

Privacy in Context-aware Mobile Business Applications

Emin İslam Tatlı
tatli@th.informatik.uni-mannheim.de

Department of Computer Science, University of Mannheim

IADIS International Conference E-Commerce
Barcelona-Spain, 9-11 December 2006

Outline

- 1 Motivation
- 2 Privacy Risks/Legacy Aspects
- 3 Existing Solutions
- 4 Shortcomings
- 5 Work Done/Future

Mobile Business Research Group

- Joint project of 7 research groups at the University of Mannheim-Germany
- Aim \Rightarrow A generic framework for context-aware and especially location-aware mobile business applications
- Web: www.m-business.uni-mannheim.de

Context-aware Mobile Business Applications

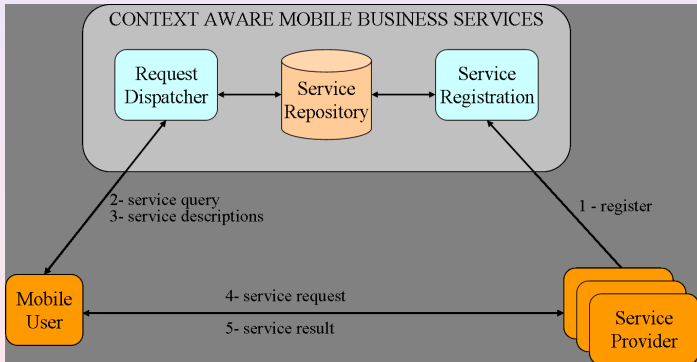
Context

- any information that can be used to characterize the situation of an entity
- Examples: location, time, identity, level of mobility, morale status, etc.

Application Examples

locating kids, people in emergency, objects like fleet management, finding the nearest pizza shop, navigation services, location-based games, etc.

SOA Architectures



Privacy

- Users require full control over their personal data.
- Privacy is a big barrier against the acceptance of m-business applications.
- The European Parliament and the Council of the European Union have published the EU Directive 2002/58/EC and 95/46/EC that are concerned with the processing of personal data and the protection of privacy in the electronic communication sector.
- But **NO COMPLETE** privacy solution exists for the user privacy in context-aware m-business applications.

The Aim

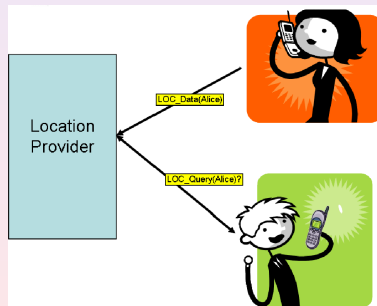
For the user-centric privacy management in context-aware mobile business applications:

- Design the architecture with the consideration of user's all privacy aspects
- Extend the privacy policy and preferences languages related to the new privacy aspects
- Develop new methods for the enforcement of privacy policies

Friend Finder

Friend Finder

a service to find out a particular person's dynamic location



Privacy Risks I

Location Reveal

- Other users can try to reveal the location of a particular user without having any permission.
- The location provider can target a single user, analyze his location data to reveal where he stays, follow his activities or even guess the place at which he would be in the future.

Privacy Risks II

User Preferences/Profiles

- UAProf [6] data can expose device capabilities and user preferences. The attackers can find out costly devices to target.
- Profiling the devices with big font sizes and displays with image-disabled feature can threaten the privacy of the device owner with a weak visual acuity.

Privacy Risks III

User Relations

- The location provider can find out who stay in the same place or travel through the same direction at the same time and reveal the relations among the users.
- The location provider can collect friend-search queries to reveal the relations among the users.

Privacy Risks IV

Dynamic Pricing

- The location provider analyzes how frequently the users retrieve the service and apply dynamic pricing which means that different users pay different amounts for the same delivered service based on their activeness.
- UAProf profiles can also be targeted for dynamic pricing.

EU-Directive 2002/58/EC I

Security - Art. 4 EU-Directive

The **service providers** must take appropriate measures to **safeguard** the security of **their services**. If a particular security risk exists, the users should be informed of these risks and any likely costs involved with providing the possible remedies.

Confidentiality - Art. 5,6 EU-Directive

Member States shall **ensure the confidentiality of communications** and the related traffic data through national legislation. They shall ensure also that the access and process of the data is allowed only if the user concerned is clearly informed and gives his consent.

EU-Directive 2002/58/EC II

Data Storage - Art. 6 EU-Directive

The user data can be **stored** and **processed** by service providers for the **duration necessary for the services** and billing purposes.

Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done. But the data stored must be erased or made anonymous when it is no longer needed for the purpose of the transmission. In addition, the users should be always in the position of withdrawing their consent to store and process their data.

EU-Directive 2002/58/EC III

Location Data Definition - Art. 2 EU-Directive

Location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

EU-Directive 2002/58/EC IV

Location Data - Art. 9 EU-Directive

Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made **anonymous**, or **with the consent of the users** or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

P3P (Platform for Privacy Preferences)

- P3P [4] is a recommendation of World Wide Web Consortium (W3C) at April 16, 2002.
- “P3P enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents” .
- It functions as follows:
 - ① Servers express their privacy policies in P3P format.
 - ② Users specify their privacy preferences in Appel format (A P3P Preference Exchange Language) [5].
 - ③ User agents retrieve server policies and compare with the user preferences to automate decision-making.
- P3P policy contains the tags: ENTITY, ACCESS, PURPOSE, RECEIPT, RETENTION, DATA, DISPUTES

Sample Policy

Yahoo Privacy Policy in P3P:

http://privacy.yahoo.com/us/w3c/p3p_us.xml

Other Works I

EPAL

- Enterprise Privacy Authorization Language (IBM) [7]
- EPAL is an XML-based privacy policy specification language for organizations to formalize internal privacy policies.
- EPAL policies can be enforced and therefore EPAL is complementary to P3P.

Other Works II

pawS

- pawS = privacy awareness system for ubiquitous environment [3]
- ubiquitous devices (i.e. webcam, printer, room light controller, etc.) specify their P3P privacy policies and user agents running on user devices compare the user preferences with the received policies.

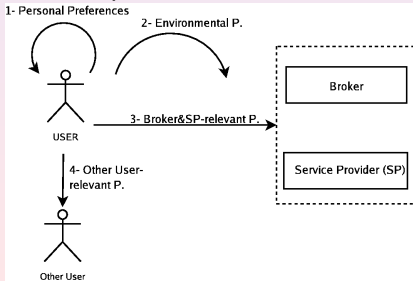
Other Works III

WASP

- focuses on context-aware mobile business applications.
- adds support of date, time, day of week and location entities within the preference language Appel.
- But...
 - only limited context data is supported.
 - no real integration or user experiments were done.

Shortcomings of P3P/Appel

- P3P does not support negotiation
- No encryption or anonymity preferences are possible in P3P/Appel
- P3P's privacy perspective is only related to service providers. Other aspects are not considered:



Completed Work I

Privacy Concerns of Friend Finder

Privacy risks of Friend Finder application, the legacy aspects regarding personal data management and shortcomings of P3P are explained in this paper.

Context Data Model for Privacy

- Schmidt et al. (2000): “There is more Context than Location” -> Human Factors and Physical Environment
- Tatli (2006): “Context Data Model for Privacy” [8]
 - ① Protected Context: User Identity, User Profile, Physical Conditions, Location, Time
 - ② Evaluated Context: User Morale, Infrastructure, Social Environment, User Tasks

Completed Work II

Context Privacy with Context Evaluation

- The privacy architecture for context-aware applications is illustrated.
- Privacy policies based on context2context relations are explained:
 - protected2protected constraint:
 - “Reveal my location only to people who are at a certain location and have a certain identity”
 - “Hide my schedule at certain dates (e.g. at the weekends)”
 - protected2evaluated constraint:
 - “Reveal my blurred location for indoor application, i.e. communication infrastructure is WLAN”
 - “Do not send my profile, identity, etc. if my status is set away”

Future Work

- 1 Formal specification of the context data model
- 2 Extending P3P/Appel based on the new formal model
- 3 Integration of the enhanced privacy policy and preferences within the m-business framework
- 4 Implementation of certain methods for policy enforcement
- 5 Usability experimentations





Conclusion

- Privacy is a big barrier against the business success in context-aware mobile business applications.
- Existing solutions based on P3P do not cover all privacy aspects.
- Privacy languages expressing different aspects which stem from the user himself, the environment, the service providers and other users should be designed.

References I

-  Bauer, Reichardt, Schüle (2006): Was will der mobile Nutzer? Forschungsergebnisse zu den Anforderungen von Nutzern an kontextsensitive Dienste (in German), University of Mannheim.
-  M. Zuidweg et al., Using P3P in a web services-based context-aware application platform, <http://www.w3.org/2003/p3p-ws/pp/utwente.pdf>.
-  Marc Langheinrich (2002), A Privacy Awareness System for Ubiquitous Computing Environments, UbiComp '02: Proceedings of the 4th international conference on Ubiquitous Computing.
-  Platform for Privacy Preferences(P3P) Project, <http://www.w3c.org/P3P>, World Wide Web Consortium.

References II

-  A P3P Preference Exchange Language (APPEL), <http://www.w3.org/TR/P3P-preferences>, World Wide Web Consortium.
-  UAProf (User Agent Profile) Specification, <http://www.openmobilealliance.org/tech/affiliates/wap/wap-248-uaprof-20011020-a.pdf>.
-  P. Ashley and S. Hada and C. Powers and M. Schunter (2003), Enterprise Privacy Authorization Language (EPAL), IBM Research.
-  Emin Islam Tati, Context Data Model for Privacy, PRIME Standardization Workshop, IBM Zürich Research Center, 6-7 July 2006.