Network Working Group   J. Peterson
Request for Comments: 4079   NeuStar
Category: Informational   July 2005

                  A Presence Architecture for the
              Distribution of GEOPRIV Location Objects

Status of This Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Copyright Notice

Abstract

   GEOPRIV defines the concept of a 'using protocol' -- a protocol that
   carries GEOPRIV location objects. GEOPRIV also defines various
   scenarios for the distribution of location objects that require the
   concepts of subscriptions and asynchronous notifications. This
   document examines some existing IETF work on the concept of presence,
   shows how presence architectures map onto GEOPRIV architectures, and
   moreover demonstrates that tools already developed for presence could
   be reused to simplify the standardization and implementation of
   GEOPRIV.

Table of Contents

[1](1). Introduction

   GEOPRIV is a standard for the transmission of location information
   and privacy policies over the Internet. Location information is a
   description of a particular spatial location, which may be
   represented as coordinates (via longitude, latitude, and so on), as
   civil addresses (such as postal addresses), or in other ways.
   GEOPRIV focuses on the privacy and security issues, from both a
   technology perspective and a policy perspective, of sharing location
   information over the Internet; it essentially defines a secure
   container class capable of carrying both location information and
   policy data governing the distribution of this information. GEOPRIV
   also defines the concept of a 'using protocol' -- a protocol that
   carries the GEOPRIV location object.

   Presence is a service defined in [RFC2778](RFC2778) [[2](2)] that allows users of a
   communications service to monitor one another's availability and
   disposition in order to make decisions about communicating. Presence
   information is highly dynamic, and it generally characterizes whether
   a user is online or offline, busy or idle, away from communications
   devices or nearby, and the like.

   This document shows the applicability of presence to GEOPRIV and
   shows that a presence protocol could be a suitable using protocol for
   GEOPRIV. This document is not intended to demonstrate that presence
   is the only method by which GEOPRIV location objects might be
   distributed. However, there are numerous applications of GEOPRIV
   that depend on the fundamental subscription/notification architecture
   that also underlies presence.

[2](2). Framework Analysis

   The GEOPRIV framework [[1](1)] defines four primary network entities: a
   Location Generator, a Location Server, a Location Recipient, and a
   Rule Holder. Three interfaces between these entities are defined,
   including a publication interface and a notification interface.

   GEOPRIV specifies that a 'using protocol' is employed to transport
   location objects from one place to another. If the publication
   interface and notification interface are network connections, then a
   using protocol would be responsible for the transmission of the
   location object. Location Recipients may request that a Location
   Server provide them with GEOPRIV location information concerning a

particular Target. The Location Generator publishes Location
Information to a Location Server, which, in coordination with
policies set by the Rule Maker, distributes the location information
to Location Recipients as necessary.

The GEOPRIV requirements document shows three scenarios for the use
of the GEOPRIV protocol. In some of these scenarios (such as the
third), a Location Recipient sends some kind of message to the
Location Server to request the periodic transmission of location
information. The location of a GEOPRIV Target is likely to vary over
time (if the Target is a person, or something similarly mobile), and
consequently the concept of a persistent subscription to the location
of a Target resulting in periodic notification is valuable to
GEOPRIV. In other scenarios, a Location Recipient may request a one-
time notification of the geographical location of the Target.

GEOPRIV places few requirements on using protocols. However, it is
clear from the description above that there must be some mechanism
allowing Location Recipients to establish a persistent subscription
in order to receive regular notification of the geographical location
of a Target as their location changes over time. There must also be
a way for Location Generators to publish location information to a
Location Server that applies further policies for distribution.

This document adopts a model in which the using protocol is
responsible for requesting subscriptions, handling publications, and
sending notifications. There are other models for GEOPRIV in which
these operations might be built into location objects themselves.
However, there is a significant amount of pre-existing work in the
IETF related to managing publications, subscriptions, and
notifications for data sets that vary over time. In fact, these
concepts all correspond exactly to architectures for presence that
have been developed in support of real-time communications
applications such as instant messaging, voice and video sessions.

Note that in some GEOPRIV scenarios, the Location Recipient does not
actively request the location of a Target; rather, it receives an
unsolicited notification of Target's location. This document focuses
on the use of presence only for scenarios in which the Location
Recipient actively solicits location information. However, it is
possible that many of these base operations of the

subscription/notification framework of presence could be reused for
cases in which the Location Recipient is passive.

3. Presence Architecture for GEOPRIV

   The Common Profile for Presence [4] (CPP) defines a set of operations
   for delivery of presence information. These primarily consist of
   subscription operations and notification operations. A subscription
   creates a persistent connection between a 'watcher' (which
   corresponds to the Location Recipient of GEOPRIV) and a 'presentity'
   (which corresponds roughly to the GEOPRIV target). When a watcher
   subscribes to a presentity, a persistent connection is created;

   notifications of presence information will henceforth be sent to the
   watcher as the presence information changes. CPP also supports
   unsubscriptions (terminating the persistent subscription) and fetches
   (one-time requests for presence information that do not result in a
   persistent subscription).

   CPP provides a number of attributes of these operations that flesh
   out the presence system. There is a system for automatically
   expiring subscriptions if they are not refreshed at user-defined
   intervals (in order to eliminate stale subscriptions). There are
   transaction and subscription identifiers used to correlate messages,
   and a URI scheme ("pres:") is defined to identify watchers and
   presentities.

   The IETF IMPP WG has also defined an XML data format for presence
   information, called the Presence Information Data Format [5] (PIDF).
   PIDF is a body that is carried by presence protocols and that
   contains presence information, including the current state of a
   presentity. PIDF is discussed in more detail in Section 4.

   At a high level, then, the presence architecture seems to have
   considerable applicability to the problem of delivering GEOPRIV
   information. However, the CPP framework is an abstract framework:
   it doesn't actually specify a protocol, instead it specifies a
   framework and a set of requirements to which presence protocols must
   conform. Also, CPP does not define any concept similar to a Location
   Server.

   However, the IETF has standardized protocols that instantiate this

framework, such as SIMPLE [6] and XMPP [7]. XMPP and SIMPLE both
have architectural elements comparable to a Location Server: points
where presentities register their availability, and where policies
for distributing presence can be managed. The presence community has
also defined a policy protocol and schema set called XCAP [8] through
which authorization policies can be provisioned in a presence server.

In summary, like GEOPRIV, presence requires an architecture for
publication, subscription, and notification for a mutable set of data
associated with a principal. Presence has already tackled many of
the harder issues associated with subscription management, including
subscription expiration, development of identifiers for principals,
and defining document formats for presence information. Rather than
reinvent work that has been done elsewhere in the IETF, GEOPRIV has
reused this existing work by specifying presence protocols as GEOPRIV
using protocols. Moreover, the existing foundational presence tools
developed in IMPP, such as PIDF, have immediate applicability to the
efforts underway in GEOPRIV to develop objects for sharing location
information.

4. GEOPRIV Extensions to PIDF

   As was mentioned above, the presence architecture developed in the
   IETF IMPP WG has defined a format for presence information called
   PIDF. PIDF is an XML format that provides presence information about
   a presentity. Primarily, this consists of status information, but it
   also optionally includes contact addresses (a way of reaching the
   presentity), timestamps, and textual notes with arbitrary content.

   PIDF is an extensible format. It defines an XML element for
   representing the status of a presentity (the status element), and it
   gives some guidance as to how this element might be extended.
   Although the authors of PIDF viewed geographical location as a
   potential category of presence information, baseline PIDF defines no
   format for location information.

   PIDF meets the security requirements given in RFC2779 [3] (see
   especially sections 5.1, 5.2, and 5.3), which parallel those of the
   GEOPRIV location object given in the GEOPRIV requirements [1]. CPP
   and PIDF specify mechanisms for mutual authentication of participants
   in a presence exchange as well as for confidentiality and integrity
   properties for presence information.

In short, many of the requirements of GEOPRIV objects map well onto the capabilities of PIDF.

5. Security Considerations

GEOPRIV information, like presence information, has very sensitive security requirements. The requirements of RFC2779 [3], which are instantiated by CPP, PIDF, and XCAP, in addition to the various derivative concrete presence protocols, such as XMPP and SIMPLE, map well onto the security requirements of the GEOPRIV protocol, as defined in the GEOPRIV requirements document and the GEOPRIV threat analysis [9] document. Specifically, the presence security requirements call for authentication of watchers, integrity and confidentiality properties, and similar measures to prevent abuse of presence information.

6. Acknowledgements

Thanks to Randall Gellens, John Morris, Hannes Tschofenig, and Behcet Sarikaya for their comments.

7. Informative References

[1]   Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "GEOPRIV requirements", RFC 3693, February 2004.

[2]   Day, M., Rosenberg, J., and H. Sugano, "A Model for Presence and Instant Messaging", RFC 2778, February 2000.

[3]   Day, M., Aggarwal, S., and J. Vincent, "Instant Messaging / Presence Protocol Requirements", RFC 2779, February 2000.

[4]   Peterson, J., "Common Profile for Presence (CPP)", RFC 3859, August 2004.

[5]   Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W., and

           J. Peterson, "Presence Information Data Format (PIDF)",
           RFC 3863, August 2004.

     [6]   Rosenberg, J., "A Presence Event Package for the Session
           Initiation Protocol (SIP)", RFC 3856, August 2004.

     [7]   Saint-Andre, P., "Extensible Messaging and Presence Protocol
           (XMPP): Instant Messaging and Presence", RFC 3921, October
           2004.

     [8]   Rosenberg, J., "The Extensible Markup Language (XML)
           Configuration Access Protocol (XCAP)", Work in Progress,
           February 2004.

     [9]   Danley, M., Morris, J., Mulligan, D., and J. Peterson, "Threat
           Analysis of the GEOPRIV Protocol", RFC 3694, February 2004.

Author's Address

     Jon Peterson
     NeuStar, Inc.
     1800 Sutter St., Suite 570
     Concord, CA 94520
     USA

     Phone: +1 925/363-8720
     EMail: jon.peterson@neustar.biz
     URI: http://www.neustar.biz/

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.

Acknowledgement