of a location for the tuple. PIDF allows tuples to have no contact element. We take this to represent the location of the presentity itself, if a single location can be unambiguously assigned to a presentity.

5.1 Geospatial Locations

Geospatial coordinates, multiple sightings and headings can be readily specified using the OpenGIS GML format. An example is shown in Figure 3.

```
<?xml version="1.0" encoding="UTF-8"?>
<presence ... xmlns:gml='http://www.opengis.net/gml'
  xmlns:loc='urn:ietf:params:xml:ns:geopriv-loc'
  entity='pres:alice@example.com'...>

  <tuple id="123">
    <status>
      <basic>open</basic>
    <status>

    <loc:location>
      <gml:Point>
        <gml:pos>40.85790 73.98857</gml:pos>
      </gml:Point>
    </loc:location>
  </tuple>
</presence>
```

Figure 3

5.2 Civil Locations

Civil locations use a hierarchy similar to [I-D.schulzrinne-geopriv-dhcp-civil]. An example is shown in Figure 4.

```
<?xml version="1.0" encoding="UTF-8"?>
<presence ... xmlns:loc='urn:ietf:params:xml:ns:geopriv-loc'
  xmlns:c='urn:ietf:params:xml:ns:geopriv-civil'
  entity='pres:alice@example.com'...>

  <tuple id="123">
```

```
      <loc:location>
        <c:c>US</c:c>
        <c:a1>NJ</c:a1>
        <c:a2>Bergen</c:a2>
        <c:a3>Leonia</c:a3>
        <c:a6>Westview</c:a6>
        <c:sts>Ave</c:sts>
        <c:hno>313</c:hno>
        <c:zip>10027</c:zip>
      </loc:location>
    </tuple>
  </presence>
```

Figure 4

5.3 Heading

Both civil and geospatial coordinates can contain heading vectors. TBD: how can GML speed, bearing, etc. be combined with civil coordinates?

6. Composition Rules

Composition is 'union' by default, i.e., all location objects are enumerated.

7. Notes on Requirements

This draft satisfies most of the requirements of draft-morris-geopriv-core. However, in a few instances, it intentionally deviates from the suggestions made. Below, we motivate our design choices.

In Section 3.2, Rule 4, the location seeker is identified simply by a URI. Unfortunately, this is insufficient, since there is no universal personal identifier. (There is no guarantee We qualify this 'user@domain' identifier with a URI scheme.

In Section 3.2, Rule 4, the accuracy requirement indicates kilometers. However, this is impossible to implement for civil coordinates and difficult for geospatial coordinates, as it requires spherical geometry. For values 'D' (local or municipial) and 'E' (state or regional), experience indicates that these nomenclatures are not used uniformly across countries. Thus, the explicit labeling by element chosen above appears to be more amenable to machine interpretation.

This document does not directly support consent. However, this can be emulated by having a one-time subscription and making the subscription itself require explicit consent from the presentity.

8. Open Issues

- Should the retention and disclosure rules apply to all RPIDS elements, not just location information?
- Given the security risks outlined above, is notification on disclosure realistic and appropriate?
- Default 'notify' element?

9. Security Considerations

See [I-D.ietf-geopriv-reqs].

References

[I-D.ietf-geopriv-reqs]
Cuellar, J., Morris, J. and D. Mulligan, "Geopriv requirements", draft-ietf-geopriv-reqs-03 (work in progress), March 2003.

[I-D.ietf-simple-pres-filter-reqs]
Moran, T., "Requirements for Presence Specific Event Notification Filtering", draft-ietf-simple-pres-filter-reqs-01 (work in progress), June 2003.

[I-D.ietf-simple-winfo-package]
Rosenberg, J., "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)", draft-ietf-simple-winfo-package-05 (work in progress), January 2003.

[I-D.morris-geopriv-core]
Morris, J., "Core Privacy Protections for Geopriv Location Object", draft-morris-geopriv-core-01 (work in progress), March 2003.

[I-D.peterson-geopriv-pres]
Peterson, J., "A Presence Architecture for the Distribution of Geopriv Location Objects", draft-peterson-geopriv-pres-00 (work in progress), February 2003.

[I-D.schulzrinne-geopriv-dhcp-civil]
Schulzrinne, H., "DHCP Option for Civil Location", draft-schulzrinne-geopriv-dhcp-civil-01 (work in progress), February 2003.

[I-D.schulzrinne-simple-rpids]
Schulzrinne, H., "RPIDS -- Rich Presence Information Data Format for Presence Based on the Session Initiation Protocol (SIP)", draft-schulzrinne-simple-rpids-01 (work in progress), February 2003.

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

[RFC2445] Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)", RFC 2445, November 1998.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

Author's Address

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

Phone: +1 212 939 7042
EMail: hgs+nsis@cs.columbia.edu
URI: http://www.cs.columbia.edu

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

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