Persistent Authentication in Smart Environments

Mads Syska Hansen, Martin Kirschmeyer, and Christian D. Jensen

Department of Informatics & Mathematical Modelling
Technical University of Denmark
Christian.Jensen@imm.dtu.dk

Abstract. Inhabitants in smart environments are often authenticated when they enter the smart environment, e.g., through biometrics or smart-/swipe-card systems. It may sometimes be necessary to re-authenticate when an inhabitant wishes to enter a restricted area or access ambient services or location based information, e.g., it is common to have swipe card terminals placed next to doors to restricted areas. This means that all access to protected resources must have individual means of authenticating users, which makes the access control system more expensive and less flexible, because access controls will not be installed unless it is absolutely necessary. The cost of installing and maintaining an authentication infrastructure and the inconvenience of repeatedly authenticating toward different location based service providers mean that new models of authentication are needed in smart environments.
This paper defines a persistent authentication model for a smart environment, which tracks inhabitants in the smart environment from the point of authentication to the protected resource, thus rendering authentication persistent by correlating the initial authentication event with the access control request. We present a proof-of-concept implementation of the proposed mechanism, which employs camera based tracking with a single stationary 3D camera that uses the "time of flight" principle. A preliminary evaluation of the proposed mechanism indicates that persistent authentication is technically possible with the proposed hardware. The proposed model is sufficiently general to allow the addition of more cameras or supplemental tracking technologies, which will improve the robustness and scalability of the proposed mechanism.

1 Introduction

Smart environments may be defined as *"a small world where all kinds of smart devices are continuously working to make inhabitants' lives more comfortable"* [1, p. 3]. It is generally assumed that a number of sensors are embedded in the environment to determine the current context of the inhabitants, so that the underlying system can anticipate their needs and provide them with services that facilitate their everyday life. Ideally, the provision of these services should be completely transparent to the inhabitant, who simply observes that services are available as they are needed, e.g., front doors open when they approach or lights are dimmed in the living room when the home cinema system starts.

Provision of such context-aware services in a smart environment requires knowledge about the inhabitants that are present in the environment and their current context.

Information about the inhabitants may include their identity, service history or profile, while information about the context includes the location of the inhabitants – either their location in absolute coordinates or their location relative to other inhabitants and the points of service provision. Moreover, knowing the exact location of inhabitants may help the smart environment to focus on the sensors that cover the areas where people are present. Fusion of data from diverse sensors and tracking of inhabitants' locations and behaviour allows the system to build accurate profiles of preferences and interaction behaviour. This raises important questions about the protection of the collected information and the privacy of inhabitants, which we do not address in this paper. Detailed knowledge of the environment, however, may also be used to enhance existing security services and provide stronger or more convenient security mechanisms; this is the topic of this paper.

In this paper, we examine the problem of authenticating principals[1] in smart environments. We propose an authentication model called *Persistent Authentication In Smart Environments* (*PAISE*), which combines traditional authentication mechanisms with sensing technologies and tracking capabilities offered by the smart environment. Without loss of generality, we limit our discussion to a single application of a secure service in a smart environment, namely an access control mechanism that controls the lock on a door to a restricted area. This application has all the essential properties of a secure server, but its familiarity and simplicity facilitates the discussion of our model.

There are different ways to ensure that the person who was authenticated is also the person who is trying to enter the restricted area. The simplest and most secure solution would probably be to enforce that only one person at a time is able to enter the corridors between the point of authentication and the restricted area, but such a solution is obviously too restrictive. Another solution is to track inhabitants from the point of authentication to the restricted area, thus correlating the authentication event with the access control request; this is the approach taken in the *PAISE* model.

The *PAISE* model proposed in this paper has been implemented in a simple prototype, which uses camera-based tracking using a 3D camera. Our evaluation shows that a single TOF camera is sufficient to track a small set of individual users in many situations, but that further work is required to improve the persistence, robustness and scalability of the system. We do, however, believe that multiple calibrated cameras [2] may help address these issues.

The rest of this paper is organised in the following way. Section 2 provides motivations for the model and a brief analysis of authentication in smart environments is presented in Section 3. Persistent authentication and the *PAISE* model is presented in Section 4 and a brief overview of the design and implementation of our *PAISE* prototype is presented in Section 5. The preliminary evaluation of our prototype is presented in Section 6 and related work is examined in Section 7. Finally, Section 8 presents our conclusions and outlines some directions for future work.

[1] We generally use *inhabitant* to refer to people in general and *principal* when we consider people in a security context.

2 Motivation

Physical access control is traditionally based on the authenticated identity of the principal. The authentication could be performed by a human guard who knows the user, by using a key, a swipe-/smart-card, a personal identification number (PIN) or a combination of the above. Many buildings have zones with different access control restrictions, so a principal moving between different zones would need to authenticate repeatedly, which would be considered an inconvenience and a distraction by most people. As a small example, consider the entrance to Building 322 at the Technical University of Denmark shown in Figure 1. Swipe-card access control and different restrictions for general access to the building and access to each of the hallways, means that principals need to authenticate twice to enter the hallway on the ground floor, even though there are no more than 6 meters between the two points of authentication. With swipe-card access to individual offices, staff would have to authenticate a third time before they can enter their own office.

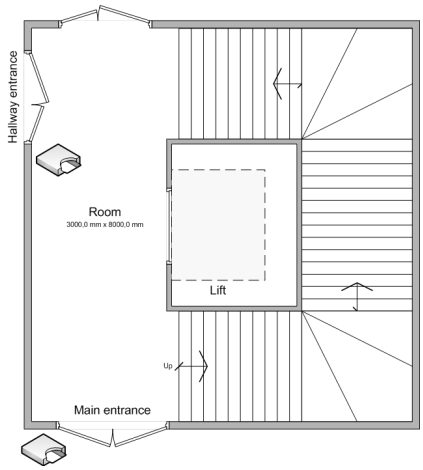

Fig. 1. East entrance to Building 322 at the Technical University of Denmark.

Depending on the physical access control policy implemented, a building could hold many points of authentication, which introduces the common known trade-off between security and usability. The more secure a solution is the less user-friendly it tends to be.

To improve the usability of such an access controlled environment one could try to introduce a system using only a single point of authentication. This solution would, however, introduce a new problem, which corresponds to what is commonly known in software as the time-of-check-to-time-of-use (TOCTTOU) problem; a kind of software bug that can be explained as a race condition between the check of the security credentials and the use of that checked credential. In a physical access control system, this problem can be translated to a location-of-check-to-location-of-use (LOCTLOU)

problem. The problem is still a race condition between the point where the principals verifies his identity and the intended use of that verification. If the principal is not alone between the verification and the point of use, then other inhabitants could usurp the authentication and enter restricted areas, which they were not authorised to enter - a race condition between users in the system.

The simplest way to protect against LOCTLOU, would be to restrict the area between the authentication and the intended use to one person at a time. This solution would, however, not be suitable, because it would impose too many restrictions on the simultaneous movements of people in the building.

3 Authentication in Smart Environments

It is a general requirement in smart environments that services are only provided to authorised users, e.g., the front door should not open for everybody. This means that services in a smart environment need to authenticate users in order to determine whether a principal is authorised or not. Authentication, however, is normally a process that requires active participation by the principal, e.g., presenting a badge, entering a password, swiping a finger across a biometric reader, etc. If we are to implement Mark Weiser's vision of ubiquitous computing [3], the authentication technologies employed in a smart environment need to be "calm" [4], which means that they should require minimal attention from the principals.

There are essentially two ways to implement calm authentication: either the principals are continuously authenticated in a way that they do not notice or they authenticate in a few strategic locations and the smart environment tracks the principal and makes the authentication information available to services as they are required.

In the first case, the authentication may either be based on biometrics that can be measured from a distance or the principal can be required to carry a small authentication token with short range communication capabilities that authenticates the principal toward the context-aware service providers in the smart environment. Typical biometric authentication technologies include fingerprint recognition, iris-/retina-scan, voice recognition and face recognition. Face recognition is the only of these technologies that does not require user involvement, but there are generally serious problems with false positives and false negatives, so we do not believe that the technology is sufficiently mature and secure for our scenario. It is also important to note that the failure mode of biometric authentication is absolute: false positives mean that unauthorised principals are granted access to a resource and false negatives may well imply that the principal has changed appearance and has to enroll with the biometric authentication system again. Smart wireless authentication tokens are convenient in many ways and, if properly used, the authentication results are both secure and non-intrusive. However, they do introduce problems when the authentication tokens are forgotten, lost or stolen. In some of these cases, principals will be tempted to borrow authentication tokens from each other, which leads to erroneous authentication.

In the second case, existing authentication technologies are used, so that authentication terminals are located in a few strategic places in the environment; we call these locations the *point of authentication*. Sensors in the smart environment are then used to

track the principals from the point of authentication, so authentication is only done once when the principal enters the smart environment from the outside. The authentication system associates the result of this authentication with the principal as he moves around in the smart environment, thus rendering the authentication persistent.

4 Persistent Authentication

The idea behind persistent authentication is to replace repetitive re-authentications with a system that tracks inhabitants in a smart environment from the point where authentication is done to the point where access control is enforced, i.e., it translates authentication in time and space from where it is done to where it is needed. This means that the event of authentication *"sticks"* to the principal, thus making it persistent.

4.1 *PAISE* Model Overview

The *PAISE* model defines four major components in a persistent authentication system: an authentication system, which is able to authenticate principals; a smart environment, which delivers the sensor data needed for tracking; an access control mechanism, which acts on the result of persistent authentication and the core component of *PAISE*, which combines the information from the authentication system and the smart environment, tracks authenticated principals in the smart environment and forward the necessary data to the access control mechanism. These components are shown in Figure 2.

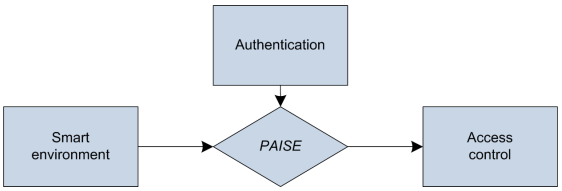

Fig. 2. The idea is to combine information from an initial authentication with information from a smart environment to perform persistent authentication.

In addition to these four components, *PAISE* also defines authentication zones and authorisation zones in the smart environment. An *authentication zone* defines the area in front of the authentication mechanism which is large enough to hold a single principal. The smart environment delivers a constant stream of sensor data to the core component, but tracking is only initiated when a principal has entered the authentication zone and successfully authenticated himself. The authentication zone must be small enough to ensure that the authentication event can be reliably linked to the principal. A typical authentication zone, in a smart environment, would be an area 0.5m $\times$ 0.5m in front of a swipe-card terminal. An *authorisation zone* defines the area in which the access control policy of a location based service must be enforced. When new principals enter an

authorisation zone the persistent authentication is forwarded to the access control mechanism of the location based service provider, which is then able to determine whether access should be granted. In the case of access through a door, in a smart environment, the authorisation zone must be small enough to ensure that most principals are able to reach and open the door while it is unlocked, but also large enough to ensure that nobody outside the authorisation zone is able to pass through the door while it is open. This allows the system to enforce the constraint that the door can only be unlocked if there are no unauthenticated or unauthorised principals inside the authorisation zone, thus preventing tailgating.

4.2 *PAISE* Security

The basic authentication in *PAISE*is performed by an authentication system that is external to the model. This means that the model supports *state of the art* authentication mechanisms based on passwords, PIN, smart-cards, authentication tokens, biometrics or multi-factor authentication [5]. The security of persistent authentication is therefore primarily a question of the systems ability to track principals after authentication.

There are different ways to locate or track inhabitants in a smart environment. The most common methods are: motion detectors based on photocells, infrared light or lasers; acoustic detectors similar to sonars or based on triangulation with multiple microphones; camera-based location and tracking systems; pressure sensitive floors [6] and token-based location and tracking systems, such as the Active Badge system [7], where each principal wears an active authentication token used to determine their location and track their movements in the smart environment.

In order to determine the overall security of a *PAISE* implementation, it is important to evaluate the tracking mechanism with respect to persistence, robustness and scalability, which we define in the following.

Persistence: The ability to track the principal and maintain the authentication. Persistence primarily address problems that arise in the day-to-day operation of the system, e.g., tracking may be lost if sensors are temporarily blinded by a flash from a tourist's camera.

Robustness: The ability to resist malicious and colluding principals' attempts to usurp the identity of other principals (each other in the case of colluding principals).

Scalability: The ability of the authenticate a large number of principals in a potentially large environment.

The different location and tracking technologies have different properties with respect to the accuracy; simplicity of installation and maintenance; and cost of installation and operation, but none of them are perfect. It is therefore important to force the system to a fail safe state, i.e., immediately classify the principal as unknown, when the tracking is lost or there is a risk of mistaken identity. As authentication always precedes authorisation, this means that no principal will ever be authorised based on suspect authentication information. If the authentication is lost, the principal has to re-authenticate at the nearest authentication zone, but this will be a rare event if the persistence and robustness of the tracking mechanism is high. Moreover, it is possible to place additional

authentication zones at several, strategically selected, locations in the smart environment so that principals will never have to move far if they need to re-authenticate. The number and locations of such additional authentication zones depend on both the persistence and robustness of the tracking mechanism and on the topography and the movement patterns of principals in the smart environment.

5 *PAISE* Prototype

In the following, we present a brief overview of the *PAISE* prototype that we have developed.

5.1 Overview

An implementation of *PAISE* consist of the four components shown on Figure 2, which is translated into a smart environment as illustrated on Figure 3.

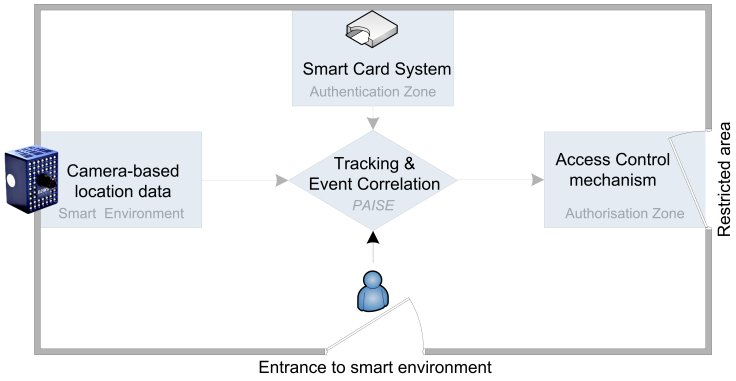

Fig. 3. Overview of the *PAISE* subcomponent connections.

The Figure shows a smart environment consisting of a single room, which has a camera-based location system. The room has access from the outside and provides principals, who authenticate using a smart-card based system, access to a restricted area. The decision to use a smart-card authentication system introduces many of the problems of token-based authentication and location systems to our prototype, i.e., that tokens can be forgotten, borrowed, lost or stolen. We would like to remind the reader that the choice of authentication system is external to our model and we simply chose smart-cards because it is reasonably secure and the hardware was available. Replacing smart-card based authentication with a system based on passwords and/or biometrics will completely eliminate this problem from our implementation. We describe each of the other elements of our prototype in greater details in the following.

5.2 Smart Environment

The sensors in the smart environment in our prototype consist of a single MESA Swiss-Ranger SR-3000 camera, which operates on the Time-Of-Flight (TOF) principle. The camera uses near-infrared[2] LED's (wavelength 850 nm[3]) to generate a depth image based on the Time-of-Flight principle. Light is sent out and the camera calculates the distance d_O based on the amount of time it takes the light moving to the object and back to the camera.

$$d_O = \frac{c}{2f} \cdot \frac{\varepsilon}{2\pi}, \tag{1}$$

where f is the frequency, c is the speed of light and ε is the phase [8, p. 9-16].

The TOF camera is able to deliver depth information out-of-the-box as the hardware inside the camera makes the needed calculations. The prototype is however quite expensive (approximately 5,000 Euros) - but the manufacturer of the Swiss-Ranger TOF camera (MESA) states that the camera should have a price in the same range as a normal web camera when a mass production starts.

5.3 Tracking in *PAISE*

Based on the depth information provided by the TOF camera, the *PAISE* prototype is able to identify objects that have the same distance and direction from the camera; such objects are commonly referred to as blobs. Each blob is a representation of an object, which is projected on to the floor of a virtual room[4] and tracking is done in two dimensions. Further details about how blobs are constructed and tracked is published elsewhere [9].

The interaction between the physical and virtual world is an important factor in *PAISE*. Decisions such as whether a user is granted access to a specific area is an access control decision, which need to be made by the system based on the location and the clearance of the user.

The main idea is to position the principals (by the location given by the tracking) in the virtual room, which corresponds to the real physical room. The locations of the principals should be checked against the predefined zones and if the users are located in these, an appropriate action is taken according to the decision tree illustrated in Figure 4. The current prototype implements the following security policy:

Authentication: The oldest blob at the authentication zone will get the clearance present at the authentication server. This means that if no credentials are present then the blob will remain unauthenticated.

Clearance: The authentication is used to label an clearance on a blob. If the blob is lost/eliminated the clearance is eliminated with the blob.

[2] Near-infrared light has a wavelength between 700 nm and 2000 nm, and is used for night-vision devises. Source: Britannica Online article 9002311 [February 13, 2008]

[3] Source: http://www.mesa-imaging.ch/prodviews.php [February 13, 2008]

[4] The virtual room is represented by an image of dimensions fitting the real room.

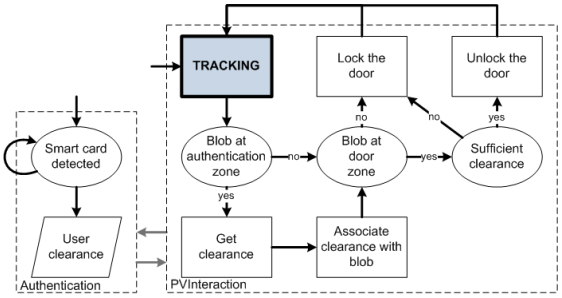

Fig. 4. Decision tree describing the access control of the electronic door lock.

Door: Access to the restricted area behind the electronically locked door is granted if a blob with the correct clearance is present at the zone (door). If more than one blob is present access is granted if just one of the blobs has the correct clearance. This allows authorised principals to accompany guests around the facility.

This security policy is quite simple, but it suffices to illustrate the advantage of persistent authentication in smart environments. The modular design of the *PAISE* prototype means that it is fairly easy to replace the authentication mechanism (*Authentication*) and the access control policy and mechanism (*Clearance* and *Door*) to reflect the needs of real environments. As an example, it is possible to implement an authentication mechanism, which does not authenticate principals if more than one blob is present in, or near, the authentication zone. It is also possible to enforce other access control policies, such as an access control policy that denies access to the protected resources when an unauthorised principal is present in, or near, the authorisation zone. This would limit the possibility of tailgating, social engineering and coercing an authorised principal to give access to an unauthorised principal.

The design and implementation of our prototype is described in greater detail in the M.Sc. Thesis of Kirschmeyer & Hansen [10].[5]

6 Evaluation

The evaluation of our prototype must determine whether it meets the important security properties in persistent authentication, namely persistence, robustness and scalability.

6.1 Evaluation Setup

The evaluation was performed in a deserted hallway in our building. The 3D camera was mounted in an angled top-view position just below the ceiling at one end of the hallway. The angle between the ceiling and the top of the camera was as small as possible. This

[5] This report is currently not available online, but it can be obtained from the library of the Department of Informatics and Mathematical Modelling at the Technical University of Denmark.

resulted in a scene that was 6.4m long, 2.3m wide and 2.3 m high. The scene was illuminated by fluorescent lights mounted in the ceiling.

The core component of the *PAISE* prototype runs on an IBM ThinkPad T60, with a 1.8GHz processor, 1.5GB internal memory and plenty of available disk space. We used a simple smart-card based authentication system, but since this is an exchangeable part of the system, and external to the *PAISE* model, we consider it beyond the scope of this evaluation.

6.2 Persistence

A number of experiments were designed to test the prototype's ability to track principals under different conditions. In particular, we wish to test how the system deals with: multiple principals, foreign objects, velocity of principals, partial occlusion and close contact between principals. The results of our evaluation is shown in Table 1.

Test	Scenario	Expected outcome	Result
1	Two principals walk in the same direction	The tracking should identify and follow the two separate users	success
2	Two principals walk in opposite directions	The tracking should identify and follow the two separate users	success
3	Two principals cross their path	The tracking should identify and follow the two separate users	success
4	One principal leaves a small object (a bag) in the scene	The tracking should follow the user and ignore the small object	success
5	One principal leaves a large object (a ladder) in the scene	The tracking should follow the user and ignore the large object	success
6	Two Principals talking (one principal is partially occluded)	The tracking should identify and follow the two separate users	success
7	Two principals shaking hands	The tracking should identify and follow the two separate users	success

Table 1. The results of the persistence evaluation.

The first three experiments validate that tracking works under normal circumstances and experiments 4 and 5 show that the system is able to handle foreign objects. Experiments 6 and 7 demonstrate the advantage of using a TOF camera, because the two principals have different distance to the TOF camera.

6.3 Robustness

An evaluation of the robustness must assess the persistence of the authentication with respect to properties that are open to manipulation by a malicious attacker. Such properties include lighting, properties of clothing, posture and velocity of principals in the smart environment.

The TOF camera operates with near infrared light, so the changes in the visible spectrum of light in experiment 1 has no effect. The attempt to *blind* the TOF camera

Test	Scenario	Expected outcome	Result
1	One principal walks in light/darkness	The tracking should follow the user regardless of the illumination of the scene	success
2	One principal points a near infrared light source at the TOF camera	The tracking system will be blinded (denial of service)	partial success
3	One principal changes clothes from black to white	The tracking should follow the user regardless of the change in black/withe contrast	success
4	One principal walks wrapped in tinfoil	The tracking should follow the user despite reflections	success
5	One principal stands and sits down	The tracking should follow the user despite the change in posture	success
6	One principal running	The tracking should follow the user	failure
7	One principal jumping around	The tracking should follow the user	failure
8	Usurpation attempted (two principals, but only one authentication)	The usurping principal will not be authenticated when he enters the authorisation zone	success
9	Two principals bump into each other	The tracking should identify and follow the two separate users	partial success

Table 2. The results of the robustness evaluation.

in experiment 2 is only partially successful, because the attacker has to be very close to the TOF camera (approximately 1m) before the attack is effective. The TOF camera has known problems with measuring distance to objects that have sharp contrasts between black and white. The attacker in experiment 3, attempts to exploit this problem by wearing a black jacket and white trousers; he further takes off the jacket to reveal a white t-shirt underneath, but the *PAISE* tracking system was able to persistently track the principal. Neither the reflections created by the tinfoil in experiment 4, nor the change in posture in experiment 5 has any effect on the tracking. Experiments 6 and 7 show that the current tracking system is unable to manage principals who move very quickly or who frequently change direction and velocity. The heavy computational load means that the frame rate of the tracking system is unable to handle large variations in the scene. In experiment 8, one principal is waiting for the other principal to authenticate and races to the authorisation zone ahead of him, but the access control mechanism does not grant access. Experiment 9 is a partial success; tracking is temporarily lost at the moment the two principals collide, but the system correctly identifies and tracks the two principals after the collision. Further experimentations are needed to build confidence in the system's ability to correctly identify principals after collisions.

The robustness of the tracking system, using a single TOF camera, is surprisingly high. Moreover, we believe that the robustness can be improved significantly by using a multi-modal tracking mechanism, e.g., a simple web camera could improve tracking robustness by including information about the colour of clothes.

6.4 Scalability

We did not design specific tests to determine the scalability of our current prototype. Our general experience with the system, however, indicate that the scalability is unsatisfactory. With more than a handful of people on the scene, the frame rate that the system is able to process with the current hardware drops below the level necessary to provide reliable tracking. However, the algorithms used to track each individual person has no interaction with the tracking of other people, so the task is well suited for parallel computation. We therefore expect to be able to develop a more scalable version of our prototype, where parallel processors are used to track principals in the scene.

7 Related Work

Corner and Noble [11–13] examine the problem of authentication when mobile devices are lost or users leave a work station logged in. They define traditional authentication mechanisms as *persistent* because they rarely limit the duration that the authentication is valid, so a user may leave a computer logged in for several days without a screensaver. This means that anyone who steals a device that is logged in or gets physical access to the workstation may usurp the authentication of the original user.

They define an *transient authentication* mechanism, where all data in the system is encrypted and a small *authentication token*, worn by the user, is needed to provide access to the encrypted data, thus ensuring that access can only be granted when the token is in close proximity to the system where the user is logged in. The token stores the cryptographic keys and the proximity mechanism is based on short range wireless communication.

The definitions of persistent and transient authentication by Corner and Noble are device centric, authentication sticks to the device as long as the user is present, so restrictions may be put on the users, e.g., they have to wear the authentication token. This creates problems when authentication tokens are forgotten, borrowed or lost. Our definition of persistent authentication is user centric, which means that authentication sticks to the user as long as the tracking from the last authentication zone is considered reliable. This means that any authentication mechanism, e.g., passwords, PIN or biometrics, can be used and that no additional requirements are placed on the user.

Bardram et al. [14] defines a context-aware user authentication mechanism, where users need a smart card to identify themselves to the system and an RFID based tracking system is used to authenticate the user. This adds complexity for the user, by requiring that he remembers two tokens, without offering significantly improved convenience, i.e., the user still has to insert the smart card into the system whenever authentication is required. Our proposal removes the need to perform specific authentication actions as long as the tracking is considered reliable.

Klosterman and Ganger [15] define a *continuous biometric-enhanced authentication* mechanism, which uses a biometric authentication module, based on face recognition, to periodically re-authenticate users who are logged in to the system. If, at some point, the biometrics of the user sitting in front of the monitor does not correspond to the biometrics of the authenticated user, re-authentication is required. This means that continuous authentication is achieved without addition requirements are placed on the user,

but their system authenticate a specific user at a specific location, where we propose to track the user so that his authentication may be reused in different locations.

8 Conclusions

In this paper we examined the problem of user authentication in smart environments. We proposed a persistent authentication model, which tracks principals in the smart environment and binds authentication information (a clearance) to principals whenever they authenticate with the system. This means that mobile users are transparently authenticated toward location based services in the smart environment. This has obvious privacy implications which we aim to address in future work.

We presented a brief overview of the prototype implementation of *PAISE*, which we have developed at the Technical University of Denmark. We have conducted a series of different experiments to evaluate our prototype and some of the results of these experiments are presented in the paper.

The evaluation shows that the *PAISE* prototype is able to track a small number of simultaneous principals who move normally in a smart environment, so that once a principal has been authenticated, the result of this authentication can be associated with the principal as he moves around in the smart environment. Our evaluation also demonstrate that the current prototype is unable to track principals who move very fast or who changes direction or location very quickly. We believe that this is primarily caused by the limited computational resources available for the prototype, which results in a relatively low frame rate from the tracking subsystem (see also the discussion of scalability below). We have also identified problems when principals are in very close contact with each other, e.g., two principals hugging. We conjecture that both of these problems may be addressed by adding more sensors to the smart environment, thus enabling a multimodal tracking mechanism. We would therefore like to explore the addition of more sensors to the environment, such as a simple colour web-camera. This would provide valuable information about the colour of clothes worn by the principals, which would help differentiate between principals in close contact and might help rebind authentication information to a principal if the tracking is lost without requiring re-authentication.

The evaluation indicates that the scalability of the current prototype is unsatisfactory, so we wish to redevelop the tracking algorithms of the *PAISE* core component to track different people in parallel on multiple processors.

Finally, we conclude that the *PAISE* model provides a useful abstraction for authentication in smart environments, which may significantly improve the usability of a traditional authentication system. Moreover, our implementation and evaluation of the *PAISE* model indicate that it is both practical and feasible.

References

1. Cook, D., Das, S.: Smart Environments: Technology, Protocols and Applications. Wiley-Interscience (2004)
2. Focken, D., Stiefelhagen, R.: Towards vision-based 3-d people tracking in a smart room. In: Proceedings of International Conference on Multimodal Interfaces (ICMI), Pittsburgh, U.S.A. (2002) 400–405

3. Weiser, M.: The computer for the 21st century. Scientific American Special Issue on Communications, Computers, and Networks (1991)
4. Weiser, M., Brown, J.S.: Designing calm technology. PowerGrid Journal **1.01** (1996)
5. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE **91** (2003) 2021–2040
6. P. Srinivasan, D. Birchfield, G.Q., Kidane, A.: Design of a pressure sensitive floor for multimodal sensing. Information Visualisation (2005)
7. Roy Want, Andy Hopper, V.F., Gibbons, J.: The active badge location system. ACM Transactions on Information Systems (TOIS) (1992)
8. Sigurjón Álrni Gudmunðsson: Robot Vision Applications using the CSEM SwissRanger Camera. Master's thesis, Institute of Informatics and Mathematical Modeling, Technical University of Denmark (2006)
9. Hansen, D., Hansen, M., Kirschmeyer, M., Larsen, R., Silvestre, D.: Cluster tracking with time-of-flight cameras. In: Proceedings of the CVPR 2008 Workshop on Time of Flight Camera based Computer Vision (TOF-CV), Anchorage, Alaska, U.S.A. (2008)
10. Kirschmeyer, M., Hansen, M.S.: Persistent authentication in smart environments. Imm-thesis-2008-16, Department of Informatics & Mathematical Modelling, Technical University of Denmark (2008)
11. Corner, M.D., Noble, B.D.: Zero-interaction authentication. In: Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MOBICOM), Atlanta, U.S.A. (2002) 1–11
12. Noble, B.D., Corner, M.D.: The case for transient authentication. In: Proceedings of the 10th ACM SIGOPS European Workshop, Saint-Emillion, France (2002) 24–29
13. Corner, M.D., Noble, B.D.: Protecting applications with transient authentication. In: Proceedings of the First ACM/USENIX International Conference on Mobile Systems, Applications and Services (MobiSys'03), San Francisco, U.S.A. (2003) 57–70
14. Bardram, J.E., Kjær, R.E., Pedersen, M.O.: Context-aware user authentication - supporting proximity-based login in pervasive computing. In: Proceedings of UbiComp 2003, Seatle, U.S.A. (2003) 107–123
15. Klosterman, A.J., Ganger, G.R.: Secure continuous biometric-enhanced authentication. Technical Report CMU-CS-00-134, Carnegie Mellon University (2000)