

Context Data Model for Privacy

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

Department of Computer Science, University of Mannheim

PRIME Standardization Workshop, 06-07 July 2006

Outline

- 1 Motivation
 - Mobile Business Research Group
 - Context-aware applications
- 2 Context Data Model
- 3 Context Data Model for Privacy
 - Privacy Concerns
 - Privacy Data Model
 - Context Interaction
- 4 Conclusion
 - Future Work

Mobile Business Research Group

- Joint project of 7 research groups at the University of Mannheim (since September 2004)
- Aim ⇒ A generic framework for context-aware and especially location-aware mobile business applications
- Web: www.m-business.uni-mannheim.de
- Security
 - Secure implementations of security protocols (LaCoDA compiler)
 - Dynamic mobile anonymity with mixing
 - Integration of efficient cryptography libraries within Java mobile platform
 - Context privacy
 - Security and usability

Context

- Context-aware applications consider context when providing their services.

Context

Any Information that can be used to characterize the situation of an entity

Dynamic Context

Information used to deliver a service which is not explicitly input by the service requester, but becomes visible during the course of the service delivery

Context-aware Applications

Bauer, Reichardt, Schüle (2006): "Was will der mobile Nutzer? Forschungsergebnisse zu den Anforderungen von Nutzern an kontextsensitive Dienste", Universität Mannheim.

Context-aware Applications

- 1 Tracking Services
 - a) Person tracking
 - b) Object tracking
- 2 Navigation Service
 - a) General navigation service
 - b) Special navigation service

Context-aware Applications (cont.)

Context-aware Applications

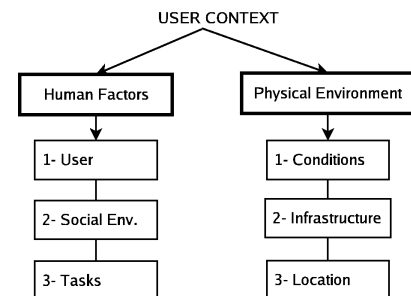
- 3 Information Services
 - a) General information services
 - b) Interactive information services
- 4 Communication Services
 - a) B2C communication services
 - b) B2B communication services
- 5 Entertainment Services
- 6 Transaction Services

Context Privacy

- Context privacy requires that a user is in the position of controlling his/her context.
- But, what is a context of a user beyond location?
 - Context Data Model is needed.
- What are the privacy concerns in the data model?
 - Privacy-aware context data model is required.
- What is the privacy relation among the context in the privacy-aware data model?
 - Context2Context privacy relation should be explicitly specified.

Context Data Model

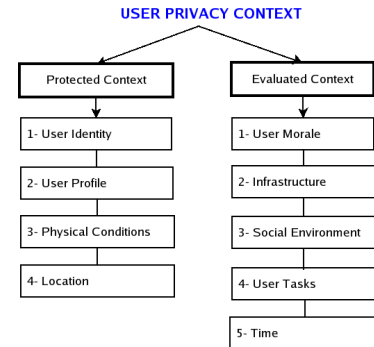
Schmidt, Beigl, Gellersen (2000): "There is more to Context than Location"



Privacy Concerns

- 1 shared context should be specified explicitly as **protected** context
- 2 a context can **affect** another context's privacy sensitivity
- 3 context **blurring**/lying can enhance privacy

Context Data Model for Privacy



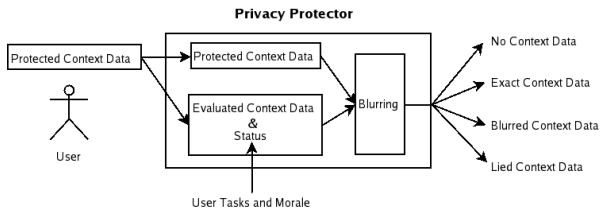
Protected Context

Protected Context	
1. User Identity	personal data like name, address, phone number, birth date, credit card number, etc.
2. User Profile	user interests, habits, schedule, etc.
3. Physical Conditions	the context around the physical surroundings like temperature, light, pressure, etc.
4. Location	the absolute or relative location of a user

Evaluated Context

Evaluated Context	
5. User Morale	user's psychological morale status
6. Infrastructure	the surrounding resources for communication capability
7. Social Environment	user's relatives, neighbors, colleagues and their relationships
8. User Tasks	the user's assigned tasks and aims
9. Time	date, time and day of week

Context Interaction



Context Interaction Examples

- 1 **Protected2Protected** context relation:
 - "Reveal my **location** only to people who are at a certain **location**"
 - "Reveal my **location** only to people who have a certain **identity**"
 - "Except for **certain people**, hide my **real identity**"
- 2 **Protected2Evaluated** context relation:
 - "Hide my **schedule** at **certain dates** (e.g. at the weekends)"
 - "Reveal my **blurred location** for indoor application, i.e. **communication infrastructure** is WLAN"
 - "Do not send my **profile, location, identity**, etc. if my **status** is set away"
 - "Never share the **physical condition context** with outdoor applications"
- 3 **Protected2Mixed** context relation:
 - "Blur my **location** for certain **people** at certain **dates/times**"

A Sample Policy

```

<protected context-property="location" action="allow|request|deny">
  <constraint on="date">
    <when condition="is|is not|before|after" date1="" date2="" />
  </constraint>
  <constraint on="time">
    <when condition="is|before|after" time1="" time2="" />
  </constraint>
  <constraint on="local_loc">
    <when condition="in|not in" place="" level="" />
  </constraint>
  <constraint on="status">
    <when condition="is" = "online|away|busy" />
  </constraint>
</protected>
  
```

Future Work

- specification of concrete elements in the new data model
- study of P3P to extend it for context-aware applications

Conclusion

- context privacy is required in context-aware applications
- context to protect should be concretely specified
- a privacy-aware context data model has been proposed