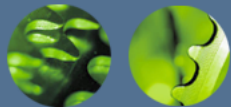




Preserving Privacy in Environments with Location-Based Applications



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



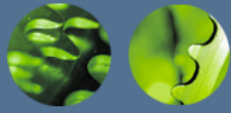
Introduction

- 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



Introduction

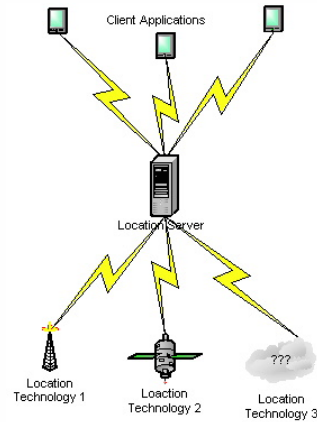
- Related Work
 - Geopriv
 - IETF initiative (November 2002)
 - Use of location objects to “encapsulate” location data & privacy requirements
 - Location Objects support tamper-resistant measures, like digital signatures
 - P3P & Appel
 - Website support to announce privacy practices
 - Automation of 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



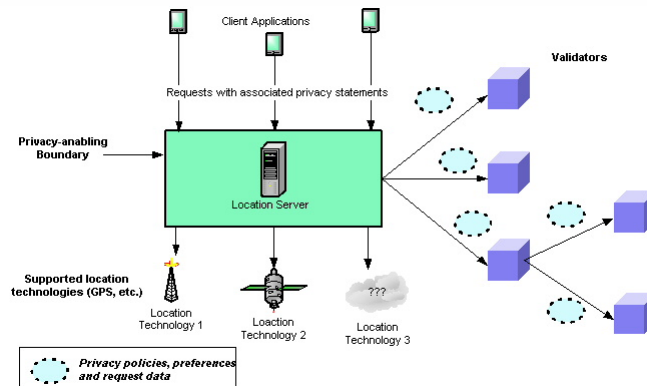
Details

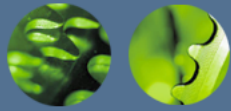
- Development Goals
 - Minimal user involvement
 - Privacy policies handle bulk of information requests
 - Privacy by default
 - “Elect to share” vs. “Elect to block”



Details

- 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



Details

- **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



Details

- **Sample Policy Table**

Parameter	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6
Company	MyEmployer.com	MyEmployer.com	*	Taxi.com	*	FindaFriend.com
Organization type	Commercial	Commercial	*	Commercial	Nonprofit, government	Commercial
Certification	*	*	*	*	*	*
Request type	*	*	Enumerate	*	Location, asynchronous	Colocation
Purpose	Safety, information, service delivery, statistics, security, other	Safety, information, service delivery, statistics, security, other	Safety, information, service delivery, security	Service delivery	Information	Service delivery
Retention	*	*	Stated purpose	Stated purpose	Stated purpose	Stated purpose
Distribution	Ours	Ours	Ours	Ours	Ours	Ours
Initiated	*	*	*	Yes	*	*
Validators	None	References a validator that can check Sally's calendar	References a verification service that checks ownership of physical locations	None	None	*
Location	*	*	*	*	*	*
Time	M-F, 9 a.m.–5 p.m.	*	*	*	*	*
Anonymity	None	None	Returns a new pseudo-identifier	None	None	None

* Any



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