SIP for Presence and Instant Messaging

A Role for Presence in “VoIP”

Awareness of other users: availability, location, ...

- To perform existing functions
  - User location, call routing, follow-me, ...

- To improve existing services
  - Call completion ratio
  - Indicate availability

- To enable new services
  - Presence per se: Simplify meeting people
  - Messaging per se: “SMS”
  - Presence and Messaging as basis for other applications
  - Location-based services
  - New inter-personal communication paradigms

- To provide another differentiator from traditional telephony
SIP: Personal Presence and Instant Messaging

- "Buddy Lists + Chat"
- Idea: re-use SIP infrastructure
  - Maintain user locations
  - Route messages
  - Contact users
- SIP Event package for "presence"
  - SUBSCRIBE / NOTIFY fit well
  - Define presence formats
- Define a new method for Instant Messaging
  - MESSAGE
  - MSRP for messaging sessions
  - Define basic message content format (text/plain)

IMPP Presence Model
SIP Entities for Presence (1)

Example: SIP for Presence

SUBSCRIBE
Event: presence
Expires: 3600
Accept: text/plain

200 OK
Event: presence
Expires: 1800

NOTIFY
Event: presence
Expires: 1759
Subscr-State: active

200 OK

SUBSCRIBE
Event: presence
Expires: 3600
Accept: text/plain

202 Accepted
Event: presence

NOTIFY
Event: presence
Expires: 1759
Subscr-State: active

200 OK
SIP Presence Notification (PIDF)

```xml
<presence ... entity="pres:jo@tzi.org">
  <tuple id="mobile-im">
    <status>
      <basic>open</basic>
    </status>
    <contact priority="0.8">im:jo@sms-gw.tzi.org</contact>
    <note xml:lang="en">Don't Disturb Please!</note>
    <note xml:lang="fr">Ne dérangez pas, s'il vous plaît</note>
    <timestamp>2006-02-23T10:49:29Z</timestamp>
  </tuple>
  <tuple id="interactive-mm">
    <status>
      <basic>closed</basic>
    </status>
    <contact priority="1.0">sip:jo@tzi.org</contact>
  </tuple>
  <note>I am in Paris this week</note>
</presence>
```

Rich Presence Information Data Format (RPID)

- Introduces additional (more descriptive) elements
  - Ideally to be derived automatically from user activity
  - Describe a tuple, a person, or a device
  - May be grouped according to a class element
- Extension for a person
  - activities away, appointment, busy, travel, steering, vacation, ...
  - mood afraid, angry, annoyed, distracted, happy, impressed, thirsty, ...
  - place-type aircraft, bus, car, home, hotel, office, outdoors, public, quiet, ...
  - sphere work, home
  - status-icon convey a URI pointing to an image
  - timezone
- Extensions for tuple, device
  - user-input active, idle (idle since)
- Extensions for a tuple
  - privacy, relationship, service-type, status-icon
Further Presence Format Extensions

- **User Agent capabilities**
  - Add further hints to a contact beyond contact means (protocol) and address
  - Set of attributes also available from the caller preferences and callee capabilities framework

- **Contact information**
  - Display name and business card
  - Pointer to home page
  - Sound + icon

- **Timed presence information**
  - Specify information about time periods (past, future)
  - E.g., as derived from a calendar entry

Learning Presence State

- **Co-location**
  - Presence agent (PA) co-located with the presence user agent (PUA)

- **REGISTER**
  - SIP UAs (de)registering for a certain AoR contribute presence state
  - Presence server may derive information from co-location w/ registrar
  - Alternative: registration event package
    - A presence server may subscribe to an AoR at a registrar
    - Registrar provides change notifications: application/reginfo+xml
    - Per AoR per contact: identification, registration state, last event, params

- **Uploading presence documents**
  - Explicit provisioning from a PUA
SIP Entities for Presence (2)

EPA: Event Publication Agent  
ESC: Event State Compositor

SUBSCRIBE / NOTIFY, PUBLISH  
e.g. REGISTER

Example: PUBLISHing State

<table>
<thead>
<tr>
<th>EPA</th>
<th>ESC</th>
</tr>
</thead>
</table>
| **Install State** | **PUBLISH**  
Event: presence  
Expires: 3600  
Content-Length: ... |
| 200 OK  
Expires: 1800  
SIP-ETag: 116xyz42 |

<table>
<thead>
<tr>
<th>EPA</th>
<th>ESC</th>
</tr>
</thead>
</table>
| **Refresh State** | **PUBLISH**  
Event: presence  
Expires: 1800  
SIP-If-Match: 116xyz42  
Content-Length: 0 |
| 200 OK  
Expires: 1800  
SIP-ETag: 891abc4190 |

<table>
<thead>
<tr>
<th>EPA</th>
<th>ESC</th>
</tr>
</thead>
</table>
| **Modify State** | **PUBLISH**  
Event: presence  
Expires: 3600  
SIP-If-Match: 891abc4190  
Content-Length: ... |
| 200 OK  
Expires: 1800  
SIP-ETag: 891abc4190 |

<table>
<thead>
<tr>
<th>EPA</th>
<th>ESC</th>
</tr>
</thead>
</table>
| **Delete State** | **PUBLISH**  
Event: presence  
Expires: 0  
SIP-If-Match: 336hoh1875  
Content-Length: 0 |
| 200 OK  
Expires: 0 |

© 2007 Jörg Ott
Excursion

Important Issue:
Privacy of Presence Information

GEOPRIV: Focus on geographic location data

Specific Threats to a Location Based System

- Who is in control?
  - Smart devices: authorized access only
  - Substrates: external control
  - Third-party services: users cannot control access!
    (e.g. cell phone company)

- Tracking applications
  - The good: friend-finder, emergency services
  - The ugly: your employer's time tracking system
  - The bad: profiling for commercial reasons (health insurance, ...), and criminal intent (e.g. surveillance)

- SPLOC (Spam over LBS)
  - Unsolicited business advertisements

- Attacks
  - Eavesdropping, forging identity, replay, DoS, ...
Aggregation of Presence & Location Information

EPA: Event Publication Agent
ESC: Event State Compositor

SUBSCRIBE / NOTIFY, PUBLISH
e.g. REGISTER

Retrieving Location Info in GEOPRIV

Publish location information on behalf of a specific target

Holds filtering rules on behalf of a specific target ("rule maker")
GEOPRIV: No Geo-Information without Privacy

- Location information is sensitive data in almost any application
  - Tracking movements, profile creation, relate with other persons' locations …
  - Equipment in use (apparently)
  - Emergency situations

- Problem: many applications rely on sensitive information
  (e.g., emergency handling, follow-me services)

- GEOPRIV
  - Location model (protocol-agnostic)
    - PIDF extension (PIDF-LO)
    - Re-use OpenGIS GML syntax
  - Rules, Policies
  - Leverage usage in existing presence protocols (esp. SIP)

GEOPRIV: Components

- Location information
  - Raw (pre-configuration databases, generated by sensors, …)
  - Computed (from multiple sensors, personal presence status, …)

- Data model (Location Objects)
  - Location information
    - Civil addresses, geo-coordinates, place type (e.g., at SIP tutorial)
  - Owner (identity)
  - Privacy rules

- Policies
  - Declaring presence processing rules formally
  - Identity of users
  - Concept of filtering and transformation
  - Designed for simplicity to ease conflict resolution
PIDF-LO Example Document

```xml
<pres:entity="pres:dku@tzi.org" xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
<tuple id="xyz">
<status>
<gp:geopriv>
<gp:location-info>
<gml:Point>
<gml:coordinates> ... </gml:coordinates>
</gml:Point>
</gp:location-info>
<gp:usage-rules>
<gp:retransmission-allowed>no</gp:retransmission-allowed>
<gp:retention-expiry>2006-01-20T10:00:00Z</gp:retention-expiry>
<gp:ruleset-reference>
https://example.org/rset.xml
</gp:ruleset-reference>
</gp:usage-rules>
</gp:geopriv>
</status>
</tuple>
</presence>
```

Civic Locations in PIDF-LO

```xml
<pres ...
  ... ...
<gp:location-info>
  <cl:civicAddress>
    <cl:country>FI</cl:country>
    <cl:A1>Espoo</cl:A1>
    <cl:A3>Espoo</cl:A3>
    <cl:A6>Otakaari</cl:A6>
    <cl:HNO>5A</cl:HNO>
    <cl:LOC>SE 324</cl:LOC>
    <cl:FLR>3</cl:FLR>
    <cl:NAM>Laboratory</cl:NAM>
  </cl:civicAddress>
</gp:location-info>
```
GEOPRIV Policies

- Framework for authorization policies
  - General framework
  - Adaptation to LBS applications

- General idea
  - Control distribution of and access to personal information by explicit rules
  - Leverage GEOPRIV framework

![Diagram showing GEOPRIV policy rules]

GEOPRIV Policy Rules

- Conditions
  - Expressions that evaluate to TRUE or FALSE
  - All conditions must evaluate to TRUE for a rule to become active
  - Some sample conditions:
    - Matching identities (URI-based)
    - Matching spheres
      (matching abstract presence state: “at home”, “at work” etc.)
    - Validity: specify timeframe, when this rule is valid

- Actions and transformations (“permissions”)
  - Specify how to handle a request
  - Formulate positive permissions
    (what the system is allowed to do)
Sample Condition (1)

Condition Processing Semantics

Policy Document

Rule
Conditions
Actions
Transformations

<ruleset xmlns="urn:ietf:params:xml:ns:common-policy">
  <rule id="f3g44r1">
    <conditions>
      <sphere value="home"/>
      <identity>
        <one id="alice@example.com"/>
        <one id="+1-212-555-1234" scheme="tel"/>
        <one id="bob@example.net" scheme="sip mailto xmpp"/>
      </identity>
    </conditions>
    <actions/>
    <transformations/>
  </rule>
</ruleset>
Transformation Rules

- Distribution transformation
  - Specify whether a LO may be distributed

- Retention transformation
  - Specify for how long the LS may keep the LO

- Keep rules transformation
  - Specify whether the LS may keep all authorization policy rules in the LO when delivering the LO to recipients

- Civic location transformation
  - Restrict the level of civic location information

- Geospatial location transformation
  - Restrict resolution of geospatial information

```
<gp:distribution-transformation> true
</gp:distribution-transformation>

<gp:retention-transformation> 3600
</gp:retention-transformation>

<gp:keep-rules-transformation> false
</gp:keep-rules-transformation>

<gp:civic-loc-transformation> city
</gp:civic-loc-transformation>

<gp:geospatial-loc-transformation>
  <gp:lat-resolution>0.2</gp:lat-resolution>
  <gp:lon-resolution>0.1</gp:lon-resolution>
</gp:geospatial-loc-transformation>
```

Sample Policy

```
<cp:ruleset
  xmlns:cp="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <cp:rule id="AA56i09">
    <cp:conditions>
      <cp:validity>
        <cp:from>2004-11-01T00:00:00+01:00</cp:from>
        <cp:until>2005-11-01T00:00:00+01:00</cp:until>
      </cp:validity>
      <gp:civic-loc-condition>
        <gp:country>DE</gp:country>
        <gp:A1>Bavaria</gp:A1>
        <gp:A3>Munich</gp:A3>
        <gp:A4>Perlach</gp:A4>
        <gp:HNO>6</gp:HNO>
      </gp:civic-loc-condition>
    </cp:conditions>
    <cp:actions/>
    <gp: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>
    </gp:transformations>
  </cp:rule>
</cp:ruleset>
```

Matching Location Filter
Sample Policy

```xml
<cp:ruleset
   xmlns:cp="urn:ietf:params:xml:ns:common-policy"
   xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <cp:rule id="AA56i09">
     <cp:conditions>
       <cp:validity>
         <cp:from>2004-11-01T00:00:00+01:00</cp:from>
         <cp:until>2005-11-01T00:00:00+01:00</cp:until>
       </cp:validity>
       <gp:civic-loc-condition>
         <gp:country>DE</gp:country>
         <gp:A1>Bavaria</gp:A1>
         <gp:A3>Munich</gp:A3>
         <gp:A4>Perlach</gp:A4>
         <gp:HNO>6</gp:HNO>
       </gp:civic-loc-condition>
     </cp:conditions>
     <cp:actions/>
   </cp:rule>
</cp:ruleset>
```

Transforming resolution of location info

GEOPRIV Summary

- **Objective:** interoperability and assurance of LBS security and privacy goals
- **Conceptual model for dealing with security issues in LBS**
  - Location Generator, Rule Maker, Location Server, Rule Set, Subscriber
  - Conceptually compatible with personal presence architecture (IMPP)
- **Data model for Location Objects**
  - Representing location information
  - Usage rules
  - Recommendations for secure transport (S/MIME)
- **Policies**
  - Control distribution of and access to personal information by explicit rules
  - Allows tailoring "revealed" presence / location information to the recipient
- **NOT GEOPRIV:**
  - Transport protocols for location objects, rules
  - For SIP-based presence, S/MIME can be applied

For exclusive use with TKK Netlab course S-38.3152 Networked Multimedia Protocols and Services
End of Excursion:

Back to SIP for Presence & IM

SIP for Instant Messaging (IM)

- UAs may send and receive messages
  - Similar model to Presence
- Receivers indicate support when registering
  Contact: sip:jo@tzi.org;methods="MESSAGE"
- Senders just send
  - Use sip: or im: URLs
  - Congestion control is important!
- For longer “chat sessions”
  - Create a persistent IM session
    - Just another media type
  - May not be able use TCP or TLS
  - Use MSRP-based session instead
Presence & IM Security

- Authentication of (Subscription) Requests
  - Standard SIP mechanisms: 401/407 responses

- Authorization: Users must stay in control of subscriptions
  - May subscribe to their own subscription state ("watcher info")
  - Receive notifications for every subscription attempt
  - May authorize each subscription
  - May retrieve lists of and cancel existing subscriptions
  - Control distribution of state (e.g. GEOPRIV)

- Authentication of Instant Messages
  - May include contents to be automatically acted upon
  - User / system needs to validate originator

- Meta-issue: end-to-end authentication

Issue: Congestion Control

- PUBLISH, NOTIFY: Throttling of events
  - Keep event rate under control: one PUBLISH / NOTIFY per RTT
  - To be defined on a per-package basis

- MESSAGE: Message frequency
  - Only one outstanding message: one MESSAGE per RTT
    - But: messages are stand-alone; no dialog context to check against

- MESSAGE: Large messages
  - UDP is an acceptable transport for SIP: no congestion control
  - Even if TCP is used: impacts SIP infrastructure components

- Approach: Message Session Relay Protocol (MSRP)
  - Move message sessions off the SIP infrastructure
Message Session Relay Protocol (MSRP)

- Protocol for Messaging Sessions
  - Uses TCP or another reliable and congestion controlled transport
  - Message encoding similar to SIP and HTTP
- Just another media protocol
  - Messaging sessions require explicit setup and teardown
    - E.g., SIP dialogs (INVITE, BYE)
  - SDP to describe sessions (m=message)
  - Uses SDP Offer/Answer to convey parameters
    - Exchange dynamic transport addresses for communications (MSRP URLs)
    - Negotiate supported message formats
  - SEND method to convey messages
    - May request confirmation from the remote side (on success and/or failure)
    - Support for chunking of large messages (2 KB chunks)
  - REPORT method to provide confirmations
- Two modes of operation
  - Direct communication between peers (simple case)
  - Communication via relays (NATs, firewalls, policy)
Communication via a Relay

Choose URL

AUTH

200 OK

Choose URL

SIP INVITE

200 OK

ACK

SEND

200 OK

REPORT

SIP BYE

200 OK

MSRP id314 AUTH
To-Path: msrps://a.org:8888/42
From-Path: msrps://a.org:8888/42
Expires: 600
Authorization: ...
-------id314$

Choose URL

200 OK

MSRP id314 200 OK
Expires: 300
Use-Path: msrps://r.org:9999/35
-------id314$

SEND

200 OK

REPORT

MSRP e2718 SEND
To-Path: msrps://r.org:9999/35
From-Path: msrps://a.org:8888/42
msrp://b.org:7777/bb;tcp
a=

MSRP rrr33 SEND
To-Path: msrps://b.org:7777/bb
From-Path: msrps://r.org:9999/35
msrp://a.org:8888/42