Preserving Privacy in Environments with Location-Based Applications

Nathan Sulinski

Introduction

“The increase in location-based applications makes protecting personal location information a major challenge. Addressing this challenge requires a mechanism that lets users automate control of their location information, thereby minimizing the extent to which the system intrudes on their lives.”

--Ginger Myles, Adrian Friday, Nigel Davies
Introduction

• Initial Problem
  – Location based applications are on the rise so the privacy concerns associated with them must be addressed

• Solution Requirements
  – Minimize intrusiveness on user
  – Minimize demands on user

• Related Work
  – Geopriv
    • IETF initiative (November 2002)
    • Use of location objects to “encapsulate” location data & privacy requirements
    • Location Objects support tamper-resistant measures, like digital signatures
  – P3P & Appel
    • Website support to announce privacy practices
    • Automation of user decisions (reject/accept)
    • P3P described user agent architecture
    • Appel is a language used to describe privacy policies
  – pawS
    • Beacons announce policy of each service
    • “Privacy Proxies” check policies against user preferences
Introduction

• LocServ Approach
  – “...middleware service that lies between location-based applications and location-tracking technologies.”
  – Enables application development independent of underlying location technology

Details

• System Constraints
  – Organization: Restrict location info to specific organizations
  – Service: Acceptance of certain information from new entities
  – Time: Additional parameter to govern organizational tracking
  – Location: Tracking allowed based on location
  – Request Type: Restriction on type of request to be accepted
  – Context:
    – Legislative: Flexibility to comply with legislation
    – Interaction Minimization: Minimize user interaction
• Development Goals
  – Minimal user involvement
    • Privacy policies handle bulk of information requests
  – Privacy by default
    • “Elect to share” vs. “Elect to block”

• System Architecture
Details

• Applications

• Queries (Information Requests)
  – Location (location details for user)
  – Enumeration (lists of users at specific location)
  – Asynchronous (event information)

Details

• Supporting Technology
  – GPS
  – Active Bat

• Validators
  – User’s privacy preferences
  – Registered with each Location Server
• **Privacy Policies (enhanced P3P)**
  
  **Entity**
  - **Original**: Mechanism for describing business & contact information for organization.
  - **Enhanced**: Type & Cert fields

  **Purpose**
  - **Original**: Orientation towards e-commerce & web interactions
  - **Enhanced**: Broadened with new set of classifications

  **Request Initiation**
  - **Original**: n/a
  - **Enhanced**: Solicited vs. Unsolicited

---

**Sample Policy Table**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Rule 1</th>
<th>Rule 2</th>
<th>Rule 3</th>
<th>Rule 4</th>
<th>Rule 5</th>
<th>Rule 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company type</td>
<td>MyEmployee.com</td>
<td>MyEmployee.com</td>
<td>*</td>
<td>Taxi.com</td>
<td>*</td>
<td>FindAFriend.com</td>
</tr>
<tr>
<td>Organization type</td>
<td>Commercial</td>
<td>Commercial</td>
<td>*</td>
<td>Commercial</td>
<td>Nonprofit, government</td>
<td>Commercial</td>
</tr>
<tr>
<td>Certification</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Request type</td>
<td>*</td>
<td>*</td>
<td>Enumerate</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Purpose</td>
<td>Safety, information, service delivery, statistics, security, other</td>
<td>Safety, information, service delivery, statistics, security, other</td>
<td>Safety, information, service delivery, security</td>
<td>Service delivery</td>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Retention</td>
<td>*</td>
<td>Stated purpose</td>
<td>Stated purpose</td>
<td>Stated purpose</td>
<td>Stated purpose</td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td>Ours</td>
<td>Ours</td>
<td>Ours</td>
<td>Ours</td>
<td>Ours</td>
<td></td>
</tr>
<tr>
<td>Initiator</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Yes</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Validators</td>
<td>None</td>
<td>References a validator that can check Sally’s calendar</td>
<td>References a verification service that checks ownership of physical locations</td>
<td>None</td>
<td>None</td>
<td>*</td>
</tr>
<tr>
<td>Location</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Time</td>
<td>M-F, 9 a.m. - 5 p.m.</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Anonymity</td>
<td>None</td>
<td>None</td>
<td>Returns a new pseudo-identifier</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

* Day
Conclusion

• Currently being implemented in conjunction with ongoing research to create “deployable pervasive systems”

• Lancaster Guide tourist system
  – Allow users to create their own Guide content

• Pervasive healthcare based on mobile devices
  – Reassure patients of the privacy of their data