

# **A Privacy Enhancing Infrastructure for Context-Awareness**

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

<http://www.cs.kent.ac.uk/projects/ubi>

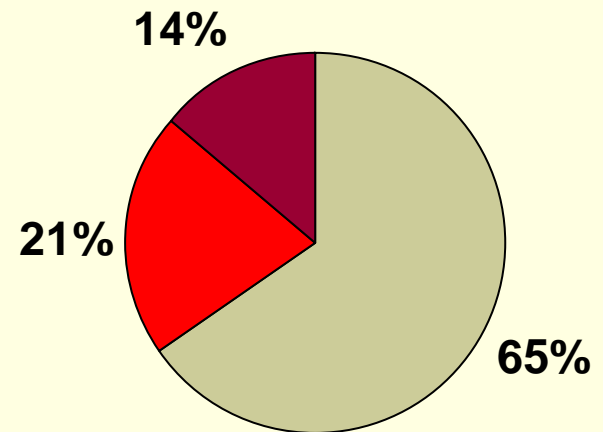
# Introduction

- Context-aware environments are *real*
- So are *privacy concerns*

“I am worried about the security of my personal information travelling on the internet and email”

[ICM Poll - The Guardian]

(2002)



■ Agree ■ Disagree ■ No opinion

# Introduction

---

- Context-awareness aggravate concerns
  - Richness of data
  - Quantity of data
- Privacy protection
  - Alternative to being *offline*
  - Trust formation

# Introduction

---

- Project aims:
  - Ease the development of privacy-friendly context-aware applications
  - Evaluation of the practicality of privacy protection in ubiquitous environments

# Context

---

- Definition:

Context is information related to an entity, where the information may be an entity itself.

# Context

---

- Entities
  - People, places, and things [Cooltown]
  - Activities
  - Concepts
- Existence of relationship
- Application specific definitions
- Real world = Infinitely complex network

# Privacy

---

- Definition:

“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”

[A.F. Westin]

# Privacy

---

- Flow of information
  - Contrast to physical privacy
- Ownership with subject
- Disclosure = loss of control
- Determinant of disclosure
  - Trust

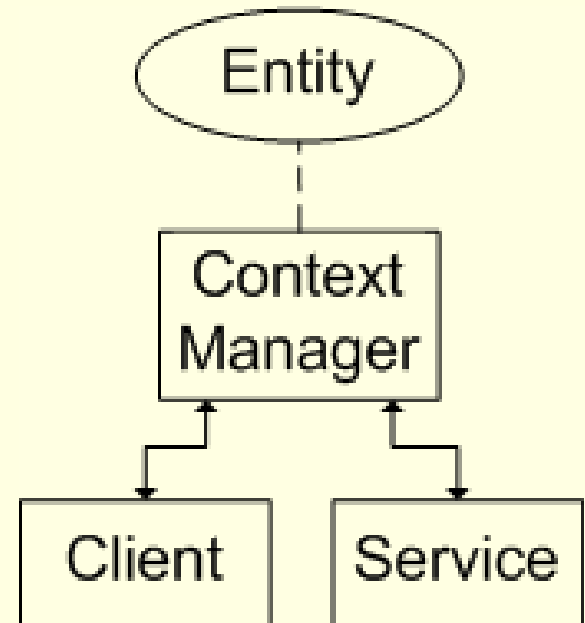
# Requirements

---

- Privacy protection mechanism
  - Offline privacy = necessary online privacy
  - Known and unknown agents
- Common application support
  - In-out boards
  - Call forwarding
- Heterogeneous devices
  - Limited capabilities
  - Variable Connectivity

# Infrastructure

- Entities
- Context Managers
  - Storage
  - Processing
  - Privacy protection
- Clients
  - Context consumer
- Services
  - Context producer



# Infrastructure

---

- Privacy protection

- Stage 1 - Authentication

- Username-password combination
    - Public key mechanism

- Stage 2 - Access Control

- Role based access control (RBAC)
    - The Platform for Privacy Preferences (P3P)

# Infrastructure

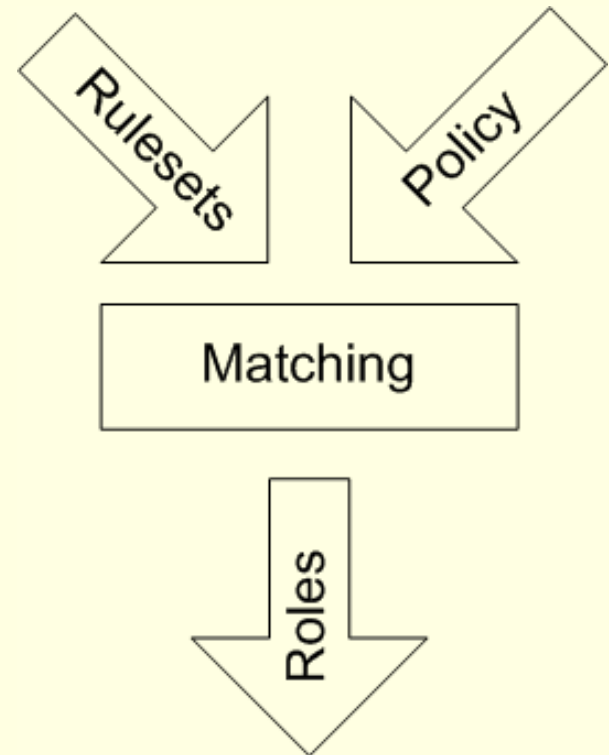
---

- Role based access control
  - RBAC0
  - Best access
  - Permission
    - Access Control
      - Read, Write, History
  - User permission

# Infrastructure

## ■ P3P

- Policy
  - Contract
- Ruleset
  - Preferences
- Matching
  - Role Assignment



# Future work

---

- Infrastructure integration
  - Context-aware office
  - Smart home
- Psuedonymity
- Anonymity

# Conclusion

---

- We have extended P3P and combined it with RBAC to provide a privacy enhancing infrastructure
- Our un-optimised implementation shows that these mechanisms perform well even on limited devices
- Simple applications has also been successfully created as a proof of concept