Medical Applications

Tejinder Judge

Jacob Bardram

- Professor at University of Copenhagen
- His research areas are Ubiquitous Computing, Computer Supported Cooperative Work (CSCW), and Human-Computer Interaction (HCI)
- Main application area of this research is healthcare, especially Pervasive Healthcare

Central theme of these papers

- The main challenge in the shift from desktop computing, to ubiquitous and pervasive computing, is **user authentication**
- A domain where this challenge is easily seen is healthcare

Paper 1

Context-Aware User Authentication – Supporting Proximity-Based Login in Pervasive Computing

- Jakob Bardram, Rasmus Kjær, and Michael Pedersen
- Proceedings of Ubicomp 2003

Motivation

- Problems with Electronic Patient Records (EPR)
  - Clinicians have to log in 20-30 times a day
  - Have to log on to different machines based on location
  - Made easy to share passwords like '1234'

Activity-Based Computing

- The basic idea is to represent a user's (work) activity as a collection of computational services
- Make such activities available on various stationary and mobile computing equipment in a hospital
- Clinicians can initiate a set of activities, and access these on various devices in the hospital

Method

- Participatory design sessions and workshops
  - 12 workshops, 4-6 hours each with 6-10 participants (most of which were clinicians)
- Several user authentication mechanisms were designed implemented and evaluated

Requirements for a pervasive computing user authentication mechanism

- Proximity based
- Secure
- Active gesture
- Support for logout

Context-aware user authentication

- 3 key principles
  - First, it uses a **physical token** used for active gesturing and as the basis for authentication
  - Second, it uses a context-awareness system to verify the **location** of the user, and to log out the user when she leaves a certain place
  - Third, it contains **'fall-back' mechanisms**, so that if either of the two components in the system falls out, the user authentication mechanism switches to other mechanisms.

Authentication protocol

- The authentication protocol runs on a JavaCard
- The following information is stored on the card:
  - An id for the user the card belongs to.
  - The user's password.
  - The user's pair of a secret key (KS) and public key (KP).

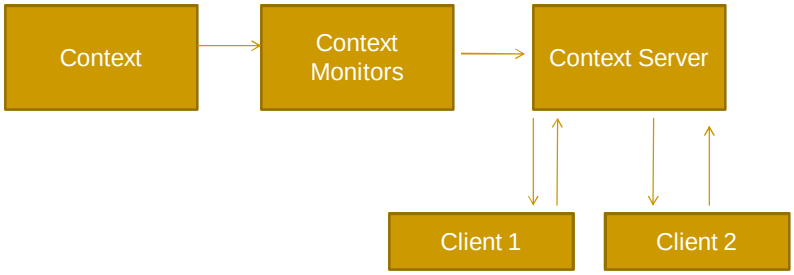
Authentication protocol

1. The client receives notification that user *P is in the room (optional).*
2. The user places his smart card in the card reader.
3. The client requests the *id from the smart card.*
4. The client looks up the person in the Context Server based on the *id from the card.*

Authentication protocol

5. There are two distinct cases based on the probability that the user is in the same place as the client.
   - Case A: The probability is greater that a certain threshold.
     - **The smart card is asked to verify that it holds the user's secret key, *KS.***
   - Case B: The location of the user is not sufficiently sure.
     - **The computer asks the user to enter his *password.***
     - **The smart card accepts or rejects the user based on the password.**

Infrastructure



Security analysis

It is possible for someone to authenticate as a legitimate user by the following:

1. Steal the smart card and fake the location of a legitimate user
2. Steal the smart card and be in the same room as the legitimate user.
3. Steal the smart card and acquire the user's password somehow

Possible solutions

- Voice monitor that can identify and locate a user based on voice
- Additional checks (e.g. is user still on his shift?)
- Using biometrics instead of a password

Paper 2

Applications of context-aware computing in hospital work: examples and design principles

- Jakob Bardram
- Proceedings of the 2004 ACM Symposium on Applied Computing

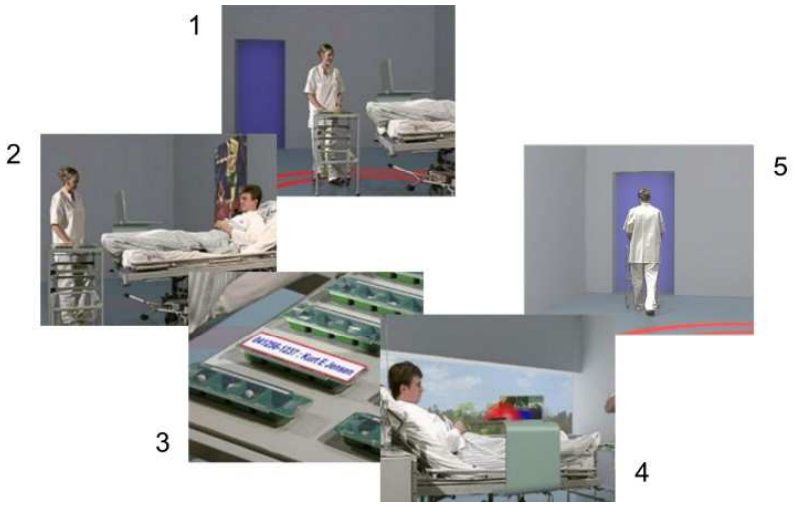
Motivation

- Addressing the problems of clinical computer systems being unaware of their usage context
- Example Electronic Patient Records (EPR)
  - Same interface is used in the ward, operating theater, medicine room
  - Doctors and nurses need to manually adjust the interface.

Method

- Design and implementation of context-aware clinical applications
  - Context-aware Electronic Patient Records (EPR)
  - Context-aware pill container
  - Context-aware hospital bed
- Design was a result of 15 workshops over 2 years
  - Each workshop was 4-7 hours, had 5-12 participants each
  - 8 participants were clinicians

Scenarios of context-awareness in hospitals



Prototype of context-aware hospital bed

- The bed has an integrated computer, a touch sensitive display, various RFID sensors
- The patient is identified using RFID tags in an armband and the personal profile is loaded into the computer

The Context-Aware Hospital Bed.

Prototype of context aware pill container

- Current implementation is based on RFID technology

The Context-Aware Pill Container. a – the vision with fingerprint recognition and a LED indicating proximity to the patient. b – the current prototype based on RFID technology.

Lessons learned

- Context-awareness is particular useful for user-interface navigation
- Context is more than location
- Physical things reveal activity
- Using context-awareness to suggest courses of action

Design principles

- Framework for context awareness in medical work
  1. Runtime Infrastructure
  2. Programming Framework (API)

Runtime Infrastructure

- Distributed and Cooperating Services
- Security and Privacy
- Lookup and Discovery
- Extensible

Application Programmer Interface

- Semantic-free modeling
- Context transformation
- Context quality
- Support for activities

Future work

- Creating a Java Context- Awareness Framework (JCAF) that addresses these design principles

Paper 3

Security in Context - Lessons Learned from Security Studies in Hospitals

- Jakob Bardram
- CHI 2007 Workshop on Security User Studies: Methodologies and Best Practices

Motivation

- Conventional login procedures cause usability problems especially in a hospital setting
- User studies show that the use of cryptic passwords made users write the passwords on the computer displays

Proposed solution

- *User-centered security* that has usability as a primary goal

Current security challenges

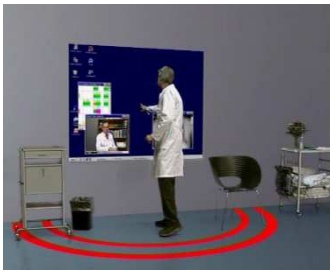
- Collaborating using an EPR
  - No longer easy for nurses to work together around digitized records
  - Technological challenge: is to enable users to share' a login, i.e. enabling some kind of collective user authentication.


Current security challenges

- User authentication in the design of home monitoring devices for the elderly
  - An elderly lady has severe problems of using the tablet PC and did not succeed in authenticating herself to the system using the finger print scanner

Prototype of proximity-based user authentication mechanism

- The overall goal with this proximity-based user authentication technology was to log in the user when he or she approached a computer, like a large public display.



Evaluation of prototype and results

- Logging in a person by proximity might not work in a real hospital
  - Authentication needs to be triggered by some gesture from the user
- Need fast switching between users
  - "Shift user" command while leaving screen intact

Lessons learned from multiple security studies

- Ethnographic field studies are useful in understanding security and usability problems
- Design security technologies based on what users do not by merely improving existing security technologies

Lessons learned from multiple security studies

- Making security more usable is to realize the need for many different kinds of security – one size does not fit all
- Make security visible and understandable

Central theme of these papers

- The main challenge in the shift from desktop computing, to ubiquitous and pervasive computing, is **user authentication**

Conclusion and critique

- Provided two solutions to **user authentication**
  - Context based authentication
  - Proximity based authentication
- Provided a domain and justification for using context-aware applications and activity-based computing in a hospital
- Did not discuss possible pitfalls of using context-aware applications in a hospital

Discussion

What are the tradeoffs to using context based applications in hospitals?

How can we design with users who prefer having no security hassle?

How can we implement security mechanisms which are sufficiently secure while being usable?

How do we evaluate such technologies?