Geographical Location and Privacy at the IETF

Hannes Tschofenig

Acknowledgements

- This slide set is based on slides by Jon Peterson.
- Acknowledgements to the IETF Geopriv working group and in particular to the following members:
  - Ted Hardie
  - Jon Peterson
  - Allison Mankin
  - Henning Schulzrinne
  - James Polk
  - John Morries
  - Jorge Cuellar
  - Jonathan Rosenberg
  - Andrew Newton
  - Randall Gellens

Geographical Location

- Location can be described in many ways
  - Civic (postal) address
  - Geospatial info
  - Place type
- Sometimes the end host knows its location and sometimes someone else in the network knows it.
- Privacy plays an important role and needs to be considered very early in the design

IETF Approach
Overview

- Offer standardized location information that can be exchanged in a number of protocols (using protocols)

- Offer a privacy framework to authorize distribution of location information using privacy rules

- Allow end host to learn location information (e.g., DHCP)

Location Info and Using Protocols

- Work done in GEOPRIV WG
  - Met for the first time at 50th IETF (August 2001)
  - Charter with strong privacy focus
  - Participation from industry vendors, standards professionals, policy experts, and academia
- Identify using protocols for carrying location information allowing a push/pull and a subscription model
  - Example: SIP
- Location format, as defined by OpenGIS, was reused: Geography Markup Language (GML)

Privacy Framework

- Location Information never travels without privacy rules: Location Object = Location Info + Privacy Rules
- Motivation:
  - Third parties enforce policies on behalf of “rule maker”
  - Rule Maker may not be the owner of the target device
  - Distributed authorization decision while location information travels through the network
  - Simple conflict resolution to deal with failure cases, distributed environment and to avoid unwanted leakage of information
- Result: Two authorization policy rule sets
  - Basic authorization rules: Very basic policies
  - Extended authorization policy: Flexible, extensible but still simple policies with high expressiveness
- Presence Information Data Format (PIDF) enhanced to carry Location Object

Basic GEOPRIV Architecture

Target

Might (or might not) have a relationship with the entities below.

Location Generator

Publication

Location Server

Notification

Location Recipient

Policy

Rule Repository

Benefits

- Geopriv architecture maps nicely to the presence architecture:
  - Integration of authorization framework into presence architecture
  - Enhancing presence architecture with Location Objects
  - Rich semantic due to combination of SIP and Geopriv -> Emergency Context Resolution with Internet Technologies (ECRIT)
    - Call identification
    - Call routing (based on location and other context information)

Backup Slides

PIDF-LO

- Presence Information Data Format (PIDF) is an XML-based format for presence
- Extends PIDF to accommodate two new elements:
  - Location-Info
    - Encapsulates a location information
    - GML 3.0 <feature.xsd> schema is mandatory-to-implement for all GEOPRIV-compliant applications
    - Also defines an optional civic location format
  - Usage-rules
    - Used to indicate privacy preferences

Abbreviated PIDF-LO example

```
<presence… entity="pres:joe@example.com">
 <tuple id="12345">
  <status>
   <geopriv>
    <location-info>
      <gml…>
      </gml>
    </location-info>
    <usage-rules>
      <retention-expiry/>
      <retransmission-allowed/>
      <note-well>…</note-well>
    </usage-rules>
   </geopriv>
  </status>
 </tuple>
</presence>
```

Location specific information
- GMLv3
- Civic Location

Authorization Rules

Example of GML 3.0

```
<location-info>
 <gml:location>
  <gml:Point gml:id="point96"
     srsName="epsg:4326">
  <gml:coordinates>31:56:00S
     115:50:00E</gml:coordinates>
  </gml:Point>
 </gml:location>
</location-info>
```

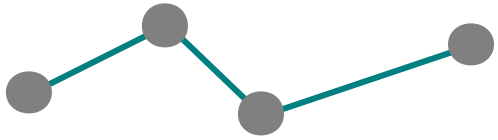
Typical GML Geometries

- Point:

```
<Point gid="P1" srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
  <coord><X>56.1</X><Y>0.45</Y></coord>
</Point>
```

- LineString:

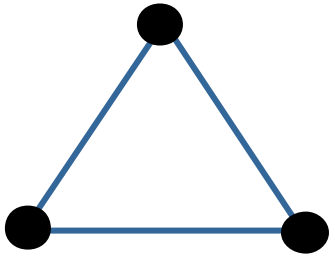
```
<LineString srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
  <coordinates>100.0,100.0 230.0,80.0 350.0,130.0 </coordinates>
</LineString>
```



- Linear Ring:

```
<LinearRing srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
  <coordinates>
    100.0,100.0
    230.0,80.0
    350.0,130.0
    100.0,100.0
  </coordinates>
</LinearRing>
```

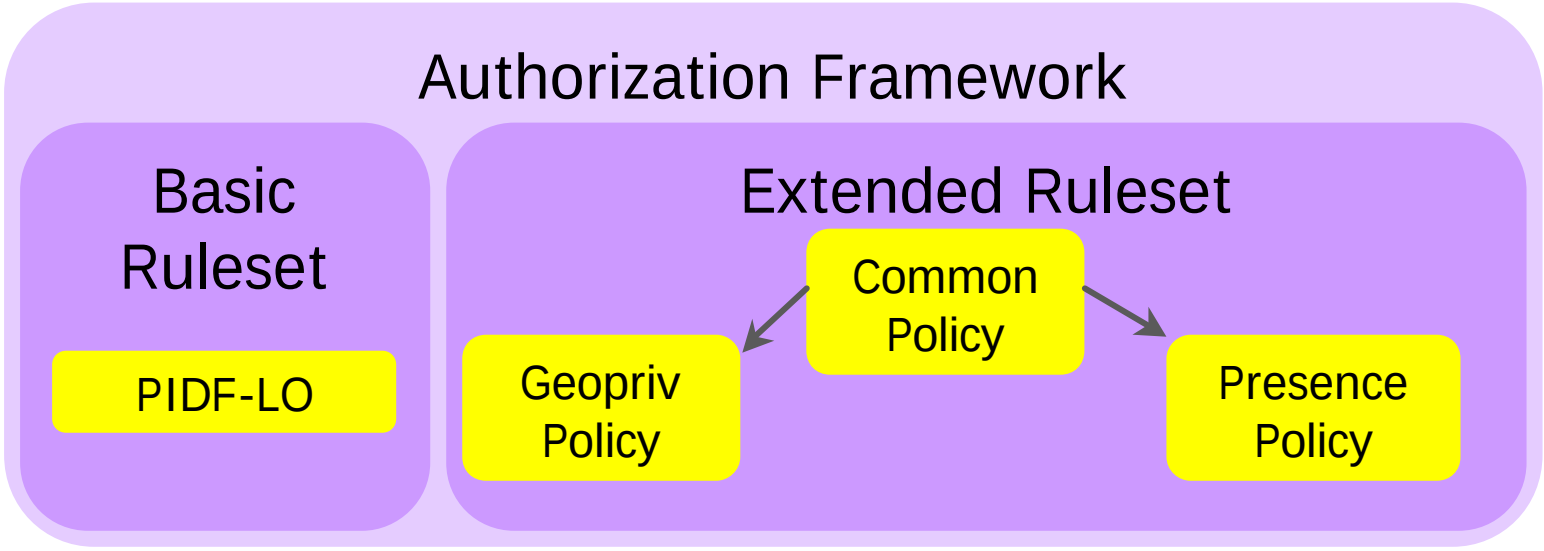
Both points must be equal



Civic Location Example

```
<gp:location-info>
  <cl:civilAddress>
    <cl:country>US</cl:country>
    <cl:A1>New York</cl:A1>
    <cl:A3>New York</cl:A3>
    <cl:A6>Broadway</cl:A6>
    <cl:HNO>123</cl:HNO>
    <cl:LOC>Suite 75</cl:LOC>
    <cl:PC>10027-0401</cl:PC>
  </cl:civilAddress>
</gp:location-info>
```

Authorization for Presence and Location Information



• Authorization language based on XML designed with designe d with simplicity and privacy preserving properties in mind.

Basic Ruleset

- Attached to PIDF-LO and MUST always be present:
  - Retention expires (how long can you keep the object)
  - Policy for retransmission of location information
  - Reference to an external ruleset
  - A “note well” of free text, human readable privacy policy
- Example:

```
<gp:usage-rules>
  <gp:retransmission-allowed>
      yes
  </gp:retransmission-allowed>
  <gp:retention-expiry>
      2003-06-23T04:57:29Z
  </gp:retention-expiry>
  <note-well>
      Text for the privacy statement goes in there.
  </note-well>
</gp:usage-rules>
```

Extended Ruleset (1/2)

- Full authorization policy ruleset either
  - attached to the PIDF-LO document or
  - referenced within the PIDF-LO document
- Rules can be uploaded to a third party entity (e.g., Location Server)
- Special conflict resolution mechanism to limit problems in a distributed environment
  - Permit only
  - Additive permissions
  - Upgradeable
  - Versioning support
  - No false assurance

Extended Ruleset (2/2)

- Rule consists of:
  - conditions part
  - actions parts
  - transformations part
- Common policy document is extended by
  - Presence specific document
  - Geopriv specific document

Rule Example (1/2)

```
<cp:rule id="AA56i09">
  <cp:conditions>
    <cp:identity>
      <cp:id>jack@example.com</cp:id>
    </cp:identity>
   <cp:validity>
     <cp:from>2004-11-01T00:00:00+01:00</cp:from>
     <cp:to>2005-11-01T00:00:00+01:00</cp:to>
   </cp:validity>
   <gp:civic-loc-condition>
     <country>DE</country>
     <A1>Bavaria</A1>
     <A3>Munich</A3>
     <A4>Perlach</A4>
     <A6>Otto-Hahn-Ring</A6>
     <HNO>6</HNO>
   </gp:civic-loc-condition>
 </cp:conditions>
```

Rule Example (2/2)

```
 <cp:actions></cp:actions>

  <cp:transformations>
     <gp:distribution-transformation>
       true
     </gp:distribution-transformation>
     <gp:keep-rules-transformation>
       true
     </gp:keep-rules-transformation>
     <gp:civic-loc-transformation>full
           </gp:civic-loc-transformation>
     <gp:geospatial-loc-transformation>
       <gp:lat-resolution>0.00001</gp:lat-resolution>
       <gp:lon-resolution>0.00001</gp:lon-resolution>
     </gp:geospatial-loc-transformation>
   </cp:transformations>

</cp:rule>
```

References

- Geopriv Working Group
  - http://www.ietf.org/html.charters/geopriv-charter.html
- Emergency Context Resolution with Internet Technologies (Ecrit) Working Group
  - http://www.ietf.org/html.charters/ecrit-charter.html
  - http://www.ietf-ecrit.org
- GMLv3
  - http://www.opengis.org
  - http://schemas.opengis.net/gml/3.0.0/base/