The IETF Geopriv and Presence Architecture Focusing on Location Privacy

Hannes Tschofenig*, Henning Schulzrinne†, Andrew Newton‡, Jon Peterson§, Allison Mankin¶
*Siemens Networks GmbH Co KG, Email: Hannes.Tschofenig@siemens.com
†Columbia University, Email: hgs@cs.columbia.edu
‡SunRocket, Email: andy.newton@sunrocket.com
§NeuStar, Email: jon.peterson@neustar.biz
¶National Science Foundation, Email: mankin@psg.com

***Abstract*— The Geographic Location/Privacy (Geopriv) working group 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 concept of subscriptions and asynchronous notifications. This document shows the big picture with the alignment of the Geopriv and the presence architecture.**

I. Introduction

Geopriv is a standard for the transmission of location information 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), or as civic addresses (such as postal addresses). The Geography Markup Language (GML) [1] is reused for the geospatial location format whereas civic information format was defined by the Geopriv working group (see [2]) and later extended in [3]. The work in the IETF Geopriv working group [4] particularly focused on the privacy and security issues, both from 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. So far, the work on using protocols has focused on SIP.

This document reuses Geopriv terminology defined in [5].

II. Framework

A. Entities

In [5] four primary entities are defined: 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.

Figure 1 shows how these entities interact and some example protocols are listed.

The usage of Geopriv is very flexible and might, in some scenarios, involve a number of different protocols as shown in Figure 1.

Position paper for the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement; 17 and 18 October 2006; Ispra/Italy

Fig. 1. Geopriv Entities

The privacy properties of Geopriv therefore depend a lot on the specific protocols being used. This may be seen as an advantage since existing protocols already provide a number of security mechanisms (e.g., anonymity support).

B. Using Protocol

Geopriv specifies that a 'using protocol' is employed to transport location objects from one place to another. Geopriv places a few requirements on these using protocols, which are described in [5]. 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 [5] shows three scenarios for the use of the Geopriv protocol. In some of these scenarios, 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. A Location Genera-

tor publishes location information to a Location Server that applies further policies for distribution.

When the abstract Geopriv architecture is combined with the presence architecture a model is created in which the using protocol is responsible for requesting subscriptions, handling publications, and sending notifications. There are other models for Geopriv in which such 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.

C. Location Object

The presence architecture developed in the IETF Instant Messaging and Presence Protocol (IMPP) working group [6] has defined a format for presence information called Presence Information Data Format (PIDF). PIDF is an XML format that provides presence information about a presentity - primarily, this consists of status information, but 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 gives some guidance on how this element might be extended. An extension to PIDF has been defined with a Presence-based Geopriv Location Object Format (PIDF-LO) [7] to carry Location Objects within PIDF. The term Location Object denotes location information that travels with privacy policies.

PIDF meets the security requirements given in RFC 2779 [8] (see especially Section 5.1, 5.2 and 5.3), which parallel the security requirements of the Geopriv Location Object given in the Geopriv requirements [5]. The Common Profile for Presence (CPP) [9] and PIDF specify mechanisms for mutual authentication of participants in a presence exchange as well as confidentiality and integrity properties for presence information.

PIDF-LO carries either civic, geospatial location information or both. The format of civic location information was first defined [2] since there was no prior work to reuse. The XML schema for the civic location information was provided within PIDF-LO and defines a number of elements representing tokens refering to location information, such as 'A1' representing the name of country. Later, the list of tokens was extended with [3]. With GML, however, there was plenty of work for encoding of various geospatial shapes, including Points, Polygons, Cycles, Ellipses, Arc Bands, Spheres, Ellipsoids, and Prisms. PIDF-LO mandates support for the GML 'feature.xsd' schema only that includes support for the above-mentioned shapes but excludes support for dynamic features, such as velocity.

D. Authorization Policies

In the Geopriv architecture, as indicated in Figure 1, location information must only be disclosed to authorized watchers. To ensure that the Location Server can make an informed decision it needs to possess rules indicating who has access to location items. In some scenarios the Location Server is co-located with the Target (e.g., because the Target obtained location information from the access network or via a GPS module) and the Target itself makes the authorization decision whether to disclose location information.

In some other scenarios the end host delegates some of these functions to a separate entity, the Location Server or Presence Server. The Rule Maker therefore needs to upload authorization policies, in the form of conditions, actions and transformations, to this server. Note that the Target will often play the role of the Rule Maker although there are cases where this is not desired. For example, parents (in the role of Rule Makers) might want to create authorization policies for their kids (in the role of Targets). Whenever a watcher requests access to location information of the Target the Location Server would first check the conditions part of the policies and in case of one or several rules matching evaluate the actions and transformations parts. More details about these authorization policies that are referred as Common-Policy [10] and Geopriv-Policy [11] will be described after we introduce the basic policy rules.

The basic policy rules are much simpler and travel always with location information (with a reference to a richer set of policy rules). Note that the term 'Location Object' is used when location information is bundled together with policy rules (within a PIDF-LO). These basic policy rules are also encoded as XML elements, as described in [7], and convey the following information:

- RETRANSMISSION-ALLOWED: This element provides information whether the Recipient of this Location Object is permitted to share the enclosed Location Information, or the object as a whole, with other parties.
- RETENTION-EXPIRES: This field specifies an absolute date at which time the Recipient is no longer permitted to possess the location information.
- RULESET-REFERENCE: This field contains a URI that indicates where a fuller ruleset of policies as available with [10] and [11].
- NOTE-WELL: This field contains a block of text containing further generic privacy directives.

Before a Location Server or Presence Server constructs a PIDF-LO that contains, among other things, privacy rules, location and presence information it needs to process the authorization policies. The Common-Policy [10] documents provides the basic rule structure using conditions, actions and transformations. Common-Policy only provides a few condition elements, namely identity-based conditions as well as sphere and validity. These elements are described in more detail in Section 7 of [10]. The conflict resolution mechanism defined in Common-Policy is important since it aims to offer privacy enhancing capabilities by demanding that permissions are additive; Applying additional policy rules only adds permissions rather than deleting them. This algorithm was designed to consider the fact that authorization policies might be distributed or evaluated in a distributed fashion

as the Location Object travels its way towards Location Recipients. If dereferencing a policy ruleset fails, privacy is not leaked. Geopriv-Policy [11] then extends Common-Policy with location-specific authorization policies with respect to conditions and transformations. The conditions part allow to make decisions based on the current location of the Target. The transformations enable the Rule Maker to control the values of information carried in the PIDF-LO, both location information and basic privacy rules. As a privacy feature, the Rule Maker is given the ability to control the granularity of the civic and geospatial location information that gets transmitted to the Location Recipient.

Common-Policy was extended with Presence Authorization Rules [12] to perform authorization decisions for a presence based system. For a location-based presence system the Geopriv Policies and the Presence Authorization Rules would be combined by the Rule Maker.

Examples for authorization policies can be found in Section 9 of [11] and in Section 5 of [12].

III. Geopriv-Based Presence Architecture

This section shows the applicability of presence to Geopriv, as a more specific example. There are numerous applications of Geopriv that depend on the fundamental subscription/notification architecture that also underlies presence.

A. Introduction

Presence is a service defined in RFC 2778 [13] 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 generally characterizes whether a not a user is online or offline, busy or idle, away from communications devices or nearby, and the like.

CPP [9] 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 Location Server). 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 result in no 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.

At a high-level, then, the presence architecture is applicable to the problem of delivering Geopriv information. However, the CPP framework is an abstract framework - it does not actually specify a protocol, 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, nor any way for presence information to be published to a Location Server.

Fig. 2. Example of a location-based Instant Messaging Application

SIMPLE [14], the application of the Session Initiation Protocol (SIP) to instant messaging and presence, is one protocol that instantiates the CPP format and extends it in a number of important ways. SIP has native support for subscriptions and notifications (in its events framework [15]) and has added an event package [16] for presence in order to satisfy the requirements of CPP. Above and beyond CPP, SIMPLE has done work on a publication method [17] that will allow presence information to be published by presentities to a server that will apply various policies before sharing presence information with watchers (in the SIMPLE publication architecture, this server is known as a compositor). With the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) [18] a protocol was specified that allows authorization policies to be provisioned in to a presence or a location server.

B. Sample Instantiation

To be more specific, consider an instant messaging application where users distribute their presence information including location information. Figure 2 shows the participating entities graphically.

Consider a presentity who wishes to distribute location information as part of the presence information. After registering to the Location Server which is a presence service location information as part of a PIDF document. If a Watcher (i.e., Location Recipient) wants to fetch presence information of a particular presentity (i.e., Target) in this example. The Location Object, which contains location information and authorization policies, is sent to the Watcher confidentially. For further distribution of the Location Object by the Watcher the attached policies in the PIDF-LO need to be inspected.

In many cases the Presentity might not allow unrestricted distribution of presence and location information. Therefore, authorization policies need to be available at the Location Server to evaluate whether a particular watcher is allowed to retrieve certain presence information items. These policies are created, modified and delete by the Rule Holder as shown in Figure 2, for example, using XCAP. In many scenarios the Rule Holder will be equivalent with the Presentity or Target. In other scenarios, these policies might be provided by a third party, e.g., parents create these policies for their children.

IV. Conclusion

Privacy is a feature of an entire architecture. The work on authorization policies to limit the distribution of location and presence information is an important building block. The ability to allow policies to travel with location information is the next step to improve privacy protection[1]. In order to accomplish results that are usable by the Internet community as a large it is required to fulfill two requirements:

- The solution must be as simple as possible in order to have a chance to see deployment. For example, reusing existing policy languages, such as the eXtensible Access Control Markup Language (XACML) that provides a very flexible framework, would have made the Geopriv architecture considerably more complex. In fact, an XACML [19] based solution was proposed (see [20]) and rejected by the working group. More complex identity based conditions were also postponed to future versions, such as identity based conditions that align the Security Assertion Markup Language (SAML) with the Geopriv authorization policies (as described in [21]) in order to simplify the base specification. The same is true for non-identity based authorization mechanisms.
- The solution has to leverage available and deployed protocols as much as possible to lower the development effort and to lower the barrier of deployment. The working group is able to develop the SIP using protocol case to fullness, in SIP Location Conveyance [22], because SIP offers a rich semantic with regard to user identities and privacy aspects.

  The working group started with SIP as a using protocol[2], as described in SIP Location Conveyance [22]. SIP offers a rich semantic with regard to user identities and privacy aspects. Recent work in SIP regarding privacy [24], [25], SIP identity enhancements [26], [27], the SIP Certificate Management Service [28] and SAML usage within SIP [29] can be reused.

V. Acknowledgements

We would like to thank Brian Rosen, Carl Reed, James Polk, James Winterbottom, John Morris, John Schnizlein, Jonathan Rosenberg, Jorge Cuellar, Marc Linsner, Martin Thomson, Randall Gellens and Ted Hardie for their invaluable help in the Geopriv working group.

References

[1] "Open Geography Markup Language (GML) Implementation Specification," Jan. 2003, oGC 02-023r4, http://www.opengeospatial.org/specs/?page=specs.

[2] H. Schulzrinne, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," Jan. 2006, IETF draft (work in progress), draft-ietf-geopriv-dhcp-civil-09.txt.

[3] M. Thomson and J. Winterbottom, "Revised Civic Location Format for PIDF-LO," Apr. 2006, IETF draft (work in progress), draft-ietf-geopriv-revised-civic-lo-02.txt.

[4] "Geographic Location/Privacy (geopriv)," Sept. 2006, http://www.ietf.org/html.charters/geopriv-charter.html.

[5] J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk, "Geopriv Requirements," Oct. 2003, RFC 3693, Request For Comments.

[6] "Instant Messaging and Presence Protocol (impp)," Sept. 2006, http://www.ietf.org/html.charters/OLD/impp-charter.html.

[7] J. Peterson, "A Presence-based GEOPRIV Location Object Format," Dec. 2005, RFC 4119, Request For Comments.

[8] M. Day, S. Aggarwal, and J. Vincent, "Instant Messaging / Presence Protocol Requirements," Feb. 2000, RFC 2779, Request For Comments.

[9] J. Peterson, "Common Profile for Presence (CPP)," Aug. 2004, RFC 3859, Request For Comments.

[10] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," Aug. 2006, IETF draft (work in progress), draft-ietf-simple-xcap-11.txt.

[11] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, and J. Polk, "A Document Format for Expressing Privacy Preferences for Location Information," Feb. 2006, IETF draft (work in progress), draft-ietf-geopriv-policy-08.txt.

[12] J. Rosenberg, "Presence Authorization Rules," June 2006, IETF draft (work in progress), draft-ietf-simple-presence-rules-07.txt.

[13] M. Day, J. Rosenberg, and H. Sugano, "A Model for Presence and Instant Messaging," Feb. 2000, RFC 2778, Request For Comments.

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

[15] A. Roach, "Session Initiation Protocol(SIP)-Specific Event Notification," June 2002, RFC 3265, Request For Comments.

[16] J. Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)," Aug. 2004, RFC 3856, Request For Comments.

[17] A. Niemi, "Session Initiation Protocol (SIP) Extension for Event State Publication," Oct. 2004, RFC 3903, Request For Comments.

[18] J. Rosenberg, "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," May 2006, IETF draft (work in progress), draft-ietf-simple-xcap-11.txt.

[19] "The OASIS eXtensible Access Control Markup Language (XACML), Version 2.0," Feb. 2005, http://www.oasis-open.org/committees/xacml.

[20] H. Tschofenig and J. Cuellar, "Geopriv Authorization Policies," June 2003, IETF draft (expired), draft-tschofenig-geopriv-authz-policies-00.txt.

[21] C. Guenther, "SAML in Authorization Policies," Feb. 2005, IETF draft (expired), draft-guenther-saml-policy-00.txt.

[22] J. Polk and B. Rosen, "Session Initiation Protocol Location Conveyance," Sept. 2006, IETF draft (work in progress), draft-ietf-sip-location-conveyance-04.txt.

[23] H. Tschofenig, F. Adrangi, M. Jones, and A. Lior, "Carrying Location Objects in RADIUS," Sept. 2006, IETF draft (work in progress), draft-ietf-geopriv-radius-lo-10.txt.

[24] C. Jennings, J. Peterson, and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," Nov. 2002, RFC 3325, Request For Comments.

[25] J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)," Nov. 2002, RFC 3323, Request For Comments.

[26] J.Peterson, "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," Sept. 2004, RFC 3893, Request For Comments.

[27] J. Peterson and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," Aug. 2006, RFC 4474, Request For Comments.

[28] C. Jennings, J. Peterson, and J. Fischl, "Certificate Management Service for The Session Initiation Protocol (SIP)," May 2006, IETF draft (work in progress), draft-ietf-sip-certs-01.txt.

[29] H. Tschofenig, J. Hodges, J. Peterson, J. Polk, and D. Sicker, "SIP SAML Profile and Binding," 2006, IETF draft (work in progress), draft-ietf-sip-saml-00.txt.

[1] The ability for a Location Recipient to publish its privacy policies, similiarly to the model offered by P3P, is not offered by the Geopriv architecture.

[2] Note that RADIUS is another Geopriv using protocol [23] but a description is outside the scope of this paper.