# Location Privacy Enforcement in a Location-Based Services Platform

John F. Buford, Xiaotao Wu, Saratchand Kanuri, Ratan Bajpai, Venkatesh Krishnaswamy
Avaya Labs Research
Basking Ridge, New Jersey 07920, USA

*Abstract*—**Location privacy management is an important requirement for location based services. Here we describe the design and implementation of location privacy enforcement mechanisms based on the IETF Geopriv specifications as part a location-based services platform that we previously developed. Our design involves a new and more efficient session-based access validation mechanism. In addition, we evaluate the expressiveness of Geopriv rules for describing a variety of privacy rules. We find a number of limitations and propose some methods for extending the rule notation for addressing these limitations. We conclude with an overview of our prototype implementation.**

***Index Terms***—**Geopriv, Location-based Services, Privacy.**

## I. Introduction

In previous work [1] we developed an enterprise grade location-based services (LBS) platform which features 1) integration with the enterprise communications infrastructure, 2) the use of a separate architectural event processing component for performing low-level location stream processing. We implemented a number of location-based applications on this platform and evaluated its scalability.

In this paper, we extend this architecture to conform to location privacy policy enforcement as defined by the IETF GEOPRIV specifications. Location privacy is a important requirement for location-based services which transmit a target's location objects (LOs) to other parties for processing. Due to both legal and social implications, wide-spread adoption of location-based services depends on effective mechanisms for setting constraints or rules on location access, and enforcing these rules at access time.

This paper contains the following contributions: (1) a privacy enforcement model that validates at the target subscription level rather than per LO, reducing overhead; (2) analysis of limitations of the GEOPRIV policy schema and proposed extensions [2], including the need for aggregation, role-based access, and location attributes; (3) we describe a prototype implementation.

The remainder of this paper is organized as follows. We present related work in the next section. Section 3 describes the new session-based privacy enforcement mechanism. Section 4 presents examples of privacy rule sets and discusses some limitations. Section 5 summarizes our proposal to extend the rule set notation, and section 6 describes our prototype. Section 7 concludes the paper.

## II. Related Work

User's privacy is a key issue in the ability of third parties to provide LBS. Approaches for preserving user's privacy can be broadly classified into:

1. Access control of user's location information via use of location privacy policies.
2. Location anonymization which uses location hiding techniques such that a correlation between the user's identity, his location update and the location based service request cannot be made.

Standards groups working on policy based solutions include W3C Platform for Privacy Preferences (P3P) and IETF Geographic Privacy (Geopriv) working group.

P3P [10] enables a website to express privacy policies in a standard human and machine readable format. Decision making regarding specific policies can be automated via standard software tools which summarize and compare policies with user preferences and alert them where applicable. P3P policies make users aware of privacy practices of an LBS application which in turn would allow them to opt-in or opt-out based on their personal preferences. A typical P3P policy might contain name and contact information for the LBS, access provided, data collected, how the data is used, whether users can opt-in or opt-out of any of these uses, and the data retention policy.

Geopriv [3][4] provides a framework for handling user privacy issues in the context of location based services, including protocols and formats for the conveyance of location information. Geopriv defines a secure container class [9] to carry location information as well as privacy policy data that governs how this location information is used and distributed. Geopriv extends Presence Information Data Format (PIDF) to include location object (LO) conveyance, called Presence-based Geopriv Location Object Format (PIDF-LO).

In the Geopriv model (Fig. 1), a target called a location generator (LG) produces position objects as a stream of LOs. These are encoded in PIDF-LO. The LO carries basic policy rules—regarding retransmission, expiration, and a reference to a more comprehensive authorization rule set. The target separately defines the authorization rule set for location recipients (LR) which are stored at a rule maker. A location server retrieves the rule sets from the rule maker and validates requests by LRs to access a specific target's LOs.

978-1-4244-2309-5/09/$25.00 ©2009 IEEE

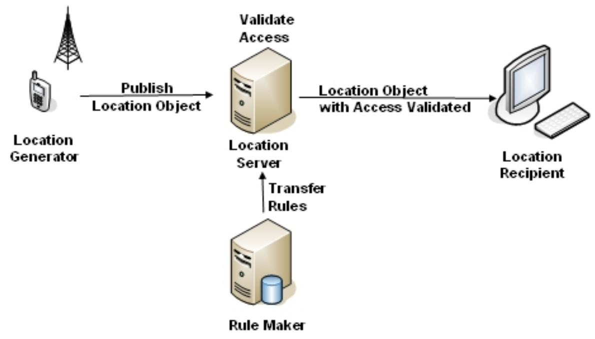

Fig. 1 GEOPRIV model

LocSrv [7] is a location server that uses a modified version of the P3P format for describing the context. Attributes of LocSrv policies include the identity of the LR, identity certification, context of request (co-located or asynchronous), retention, redistribution, and time constraint. In addition, enforcement of anonymity can be prescribed, and the use of a specified validation agent can be defined.

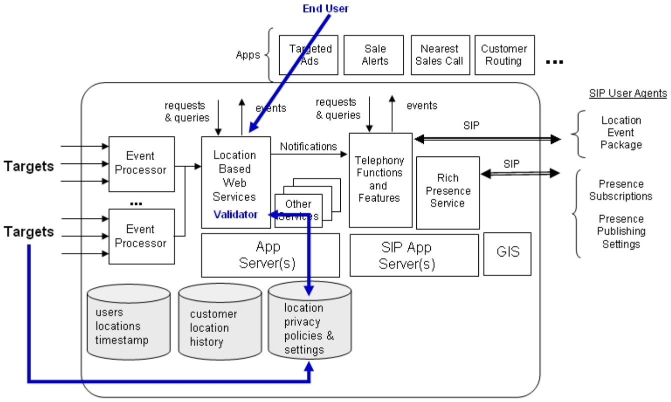

Fig. 2 LBS platform developed by authors [1] with extensions for privacy rule enforcement as indicated

Gajparia et al. [5] use an encrypted token generated by the target to enforce authorization. The token is encrypted using a security key such that only a trusted third party can access the LO. After a LBS service provider receives the token from the target, it forwards it to the trusted third party. The trusted third party decrypt the LO, applies the constraints on the LO, and sends a response to the service provider.

Location anonymization approaches include location perturbation, anonymous routing, and mix zones. A survey of these models can be found in [10]. Mokbel [6] anonymizes positions of different targets by mixing their positions in a given area.

## III. Session-Based Privacy Enforcement in LBS Platform

In this section we present new work in which we combine the Geopriv model with our previously developed LBS platform [1], as shown in Fig. 2. The LR is an application operated by a service provider or an enterprise. Targets generate a stream of location objects which are received by the event processor (EP). The EP performs spatio-temporal event correlation to produce events specific to LBS applications running on the application server. The application server also runs a service called the validator for validating other LBS application requests. The validator receives the privacy rule sets for a target from either the target or from a rule maker server.

As an example, an asset tracking application might request a notification be sent to it when an asset moves outside a given area. In our platform, the asset tracking service runs on an application server. When it receives a request from some application for a notification, the request is forwarded to the event processor. The EP monitors the stream of LOs for that target, and when the location leaves the indicated area, the EP forwards an event to the asset tracking service. Advantages of this architecture are reducing the overhead on the application server, reducing overall message traffic, and permitting other types of events to be integrated in the processing [1].

Since the asset position is determined by the owner or user of the asset, privacy issues arise. Before the asset tracking service forwards the request to the EP, it first validates that the user of the application is authorized according the current rule set for that target. The asset tracking service invokes the validator service, identifying the target, the LR, and other parameters of the request. The validator evaluates the request against the rule sets. It can determine that the request is permitted completely, permitted partially, or not allowed. A partial permission would occur if the permission is constrained by time or area, and the request exceeds the constraint in an overlapping way. The validator returns a modified request with the permitted attributes if a partial permission case occurs. If the request is validated, then the service forwards the request to the EP. Otherwise the application is notified of an authorization failure.

The validation is effective until the application terminates or cancels the request. In addition, the target may subsequently change the rule set. Rule set changes are propagated to the validator. When the validator receives notification of a rule set change, it checks all active sessions that is has validated to determine which ones might be effected. Any session that is rescinded is notified, the request to the EP is terminated, and the application receives an authorization failure notification.

In Geopriv, the rule maker can be implemented by an XCAP [14] server. Then, dynamic rule set changes can be propagated from an XCAP server using XML patches as described in [15]. The implications of this for our design are: 1) the validator uses SIP event package to subscribe to changes in each XML rule set document, 2) the validator processes these changes in the form of XML patches, 3) the validator determines which active permission(s) are effected by the change, and processes these as described above.

The steps in the privacy authorization mechanism are shown in Fig. 3.

## IV. Privacy Rule Set Examples

### A. Scope and Basic Example

The Geopriv access control rule set [12][13] permits the following types of controls over location information:

- prohibiting dissemination to particular individuals
- prohibiting dissemination during particular times
- prohibiting dissemination when the target is located in a specific region
- constraining that only certain parts of the LO are to be distributed to recipients
- specifying that the resolution of parts of the LO are to be reduced.

Policy rules have an if-then syntax as shown below. Conditions can be combinations of identity, sphere, or validity period. If all conditions match, then the permission is granted, subject to actions or transformations such as reducing the resolution of the LO. Location-specific conditions are added to the policy rules by [13].

```
<rule id="f3g44r1">
  <conditions>
    <identity>
       <!-- list of entities the rule applies to -->
    </identity>
       <!-- states the target must be in for the rule to match -->
    <sphere value="work"/>
       <!-- rule validity period -->
    <validity>
       <from></from>
       <until></until>
    </validity>
  </conditions>
  <actions/>
  <transformations/>
</rule>
```

For example, the following is an example rule set with one rule using the Geopriv common policy [12].

Bob is permitted access while the target is at work during a 2 hour period on 12-24-2004 (source: [12])

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy">
   <rule id="f3g44r1">
      <conditions>
         <identity>
            <one id="sip:bob@example.com"/>
         </identity>
         <sphere value="work"/>
         <validity>
            <from>2003-12-24T17:00:00+01:00</from>
            <until>2003-12-24T19:00:00+01:00</until>
         </validity>
      </conditions>
      <actions/>
      <transformations/>
   </rule>
</ruleset>
```

In the remaining examples we show only the necessary XML fragments to illustrate key issues regarding the expressiveness of these rules.

### B. *Identity vs. Groups*

The identity condition requires that permitted LRs be enumerated; alternately, an entire domain can be specified. The following example illustrates a scenario in which a group is not a single domain.

I permit my buddies in NYC to see my location only when I am in NYC.

```
       <identity>
                 <one id="sip:alice@example.com"/>
                 <one id="tel:+1-212-555-1234" />
                 <one id="mailto:bob@example.net" />
      </identity>
         <gp:location-condition>
           <gp:location profile="civic-condition"
             xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
             <country>USA</country>
             <A1>NY</A1>
             <A3>NYC</A3>
           </gp:location>
         </gp:location-condition>
```

A disadvantage of explicit enumeration is frequent maintenance. Each time one's social network or buddy list changes, then the rule set has to be changed and re-issued. Additionally it is common to have contact lists and buddy lists maintained in other applications. Being able to reference these lists via a URL could be used to avoid enumeration and duplicate lists.

### C. *Enumeration vs. Group Identity*

Another example involving explicit enumeration is the following reference to "customer site".

I permit my employer to see my location when I am at a company or customer site.

```
    <gp:location-condition>
       <!--company location in civic address form-->
       <gp:location profile="civic-condition"
         xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         <country>DE</country>
         <A1>Bavaria</A1>
         <A3>Munich</A3>
         <A4>Perlach</A4>
         <A6>Otto-Hahn-Ring</A6>
         <HNO>6</HNO>
       </gp:location>
      <!—enumeration of customer sites -->
      <gp:location profile="civic-condition"
         xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         <country>DE</country>
         <A1>Bavaria</A1>
         <A3>Munich</A3>
         <A4>Perlach</A4>
         <A6>Otto-Hahn-Ring</A6>
         <HNO>8</HNO>
       </gp:location>
     </gp:location-condition>
```

The goal of this rule is to distinguish when a target is at a work site versus in transit or on personal business. To avoid explicit enumeration in the rule, a URL to an external list or a DBMS query string could be added.

### D. *Large Sets*

For applications such as location-based push advertisements, users might permit notification whenever they are in the vicinity of a particular brand of retail store. For example:

I permit a vendor (e.g., BestBuy or McDonalds) to see my location when I am within .25 miles of a specific store

```
<rule id="BB56A19">
   <conditions>
       <identity>
            <many domain="McDonalds.com"> </many>
       </identity>
      <gp:location-condition>
      <gp:location profile="geodetic-condition">
     <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
        <!--this is the location of one store-->
       <gml:pos>-34.410649 150.87651</gml:pos>
       <gs:radius uom="urn:ogc:def:uom:EPSG::9001">
         0.25miles</gs:radius>
        </gs:Circle>
        </gp:location>
       </gp:location-condition>
    </coonditions>
```

A difficulty in these types of rules is for the user to actually be able to know the location of all such stores. Additionally, the list could be very large for many retail brands.

### *E. Domains and Their Representatives*

A related issue in permitting access to a large organization is to reasonably restrict those employees who actually might have the access. On the one hand, the user wants the convenience of being able to identify a specific brand, as in the previous example where we simply identify "mcdonalds.com". On the other hand, there is no control or visibility as to who in the organization (e.g., tom@hertz.com) or what portions of the organization (e.g., location-services@hilton.com), is included.

When I arrive at an airport, I permit major hotel chains (Hilton, Marriott, etc.) and major car rental chains (Hertz, Avis, etc.) to see my position at a 500m resolution

```
<rule id="BB56A19">
    <conditions>
       <identity>
            <many domain="Hilton.com"/>
             <many domain ="Marriott.org"/>
       </identity>
       <gp:location-condition>
        <gp:location profile="civic-condition">
              <country>USA</country>
              <A1>NY</A1>
               <A3>NYC</A3>
               <A4>JFK Airport</A4>
         </gp:location>
        </gp:location-condition>
       </conditions>
```

As in the previous examples, there are difficulties in explicitly listing all airports, and their positions.

## V. Extending RPID

In this section we briefly summarize our proposal to extend policy rules specification defined in [12][13] to address the limitations identified in the previous section. Further information is available in [2].

The geo-location policy [13] defines two profiles for location condition checking: the geodetic location condition profile and civic location condition profile. Users can use the two profiles to check a location against a geospatial area. But in some cases, users may want to check the attributes of a location, such as the sphere (e.g., home or work) and place type (e.g., airport) to define privacy policies. In addition, we would like to incorporate aggregation and indirection mechanisms to avoid explicit enumeration of identity and locations.

The geodetic and civic location condition profiles are not sufficient for these requirements. For example, Section IV-E's example can only work for a specific airport, not for any airport in general. Therefore, we introduce a new profile that contains the location related elements defined in Rich Presence Extensions to the Presence Information Data Format (RPID) for location condition checking. The elements we use include "place-is", "place-type", "privacy", and "sphere".

The following example uses the proposed "place-type" element to allow some hotels to access the user's location when the user is at an airport, not matter where the airport is.

```
  <rule id="NM32848">
    <conditions>
      <identity>
          <one domain="hertz.com"/>
          <one domain="avis.com"/>
          <one domain="budget.com"/>
      </identity>
      <gp:location-condition>
        <gp:location profile="rpid-condition">
          <rpid:place-type>
            <lt:airport/>
          </rpid:place-type>
        </gp:location>
      </gp:location-condition>
    </conditions>
    <transformations/>
  </rule>
</ruleset>
```

The example below uses "sphere" to allow user bob@example.net to access the user's location information. This rule keeps valid even if the user's home is moved to a new address.

```
<rule id="NM32848">
    <conditions>
      <identity>
        <many>
          <except id="sip:bob@example.net"/>
        </many>
      </identity>
      <gp:location-condition>
        <gp:location profile="rpid-condition">
          <rpid:sphere>
            <rpid:home/>
          </rpid:sphere>
        </gp:location>
      </gp:location-condition>
    </conditions>
    <transformations/>
  </rule>
```

The following example illustrates how to avoid explicit enumeration by referencing a list via an *heldref:* URI [17] or XLink to a separate file containing the list. It also incorporates an XPointer expression to select specific entries of interest.

We replace the airport place-type above with an enumeration. Assume that airports.xml contains a list of commercial airports organized geographically. When the embedded XLink/XPointer/XPath expression is parsed, it selects the elements and subtree for airports that are in NY and NJ.

The fragment of the location condition:

```
<gp:location-condition>
  <gp:location profile="civic-condition">
    <lt:airport xmlns:xlink="http://www.w3.org/1999/xlink"
      xlink:href="www.places.org/airports.xml"#xpointer(
       '//country[@name='USA']/st[@name='NJ']/place/descendant::* |
       //country[@name='USA']/st[@name='NY']/place/descendant::* '
     />
   </gp:location>
  </gp:location-condition>
```

The airports.xml file might contain (partial view):

```
<airports>
  <country name="USA">
     <st name="NJ">
         <place name="Newark-Liberty International Airport">
           <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
             <gml:pos>40.69250 -74.16867</gml:pos>
             <gs:radius uom="urn:ogc:def:uom:EPSG::9001">
```

```
                    0.25miles</gs:radius>
                </gs:Circle>
            </place>
        </st>
        <st name="NY">John F. Kennedy International Airport
            ....
        </st>
    </country>
</airports>
```

The XML list must be organized to support selection by a variety of criteria of interest. This approach can also be applied to the other enumeration examples described earlier.

## VI. Prototype of Policy Validator

The validator described in section 3 was implemented and tested with a location-based push advertisement service running on a JBoss application server. When the target approaches the area of interest (AOI), the event processor sends a notification to the web service, and advertisements are sent from the service to the target, provided the permission validation in the session is true.

The application invokes the service by submitting the identity of the user (targetID) and the area of interest(AOI). If the validator returns true then the subscription is forwarded to the event processor, a listener is added at the validator and a session is established. The validation is retained with the session state. If the privacy rule set of the target is changed, then the validation may change. Then listener is invoked and the validation is re-evaluated. The session will be updated with this new validation and subsequent changes will be done.

Fig. 4 shows the basic design of our implementation. An application invokes the init() function. This function in turn calls the validate function of the validator. If the validation succeeds, then a listener is registered at the validator using the addListener() function. Thus a session is established for this particular subscription. The LR can use the methods of the service if the validation of the session is true. When the rule set for the target changes, then the listener will be invoked and validation in the session is done again.

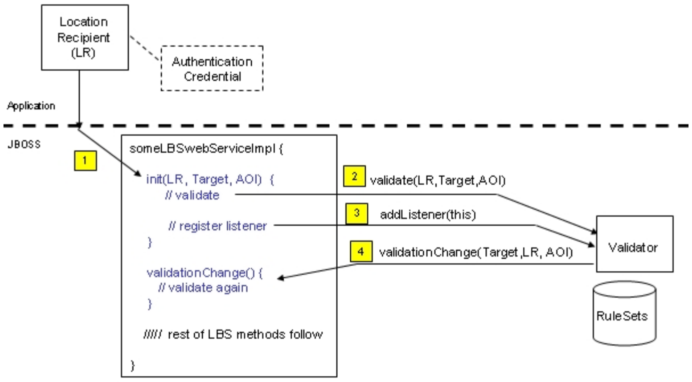

Fig. 3 Example integration of the validator and a LBS web service

## VII. Conclusion

Location privacy management is an important requirement for location based services. Here we described the design of location privacy enforcement mechanisms based on the IETF GEOPRIV specifications as part a location-based services platform that we previously developed. Our design involves a new and more efficient session-based access validation mechanism. In addition, we evaluated the expressiveness of GEOPRIV rules for describing a variety of privacy rules. We find a number of limitations and proposed some methods for addressing these limitations. Finally we described the operation of our prototype implementation.

## VIII. References

[1] J. Buford, X. Wu, R. Bajpai, S. Karthikeyan, V. Krishnaswamy. Enterprise Communications Platform Support for Integrated Location-Based Applications. Second IEEE Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST 2008). Sept 2008, Cardiff, Wales.

[2] X. Wu, J. Buford, et al. Enhancements to GEOPRIV Policy Schema. IETF Work in progress.

[3] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk, Geopriv Requirements, RFC 3693, February 2004

[4] J. Peterson, A Presence-based Geopriv Location Object Format, RFC 4119, December 2005

[5] A. S. Gajparia, C. J. Mitchell, and C. Y. Yuen. Supporting User Privacy in Location Based Services IEICE Transactions on Communications 2005 E88-B(7):2837-2847.

[6] M. F. Mokbel. Towards Privacy-Aware Location-Based Database Servers. In Proceedings of the 22nd Intl. Conf. on Data Engineering Workshops (April 03 - 07, 2006).

[7] G. Myles, A. Friday, N. Davies. Preserving Privacy in Environments with Location-Based Applications. IEEE Pervasive Computing 2, 1 (Jan. 2003), 56-64.

[8] A. R. Beresford, F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing 2, 1 (Jan. 2003), 46-55.

[9] S. Bessler. A system for locating mobile terminals with tunable privacy. J. Theor. Appl. Electron. Commer. Res. 2, 2 (Aug. 2007), 82-91.

[10] L. Liu. Protecting Location Privacy in Mobile Computing Systems: Architecture and Algorithms, The Thirteenth Annual Intl Conf on Mobile Computing and Networking (ACM Mobicom 2007), Montreal, Quebec, Canada. Sept 9-14, 2007.

[11] H. Tschofenig, H. Schulzrinne, A. Newton, J. Peterson, A Mankin, The IETF Geopriv and presence architecture focusing on location privacy, Position paper at W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Ispra, Italy, 2006.

[12] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, J. Rosenberg. Common Policy: A Document Format for Expressing Privacy Preferences. IETF RFC 4745. Feb 2007.

[13] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk. Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information. IETF draft-ietf-geopriv-policy-17, Work in progress. June 2008.

[14] J. Rosenberg. The Extensible Markup Language (XML) Configuration Access Protocol (XCAP). IETF RFC 4825. May 2007.

[15] J. Rosenberg, J. Urpalainen. An Extensible Markup Language (XML) Document Format for Indicating A Change in XML Configuration Access Protocol (XCAP) Resources. draft-ietf-simple-xcap-diff-09. Work in progress. May 2008.

[16] Open Mobile Alliance. Mobile Location Protocol (MLP). Candidate Version 3.1. OMA-LIF-MLP-V3_1-20040316-C. March 2004.

[17] M. Barnes, Ed. HTTP Enabled Location Delivery (HELD). draft-ietf-geopriv-http-location-delivery-08. Work in progress. July 2008.