TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG

Security and privacy issues in location and context-aware systems

Jan Phillip Höft

Supervisor: Matthias Kranz

Seminar Ubiquitous Human-Computer Interaction
Summerterm 2007

Institute of Operating Systems and Computer Networks
Technische Universität Braunschweig

Overview

- Motivation
- Demands on location and context-aware systems
- Disclosing personal information
- Secure use of public services
- Conclusion

Security and privacy issues in location and context-aware systems

- **Scenario of a pervasive environment**
- **New services based on context information**
- **Upcoming questions:**
  - How to manage context information?
  - How to improve security?
  - How to stay anonymous?

- **Location and context-aware systems should…**
  - …protect the user's privacy & security
  - …be adjustable
  - …be easy to handle
  - …be time-saving
  - …be energy-saving if mobile

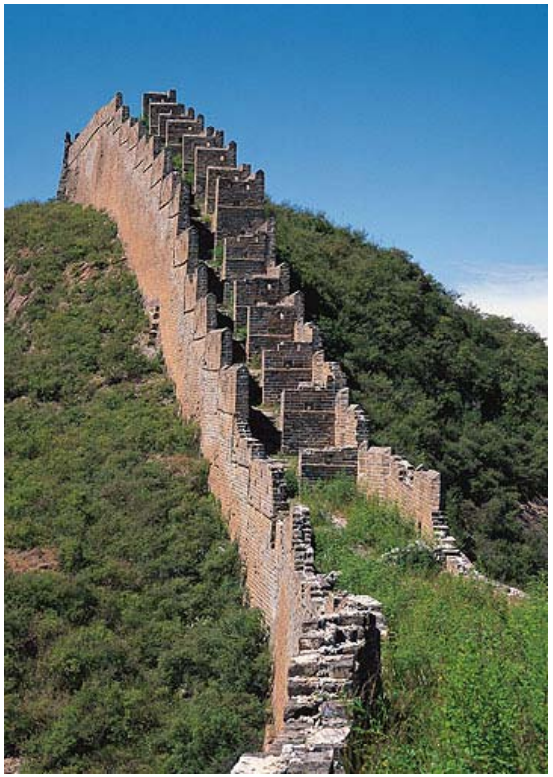
Obfuscating

- Changing the level of information's detail

	Identity	**Location** indoor/outdoor	**Activity**	**Nearby People**
Precise	True name	Room/Block	Precise	Names
Approximate	Pseudonym	Building/District	Categorical	Roles
Vague	Role	Municipality	Busy / Not Busy	Number
Undisclosed	Undisclosed	Undisclosed	Undisclosed	Undisclosed

The metaphor of virtual walls

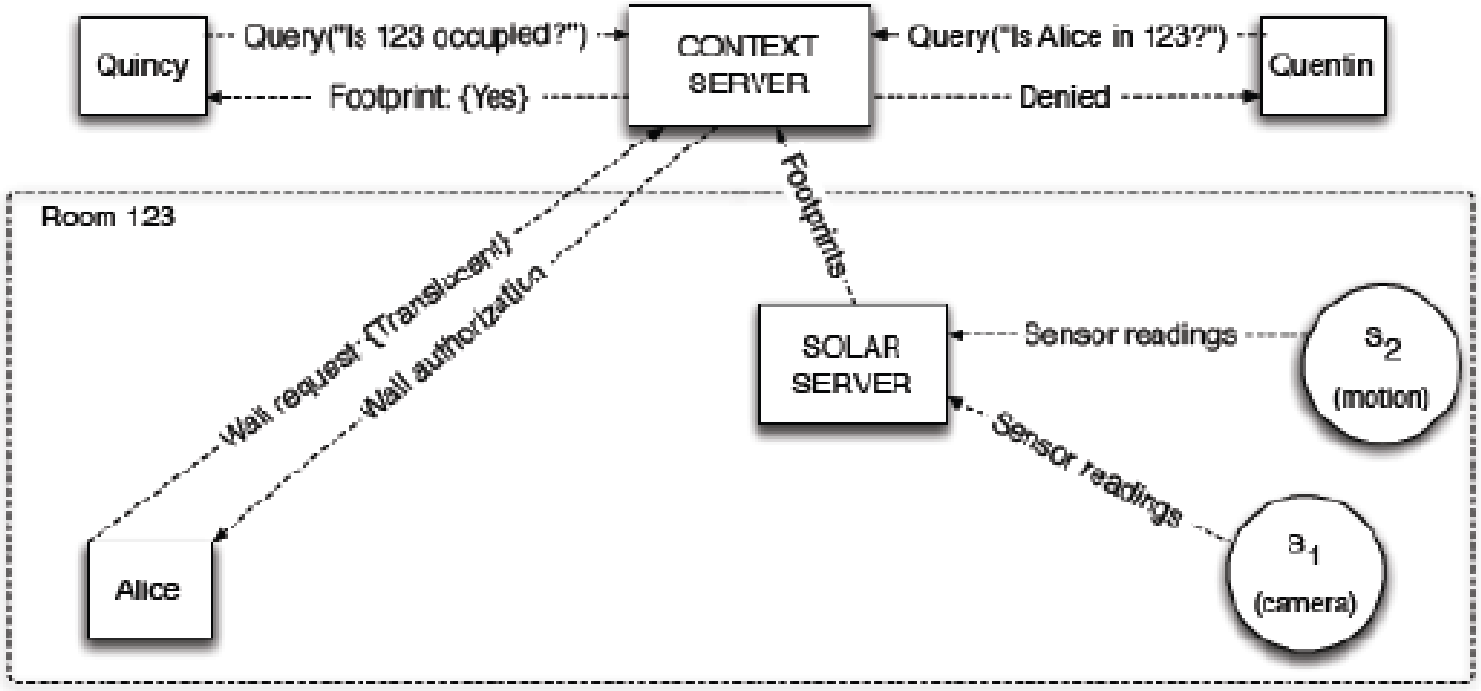
- Components
  - Places
  - Footprints
  - Solar server
  - Virtual walls
  - Context server



- **The metaphor of virtual walls**
  - Two levels of context information
    - Private information
    - Public information
  - Three levels of transparency
    - Transparent
    - Translucent
    - Opaque

The metaphor of virtual walls

- The architecture



The Metaphor of faces

- Components
  - Inquirer
    - wants to get some information
  - Situation
    - Location
    - Activity
    - Time
    - Identities of nearby people
  - Face
    - Set of information for disclosure

- **Share the secret**
  - Scenario of an untrustworthy environment
  - Private information needs to be transferred
  - Eavesdropping has to be avoided

- **Share the secret**
  - Cut the information into pieces
  - $f(x) = S_0 + S_1 x^1 + S_2 x^2 + \ldots + S_{n-1} x^{n-1}$
  - Divide the pieces on STS – Servers
  - Allow a service to collect and reassemble the information

- **Different approaches**
  - Faces / Virtual walls
  - Share the secret
- **Different scenarios**
  - Trusted environments
  - Untrustworthy environments
- **Trade-off between privacy / security and service**

Thank you very much for your attention!

- **Well shake before use**
  - How to securely connect two devices via Bluetooth?