DTU Informatics
Department of Informatics and Mathematical Modeling

Persistent Authentication in Smart Environments

Mads Syska Hansen,
Martin Kirschmeyer,
Christian Damsgaard Jensen
Systems Security Section
DTU Informatics
Technical University of Denmark
Christian.Jensen@imm.dtu.dk

Project was co-supervised with Dan Witzner Hansen, ITU

DTU Informatics
Department of Informatics and Mathematical Modeling

Smart Environments

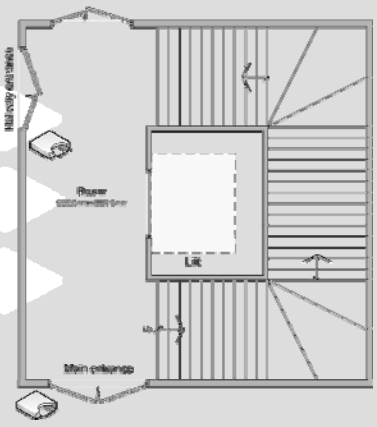
- Smart environment is *"a small world where all kinds of smart devices are continuously working to make inhabitants' lives more comfortable"*
  - Must observe the environment and control devices that provide services
- Sensors record properties of the smart environment (context)
  - Light, temperature, movements, presence, interactions, ...
- Different (distributed) service providers offer context based services
  - Location of principals, (location of) other principals, profile (history of previous interactions), subscriptions, registered preferences, ...
  - Different users may have access to different services
    - Must distinguish between principals to provide correct service
- Security mechanisms must be intuitive and convenient if they are to accompany all our actions and interactions

Security in Smart Environments

- Generally an extension of traditional security mechanisms
  - Access control based on identity of principals
- All principals must be authenticated before they can access a protected service
  - This may happen often, because services may include location based services (e.g., light or open a window by gesture control)
- Explicit interactions with security infrastructure every time a location based service is provided, is against the ambition to provide *"calm technology"*
  - Users will be distracted and convenience/productivity will suffer
- Exploiting the sensors already installed in the smart environment may help reduce inconvenience to users

Authentication Example from DTU

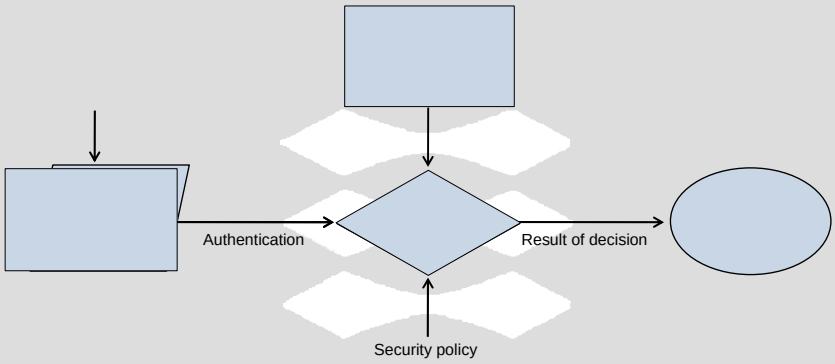
- Users authenticate when:
  - entering building
  - entering hallways
  - entering offices
- Actual authentication needs:
  - Building
    - Staff or student at DTU
  - Hallway
    - Staff or postgraduate student
  - Office
    - Inhabitant
- Also exposes the LOCLOU problem
  Location Of Check to Location Of Use
  - Slow users may be overtaken in the staircase or hallway
  - Similar to the TOCTOU problem



Authentication in Smart Environments

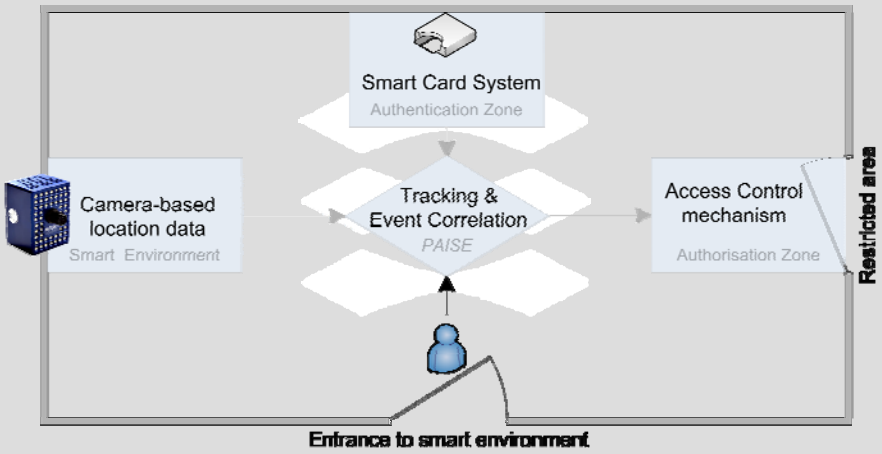
- Example of authentication with physical access control
  - Smart-card readers installed near every door to restricted areas
  - Principals must present credentials every time they wish to enter a restricted area
- This scheme has the following drawbacks
  - Inconvenient (users must stop to use smart-card)
  - Expensive (installation of smart-card readers)
- What if the smart environment is able to track users?
  - Only 1st authentication is necessary
  - Subsequent authentication may rely on tracking
    - Token based localisation of principals
    - Sensor based localisation of principals
      - Cameras, motion detectors,

Authentication and Access Control



DTU Informatics
Department of Informatics and Mathematical Modeling

PAISE

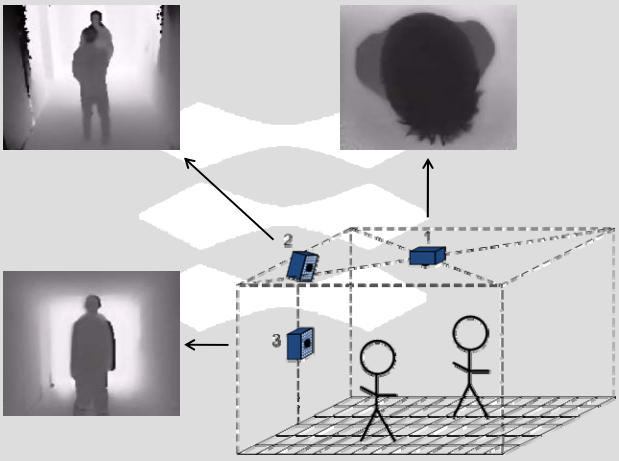


DTU Informatics
Department of Informatics and Mathematical Modeling

TOF Camera

- The camera provides both grey-scale and depth image

Camera Position

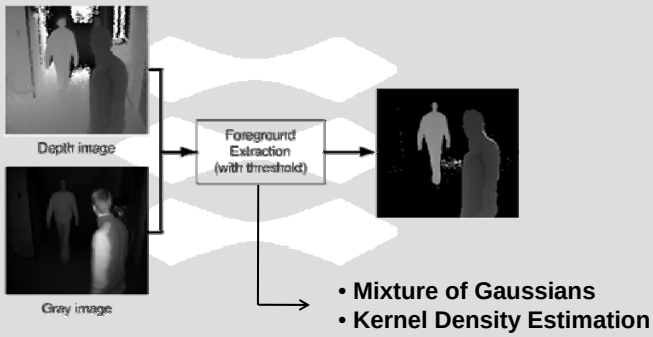


TOF Tracking in *PAISE*

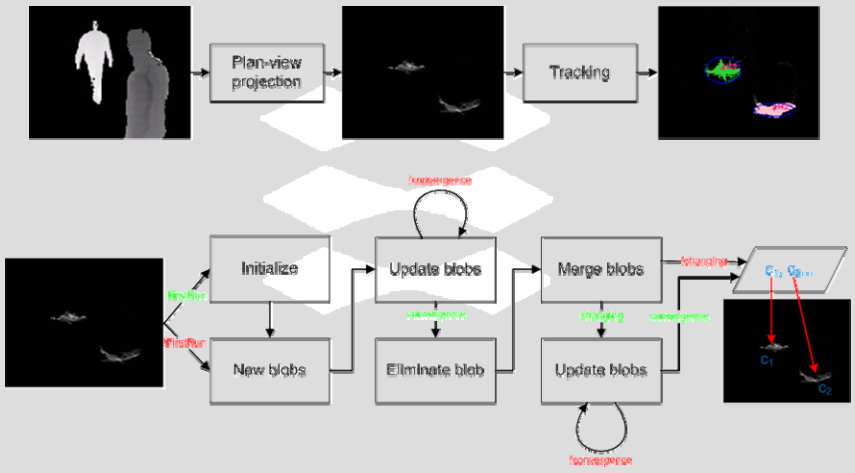
- Tracking follows 3 steps
  1. Find new users
     - Foreground extraction
  2. Track the users over time
     - Follow movements of existing blobs
  3. Determine the approximated position of all users
     - Record authentication information associated with blobs

Finding New Users

- Based on foreground extraction in the recorded images



Tracking in *PAISE*



Determining Position of Users

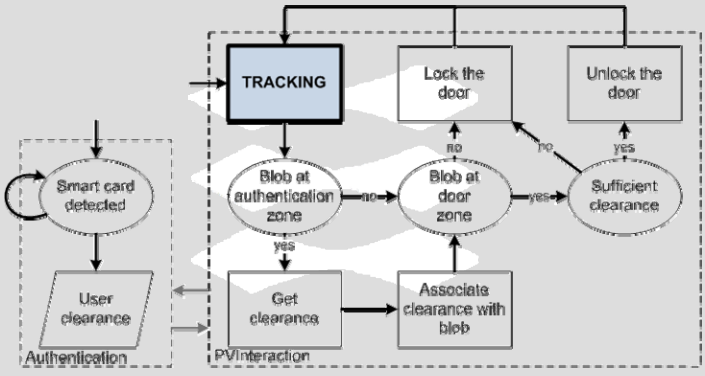
- Camera gives a distorted perspective of the scene
  - Caused by one-point perspective of camera
  - Avoided by projection of centroids
    - Using a homography gives a correct plan-view map

Plan-view map without homography

Plan-view map with homography

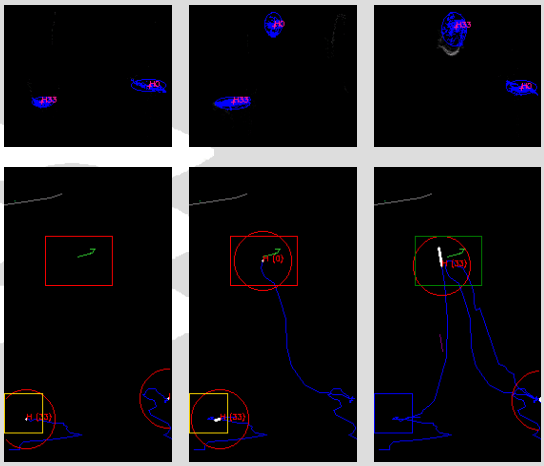
- Users may also result in more blobs (body and arms), which must be merged into a single blob

PAISE Security Policy Enforcement



PAISE Authentication Example

- Authentication zone
  - left box
    - yellow
- Authorisation zone
  - Top box
    - Red = locked
    - Green = open
- Users
  - Red circles
  - Blue tracks

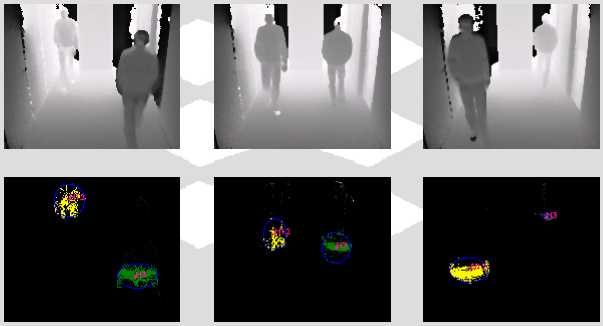


Evaluation Overview

Test number	Description	Frames
1	One person walks in illuminated scene	217
2	One person walks in darkness	222
3	One person walks in changing illumination	218
4	One person points TOF camera at TOF camera	837
5	One person changes clothes (black/white issue)	273
6	One person wrapped in cloth	245
7	One person leaves a bag in the scene	334
8	One person places a ladder in the scene	452
9	One person places chair and tables in the scene	591
10	One person standing and sitting	465
11	One person crawling	187
12	One person laying down	245
13	One person running	124
14	One person jumping	121
15	Two persons walking in same direction	224
16	Two persons walking in opposite directions	175
17	Two persons crossing	140
18	Two persons talking (occlusion phenomenon)	361
19	Two persons talking	336
20	Two persons shaking hands	205
21	Two persons walks close together and separates	234
22	Two persons bumps into each other	198
23	Two persons in the scene, wo authentication	224

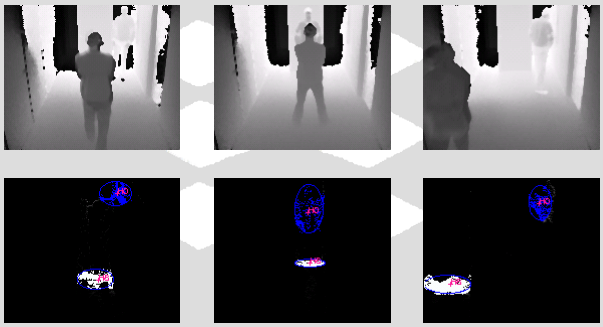
Evaluation

- Two users walking in opposite directions (Test 16)
  - Successful test



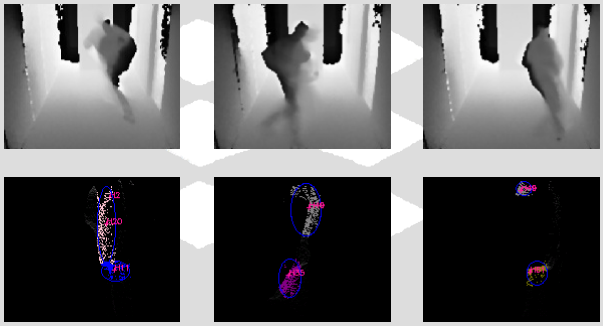
Evaluation

- Two users talking occluded (Test 18)
  - Successful test



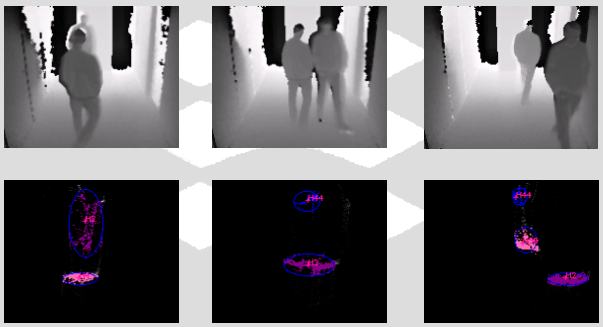
Evaluation

- One user running (Test 13)
  - Problem with frame-rate



Evaluation

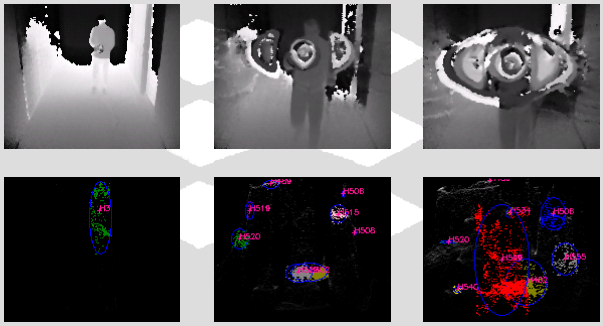
- Two users crossing paths (Test 17)
  - Problem with residual blob (but authentication is correct)



DTU Informatics
Department of Informatics and Mathematical Modeling

Evaluation

- TOF attack
  - System is attacked with a near infra-red light source



DTU Informatics
Department of Informatics and Mathematical Modeling

Conclusions

- Proposed a model of persistent authentication
  - Combines context information from smart environments with access control mechanisms
  - Authentication is recorded when users enter the env.; tracking binds authentication data to users and makes it available to servers of ambient (location based) services
- Presented a prototype base on TOF camera based tracking
  - Evaluation indicate ability to track (a few) users
  - Allows access control based on tracked authentication data
- Future Work
  - Improve scalability
    - Expensive computation may be parallelised
  - Improve robustness
    - Add more types of sensors (e.g., colour information, biometrics)

DTU Informatics
Department of Informatics and Mathematical Modeling

PAISE Software Architecture