Expressing Privacy Preferences in terms of Invasiveness

Patrik Osbakk, Nick Ryan
The Kent UbiComp Group
University of Kent

http://www.cs.kent.ac.uk/projects/ubi
Introduction

- Privacy remains an issue in Context-Aware systems
- Closed vs. Open environments
  - Homes, offices
  - Gyms, tourist attractions, shops
- Dynamic information
  - Requires flexible protection mechanisms
  - Classical RBAC not sufficient
Privacy

- Right to control
- Offline level of privacy required
- Disclosure = loss of control
- Legislation
Earlier work

- Classification and Clearance Scheme
  - Context classified according to sensitivity
  - Participants assigned clearance representing trustworthiness
  - P3P allowed unknown participants to describe intended use and gain clearance
  - CCS does not scale to deal with many participants
Earlier work

- Privacy enhancing Infrastructure
  - Role Based Access Control
    - Based on RBAC$_0$
    - Permissions: List of Access Controls
    - Access Control: read, write, history
  - Automatic role activation – best access
  - P3P now map on to roles
Limitations

- Privacy preferences context dependant
  - Subject’s context
  - Potential recipient’s context
- Single vs. Repeated request
  - Surveillance
- Impact varies with previous exposure
- Precision and Reliability
  - Rough location vs. exact coordinates
Privacy Invasive Value - concept

- New concept
  - Privacy Invasive Value (PIV)
  - Privacy Invasion (PI)
- Release of information always invasive
  - Extent of invasion variable
- Primary determinants
  - About what, to whom
  - Allows concept to extend RBAC
Privacy Invasive Value

- Access controls include PIV
- Non-fixed value
- Modifiable PIV at runtime
  - To reflect current context
  - Depending on previous actions
- Transformation of context
  - Aggregate of components
  - Obscuring or reducing accuracy
Privacy Invasion

- Participants assigned maximum PI
  - Capping single privacy invasion
  - Restricting aggregate PI and its rate of increase
- Non-fixed value
- Multidimensional view of PI
  - Different PI for different categories/regions
Implications

- Extends the range of privacy preferences
  - More scenarios can be described

- Performance cost
  - Caching less efficient
  - Compensated by increased CPU power
  - Possible benefit from explicit role activation?
Conclusion

- The Privacy Invasive Value concept:
  - Address the limitation with dynamic context

- The full potential is still unclear
  - Further benefits may exist
  - Sufficiently interesting to warrant further research