

# A Secure Pervasive Environment

Patrick G. McLean

Trusted Computer System Group  
Information Networks Division  
Defence Science and Technology Organisation  
PO Box 1500, Edinburgh 5001, South Australia

Patrick.McLean@dsto.defence.gov.au

## Abstract

This paper explores the complications encountered when attempting to create a secure pervasive computing environment. The model introduced in this paper is primarily conceptual. The chosen environment is built around a shared space containing a classified network. Since access to the classified network is only available to people once they are in this space, we investigate what is required to ensure only authorised people can enter, which highlights problems inherent in any kind of physical access control, and then how to carry this through to manage their access to information once inside the space.

A layered agent architecture is considered, using real time devices such as biometric mechanisms, door actuators and a smart card reader acting as the lower level agents. These agents are then wrapped in software allowing them to communicate with higher level agents that through the coordination of these low level agents control the security of the pervasive environment. Security is further enhanced, by preventing the classified network from communicating with the network containing the biometric devices and databases.

We also consider the security implications of using paper documents within the shared space, as well as the possibility of any other devices that could potentially be used for smuggling information out of the environment.

## 1 Introduction

Pervasive computing aims to provide users with computer-supported capabilities anywhere, anytime and in the most appropriate form for the user's current context. In order to achieve this, an increasing number of intelligent devices are required, whether portable or embedded in the user's environment. To this end most research in pervasive computing has been in building various infrastructures to facilitate its heterogeneous nature, with far less research on security in this environment. This is not to say that there hasn't been

research in security in other areas of computing and information technology. In particular, there is increasing interest in biometric-based personal identification and verification technology.

In any organisation where security matters the correct identification and verification of users is paramount. Authentication is equally important when allowing a user access to a physically secure space as it is when granting access to a secure file space. Its purpose is to ensure that each entity is correctly matched to its corresponding privileges. If someone is not accurately identified and their identification is then left unverified, unauthorised access to data and resources is a real possibility. Major security requirements, such as authorisation, auditing and non-repudiation all hinge on the accurate identification and verification of users.

However, one of the main difficulties in designing a secure pervasive environment is in ensuring that the functionality of the environment is not over-constrained by security. As a result we have two high-level requirements for our environment: security and usability. The security requirement can be further broken down into: the physical security of the environment (i.e. the security controlling the flow of people in and out of the environment) and the security of information within this environment.

The paper is structured as follows: In section 2 we give a description of the chosen environment. In section 3 the challenges of physical and information security are discussed. In section 4 we discuss requirements. Section 5 suggests an architecture for our environment. Section 6 looks at other pervasive technologies and section 7 contains the summary.

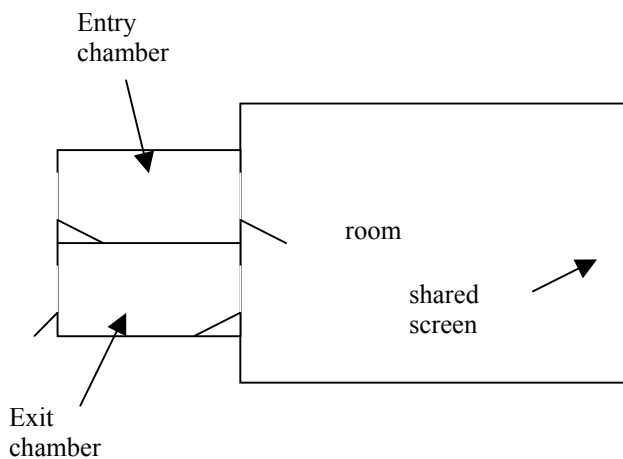
## 2 Room description

Our environment will be instantiated in the form of a room similar to the one illustrated by McCarthy and Thredgold (2002) and as shown in figure 1. The room would typically be used for meetings or as a command & control centre, so the focal point once inside the room is a shared large-screen display.

To ensure the security of information within the room, we need to have trusted devices guarding access to the room, as well as security of information available to authorised persons inside the room. The network architecture of the room incorporates a sensor network and a user network; the sensor network is so called because it uses biometric sensors, a smart-card device and door actuators, all of which are wrapped in agent software, while the user

network is the one that contains the information to be viewed or manipulated by the end user. Authentication/authorisation for accessing the room is handled by the sensor network, with authentication information being passed from the sensor network to the user network where authorisation to access information on the user network is carried out.

The use of an agent framework allows us to abstract away the implementation of the system from the functionality of the system. Working with agents is a form of reductionism. In this context they date back to Minsky's 'Society of Mind' (1986), where we have, at the lowest level of reduction, a number of dumb agents that come together to create smarter agents. These smarter agents can in turn become building blocks for a higher level of agents and so on in the belief that we will end up with top-level agents displaying intelligent behaviour. The intelligence of our room therefore comes from agent interaction. The room's low-level sensors are analogous to our own sensors, and in the same way that we are made up of higher-level agents that are able to process in a sensible way the flood of information received through our sensors without it overwhelming us so to are the room's higher-level agents able to coordinate its lower-level cousins.



**Figure 1: Possible room layout**

### 3 Physical and Information security challenges

In discussing the threats to the physical security and information security of data within an organisation, we are focusing on concealed attempts at accessing data in the workplace, "ranging from unauthorised persons following employees through open doors to data theft by employees" (from Radcliff 2001).

Network information security is traditionally implemented by technologies such as digital encryption, firewalls and VPN's, whilst in parallel physical security is being implemented by an even wider range of devices and products ranging from perimeter fencing, office doors with swipe card access, to security guards with dogs. In

the age of computer networks and with the pervasive computing age dawning a more amalgamated approach to security is needed. It is only because of the current state of technology that we can take advantage of such things as smart card readers and biometric devices, which plug into networks, and are able to provide a tighter union between information and physical security. While this amalgamation may provide tighter security in a traditional computing environment, a pervasive environment is more challenging.

In a non-pervasive environment, most people work at their computer alone within their workstation or office that is often bordered by at least three walls and if they wish to protect what they are doing they simply lock their computer. In a pervasive environment, it is expected that users will be able to access data away from their office and in shared workspaces where unauthorised disclosure of data, including login details, poses a greater risk. In this new climate of shared work spaces, the risk of someone fraudulently performing input using someone else's login details is greater and, for reasons such as this, access to these workspaces and the computers within them may require non-traditional physical and information security measures.

Again, it is one thing to try to secure information within a pervasive computing environment that is contained within a workplace, but new security threats arise when information is taken out of this environment. By removing information from the workplace, you allow potential infiltrators to circumvent a major obstacle to unauthorised access, for the workplace physical security now becomes redundant, and cannot be replaced even when data is strongly encrypted. For example, if the user's secret key, which is generated from their biometric print, automatically encrypts data downloaded to disk. Then, assuming that the biometric print being used cannot be forged, (see Matsumoto 2002) the encrypted data may be secure if it is lost or the person's laptop, disk or their token containing their private key is stolen. However if the person accesses the protected data in public, it is still susceptible to such things as shoulder surfing or if accessed through a wireless device, data intercept even if the access device remains in the keeping of authorised personnel.

While this paper primarily focuses on using biometrics to enhance security within a particular environment, physical and information security using a strong biometric would also increase privacy. Having said this, even assuming our system just stores an encrypted template of a digital biometric rather than a copy of the actual biometric, biometrics carry a fair bit of negative baggage in the way of privacy issues. For example, while our application of the technology may be for the purpose of increasing security within a specific application, there is always the possibility that the stored biometrics could be used in other applications, without the person's permission (this may be protected against by encryption, but the problem then becomes one of key management). Another concern of biometric authentication is that criminals will go to great lengths in order to appropriate

such an infallible form of authentication, thus raising the personal security concerns of the users.

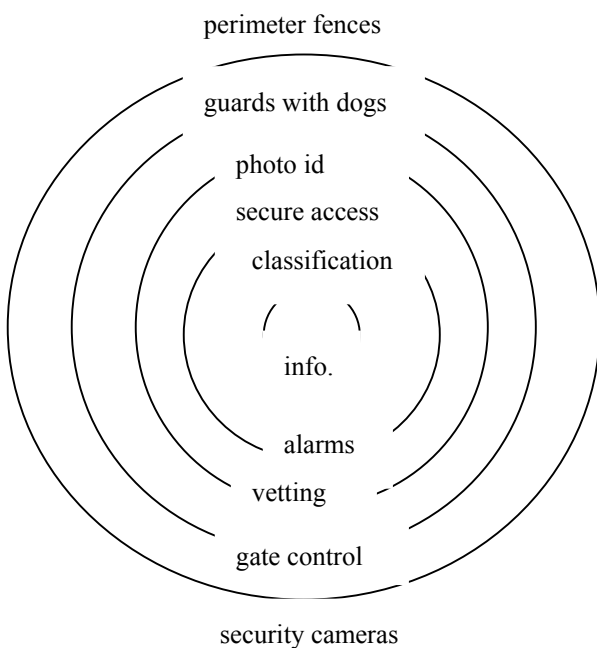
## 4 Requirements

This section looks at the different requirements for our environment.

### 4.1 Security requirements

High levels of security are typically associated with Defence, which makes it a good subject for the combining of our two security approaches. Security in defence is concerned with the security of the nation and its national interests. Its protective security objectives consist of protection of Defence premises and information, ensuring only authorised persons are allowed access to classified information.

The architecture of Defence security is traditionally based on the defence-in-depth principle, as illustrated by Blades (1997), and shown in figure 2. This means that whatever needs to be protected is circumscribed and a series of protective barriers is placed around it, so that total reliance of any one measure is not necessary.



**Figure 2: Diagrammatic representation of defence in depth**

The security mechanisms in place must forbid the unauthorised removal, extraction, copying and alteration of information. The proper control of classified documents also requires that their distribution be regulated and that an effective audit system be in place.

In any environment where we have users with different levels of clearance, and therefore different privileges in relation to what information users are cleared to see, we need to somehow control users' access to information, ensuring that they are able to see what they are authorised to see and no more. For example, in a possible Defence

scenario, if someone is cleared to see documents that are classified at Secret level this means that they are also cleared to see documents that are classified Restricted; whereas someone who is cleared to see Restricted documents is not necessarily permitted to see Secret documents, so we have a hierarchy of clearances where a lower classification is a proper subset of the classification above it.

The issue of clearances in Defence can become more complicated when we consider that a person's clearance can be made up of more than just their classification. One example is if we consider that our system needs to be used within a coalition where, although Australian Defence may allow its own personnel cleared to Secret to view Secret documents, it may not be in the interests of national security to give someone from a nation within the coalition, who is cleared by their defence department to Secret level, the ability to view the same document. Another example is the potential for a document from country A that is classified Secret, to be releasable to a person from country B with Secret clearance but not a person from country C with Secret clearance. This means that the rule previously stated for our classification hierarchy has additional provisos, such as nationality, creating a greater challenge for security within this scenario.

Taking into consideration the security challenges within a Defence environment, what we are trying to achieve is an environment where there is no unauthorised disclosure of data, while at the same time not preventing people from seeing what they are authorised to see, and where all interaction with the room network is audited. In order for this to happen we need to trust that it meets the following security and usability (4.2) requirements:

#### 4.1.1 Only allow authorised person(s) to enter room and update context appropriately

For strong security a person is authenticated based on 'something they have' (smart-card), 'something they know' (pass phrase) and 'something they are' (biometric). Updating the context of the room is based on who is in the room, to ensure there is no unauthorised access to information.

#### 4.1.2 Identify who exits the room and update context

At first blush, identifying who exits the room does not appear to be nearly as important as identifying who enters the room. But, for example, in a coalition military operation with multiple logons and where the information that is displayed on the large screen is dependant on the intersection of the various nationalities in the room, positively identifying who is in the room is important. If someone of higher classification is incorrectly identified on leaving the room as someone of a lower classification, then this person of lower classification, who is still in the room, may be privy to information they are not cleared to see because the room context has been updated incorrectly.

Without insuring that the room possesses a trusted way of knowing who is in the room, there is also potential for denial of service attacks. For example, if an unauthorised person manages to enter the room and causes the system to activate a security alert, which then blanks the rooms visual display(s), and this person then manages to exit the room unrecognised as the same person, the display(s) will stay blank. Therefore, we should, have just as strong security in place for exiting as entering the room.

#### **4.1.3 Identify who is in the room**

The solution to this point is derived from knowing who has entered the room(4.1.1) and who has exited(4.1.2).

#### **4.1.4 Audit all successful and unsuccessful attempts to access data**

One reason we audit is to investigate and examine the room's transactions with the aim of testing and verifying the error detection and fraud prevention controls that should be in place (from Tulenko 2002). While auditing itself cannot directly prevent any security breaches, it can act as a deterrent.

Another reason for auditing is to provide evidence for the reconstruction of a violation. It should be noted that the use of auditing as a deterrent could potentially diminish its success in gathering evidence as the element of surprise no longer exists, and people may therefore make greater effort to cover their tracks.

To ensure audit files are not tampered with, all security relevant events that are audited should be in secure storage. As well as the need for audit analysis tools, the timeliness of some system violation information, such as the illegal access of particularly sensitive information, may require real-time audit notification, in which case there is a requirement for both offline and online audit.

### **4.2 Usability Requirements**

Within our pervasive environment we also have the following top-level usability requirements:

1. If someone is authorised to use the room, their entry and exit to and from the room should be as convenient as possible.
2. If someone is cleared to view particular data they should be able to view it.
3. The ability of an authorised person to escort uncleared person(s) in and out of room, (for example in the case of official visitors, if they are accompanied by an authorised person for demonstration purposes) is a practical requirement.
4. Interaction with devices in the room should be easy and the display should be visually pleasing.

Point 4 is concerned with human factors in a pervasive computing environment. It is important that people using the system feel that its interface is intuitive. Points 1, 2 and 3 are discussed further in the section on Threats and Physical Access Control.

### **4.3 Trust and pervasive computing**

In an environment such as Defence or any other environment where people are working with classified information, there is already a level of confidence that the users of the system are going to act in a responsible way. In some cases this level of trust is supported by evidence such as security checks of users, but in any situation where someone employs a person to do something, there usually is an implied level of trust that that person will act as is expected of them. As we already place such a level of trust in the users of the system, maybe we only need to audit their various transactions. For example, if we trust that people will notify the room each time they enter and exit, there may be no need to enforce this through automation.

In a pervasive environment such as this, because visitors may be escorted in and out of the room there is also a level of trust placed in non-predetermined users of the system. It therefore seems that a pervasive computing environment such as this may need to be "based on trust rather than just user authentication and access control" (from Kagal, Finin & Joshi).

While there is a level of trust placed in the users of our system, the need to automate things like authentication has both security and usability advantages. From a security perspective, automated authentication makes claims of repudiation of events on the grounds that there is no enforcing of entry to and exit from the room harder to substantiate. And from a usability standpoint, if the context of the room is updated to reflect a person's personal working environment or to change the classification of the documents displayed in the room (also a security advantage), based on the person's particulars, automation will save them having to worry about setting up their workspace.

### **4.4 Threats and Physical Access Control**

In any organisation we have two main types of security threat: a threat from inside and a threat from outside the organisation. The inside threat may be a "spy" who has access to the room and wishes to reveal secret information to an enemy (but also includes an employee without malicious intent who disregards security policy and as a result unauthorised disclosure of information may occur), with the outside threat being the enemy, e.g. terrorists. We can mitigate both these threats in a number of ways using computer network related security devices; but we must also recognise that this kind of technology may have limitations and knowing what these are is vital to any security architecture. When we know the parts of the secure room that are most vulnerable to attack we can concentrate on securing them in other, perhaps more traditional, ways. If we cannot have complete trust in any particular area we should at least know its vulnerabilities.

#### **4.4.1 Entering the room**

The most difficult task with physical access control seems to be the identification of people, where we have more than one person entering a room at the same time. When someone enters their biometric, how do we know that

they actually enter the room? One person's biometric print could be used to allow someone different to enter. To avoid this situation we could use a turnstile or two interlocking doors, and have the person re-enter their biometric once in the turnstile or between the doors; but we still have the problem of making sure there is only one person in the turnstile. A simple and effective solution could be having a security officer monitoring a closed circuit TV. The fundamental problem is being able to individuate all people present without them explicitly identifying themselves. In an attempt to find a fully automated solution to this problem, the proposed architecture uses a combination of weight and other biometric technologies. By using weight sensors a persons' room entry weight can be compared with their initial registration weight.

#### 4.4.2 Still in the room

Above, we identify who is in the room by positively identifying who enters and who exits but, keeping in mind our third usability requirement, we may still achieve a high level of security by combining a couple of less intrusive biometrics. For example, face recognition combined with weight sensors. As a person's weight has the potential to change more readily than other biometrics; after initial weight registration if we have strong enough identification on entry we may be able to recalibrate a person's weight each time they enter the room allowing more accurate identification by correlation between a persons entering weight and their exit weight. As the time between visits to the room can be greater than the time between entry and exit, the initial setting up of the persons weight biometric will need to allow a reasonable margin for possible weight loss or gain.

#### 4.4.3 Escorting person(s) in and out of the room

In order to accommodate our high level requirement that there is the ability to escort uncleared persons in and out of the room, our antechamber to the room should know how many people will be entering the room by asking the authorised person (or possibly by using facial recognition). Once it knows, it can then ask all occupants for a voiceprint, face print and weight biometric, as these are all relatively non-intrusive biometrics. These templates can then be compared to a known suspect database. The room context will also need to be updated to ensure that only unclassified information is displayed. On exiting the room, the biometrics are again taken to verify against those taken on entry.

Of course, this requires a level of trust in the people authorised to use the room. If the authorised person's weight is 80kg and the weight biometric identifies it as 220kg, it can refuse entry unless at least one other person is identified. However there may actually be two other people and while face recognition may be of some assistance, the face biometric may not pick up the second person's face if it is hidden. In this case policy may require that only suitably authorised persons, in whom we have a greater degree of trust, are allowed to escort visitors in and out of the room.

#### 4.4.4 Controlled Environment

As the room is a fairly controlled environment, we want our system to prevent people from taking furniture and other devices in and out of the room as they please. The use of a weight biometric combined with machine vision is a possible solution. But because neither of these methods is very fine grained they may miss small things like cameras or PDAs hidden on a person. Even if vision technology were able to successfully identify such devices, unless briefcases, folders and notepads etc were also excluded from the room they may be incorrectly identified.

Machine vision may be suitable for checking that the room antechambers are empty after entry and exit to ensure that no recording devices have been planted.

### 5 The architecture

The security of the room is enforced by the communication channels open to agents within a layered agent architecture. The reason we use agents within our security architecture is twofold: (1) since the agent concept is very familiar (e.g. real estate agent, insurance agent etc.), it is a useful tool for encapsulating distributed biometric devices that perform a particular function; (2) having a system made up of independent components allows us enhanced adaptability. Point two is particularly important when using devices from such an active and varied research field as biometrics.

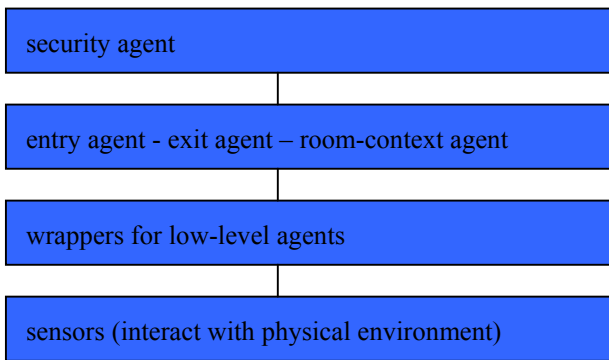
#### 5.1 Integration of Physical and Information security access control

Physical access in and out of the room and access to information once inside the room is by continuous biometric identification coupled with smart-card technology. The architecture uses a number of different types of biometric identification in a complementary manner, the belief being that a higher level of trust in having correctly identified someone can be gained by this. For example, if we have a positive match on a person's iris as well as their voice biometric, it is more probable that they were at that location than if we just have a positive match on their iris.

#### 5.2 Agent architecture

The suggested agents are as follows: *iris*, *door1*, *weight*, *voice*, *token*, *door2*, *fingerprint*, *face*, *speech*, *entry*, *exit*, *room-context* and *security*, with the agent layers illustrated in figure 3. The real time devices, such as the iris scan that interact directly with the physical environment, can be seen as low-level or level 0 agents and the wrappers for these devices that allows communication between agents, such as the *iris* agent, are level 1 agents. The *entry*, *exit* and *room-context* agents, are classed as level 2 agents because they coordinate the lower-level agents; and the *security* agent can be seen as the high level agent in the sense that it is the only agent that communicates between the networks as well as having an overseeing role.

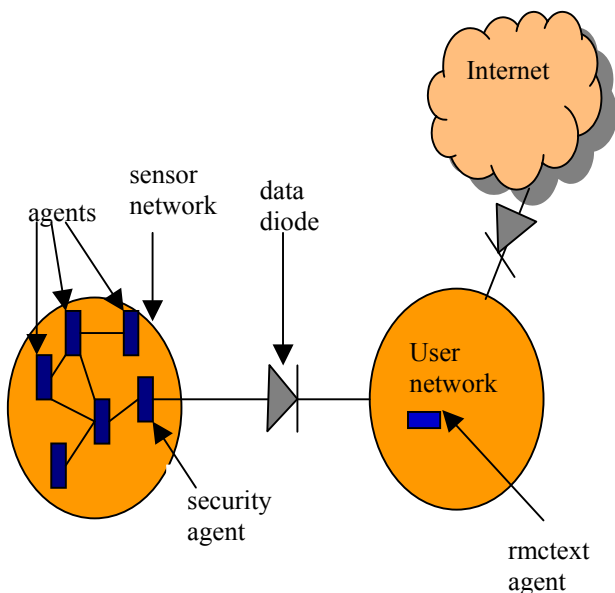
All communication from the sensor network to the user network is via the *security* agent.



**Figure 3: Agent layers**

### 5.3 Data diode

As the sensor network contains all the databases holding the biometric information of users, as well as being responsible for locking and unlocking doors, it needs to be protected from attacks via the user network. To prevent such attacks, a data diode is placed between the networks, only allowing information to travel from the sensor network to the user network as shown in figure 4.

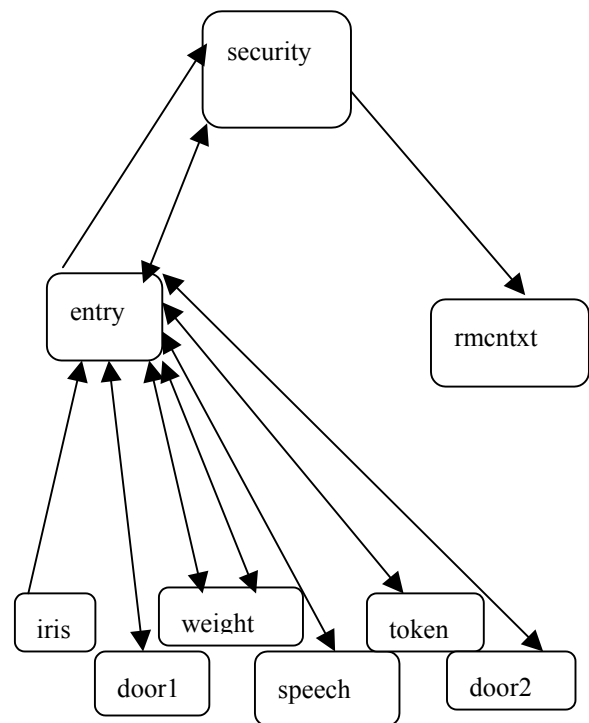


**Figure 4: Security architecture**

### 5.4 Information flow between agents on entering room

The flow of communication between agents and how they interact with each other is crucial from a security point of

view. Figure 5 shows the communication between agents when a person enters the room.



**Figure 5: Communication between agents when someone enters room**

**(I) Entry agent authenticates user - (1).** The iris system scans the person's iris; *iris* agent tells *entry* agent that iris is authorised. **(2).** *Entry* agent notifies *security* agent, *security* agent checks room list to verify person is not already registered as being in room. **(II) Security agent authorises entry to antechamber - (3).** *Security* agent notifies *entry* agent that it is okay to continue. **(4).** *Entry* agent tells *door1* agent to open door. **(5).** Door stays open for a reasonable period to allow entry (*door1* agent should activate a security event if open any longer) and then notifies *entry* agent when it is closed. **(III) Entry agent verifies authentication and registers number and identification of people, before allowing entry to room - (6).** *Entry* agent then notifies *weight* agent to begin processing. **(7).** *Weight* agent notifies *entry* agent with weight details. **(8).** *Entry* agent then notifies *speech* agent with instructions for processing depending on what details it receives from *weight* agent (e.g. if persons biometric is considerably higher or lower than registration weight ask for voice print and face print of anyone else present). **(9).** *Speech* agent sends details to *entry* agent and **(10)** *entry* agent tells *token* agent to allow processing. **(11).** *Token* agent sends person details to *entry* agent, if biometric and token details match, **(12).** *Entry* agent tells *door2* agent to unlock door. **(13).** *Entry* agent notifies *security* agent that person has entered room. **(IV) Context-agent updates room context - (14).** *Security* agent updates list of people in room and sends details to the *room-context* agent, which updates room

context (a person's classification may be an attribute of their biometric or of a separately stored certificate). (15). *Door2* agent informs *entry* agent when it has closed (both *door1* and *door2* agents should have autonomy over activation of security events where local threats are encountered such as the door being chocked open). (V) **Entry agent checks that antechamber is empty** - (16). *Entry* agent tells *weight* agent to begin processing, to check that entry antechamber is empty and if not empty activate security event. (17). *Weight* agent notifies *entry* agent when it is finished so that *entry* agent can continue processing.

The updating of the room context is more significant if we wish to filter information based on the intersection of the clearances of who is in the room (as a stronger method of enforcing the prevention of unauthorised disclosure of information) rather than individually. In the former case the room is forced to consider the relationships between the people in the room; whereas in the later case it may just be a case of announcing someone's imminent arrival thus notifying people in the room, so that they are aware that there are other people in the room possibly not cleared to see the information in their session. In this case, the person may blank their screen or, for stronger security, their screen is automatically locked. In both scenarios, we propose to use SIFTEX, which is a filtering application prototype under development. For example, in a coalition environment if someone new enters the room and either their classification level or nationality differs from all the classification levels or nationalities in the room, then the room classification context is updated, so that if their classification is lower than any in the room, and/or their nationality is different, filtering of information is performed on their classification combined with the intersection of all the different nationalities within the room. Since the security of information in the room depends so heavily on the *security* agent, it is necessary that the *security* agent send still-alive signals to the user network.

## 5.5 Room-Context/Session Agent

Once in the room, the *security* agent uses information provided to it by the *fingerprint*, *speech* or *face* recognition agents (using biometric devices that are attached to workstations throughout the room) to tell the *room-context* agent the person's particulars and the machine they are interfacing with. The *room-context* agent then uses this information to filter information appropriate to the person's level of clearance before it is sent to that particular machine. Each time the *security* agent receives information from one of the low-level agents in this manner, it checks that the person is registered as being in the room and activates a security event if they are not, such as ending all sessions and advising the occupants of the situation. In this way the *room-context* agent is used for such things as logging onto a workstation or opening a session on the large screen.

In the event that we are filtering data based on the intersection of clearances in the room, it may be

necessary that users who already have a session open be given a warning before their current session is ended and a new session based on the changed room context is started.

## 5.6 Flexible Agents

When we conceptualise a community of agents we may expect them to be more dynamic than the agents listed above (e.g. allowing our *security* agent to make decisions about which agents are available to handle sub-parts of a particular task rather than having a commune of tightly bound objects) but it is only recommended that this level of restriction apply during entry to the room. It seems reasonable that we expect our agents that guard entry to the room to offer the highest level of assurance with little independence, giving us an unconditional login process.

Once in the room, our agents can demonstrate more autonomy. There may be flexibility in how the *security* agent identifies someone for a particular session, for example through the *fingerprint* agent or a combination of *fingerprint* and facial identification. It may be that identifying a match on 16 ridge characteristics in a fingerprint constitutes a positive identification in a court of law, but if the *fingerprint* agent returns only 14 matches, rather than reject the person and activate a security event, the *security* agent might ask for another scan via the *speech* agent or alternatively have the *face recognition* agent confirm the person's identification. This would be analogous to the current practice when attempting to log into your workstation, instead of being locked out after the first failed attempt you are given 2 more attempts.

## 6 Other Pervasive Technologies

This section explores the potential of other technologies with respect to security in a pervasive environment.

### 6.1 Vision Technology

As an alternative to the *weight* agent, the use of vision technology was investigated. While machine vision is far from emulating the human eye, in controlled environments it can be more successful than human vision for identifying or recognising an object, as discussed by Whelan and Molloy (2001). One could consider a camera on the ceiling of both antechambers that takes a snap shot once both doors are locked and then counts the number of people present. Increasing the number of cameras in the room would give a more accurate reading. The antechamber should be a reasonably fixed environment, which will assist the use of vision technology in that it will allow the system to compute a background subtraction to prevent background interference when capturing a new image for processing as demonstrated by Brooks (1997). It was initially thought that in such a controlled environment if enough cameras were positioned appropriately to cover all angles and to try and prevent false positives, such as a coat on the floor being recognised as a person, it might be suitable at least for identifying if there is more than one person. The system may also be assisted by posting a

sign requesting that occupants remove their hats and directing a person stand a particular way (legs together and arms by side), to avoid false negatives.

Taking the aforementioned into consideration, the machine vision component does not look very friendly for the user and does not address our top-level usability requirement of allowing the escorting of visitors. While the room's antechambers are reasonably constrained environments, the machine vision system has to be told exactly what to look for, so apart from ensuring there is no background noise separate from the person(s) in the antechamber (if there is more than one person the noise of each persons image will affect the other), we also need to give the system a template of a person or a person's head. However, because there is much variation between people's shapes, current machine vision technology is not considered suitable for use in this area.

## 6.2 Paper documents

To allow paper copies in the room, we need to be able to identify and track individual documents in such a way that if either the tracking system or document id is tampered with (i.e. trying to remove it), a security event is activated, thus preventing the document from being taken out of the room. We also need to prevent or register copies that are made of the document and to bind each document to a particular authorised person each time it is handled. As a person is only allowed to interact with a soft copy which they are authorised to view, if they print this copy it may be possible to bind their biometric to the document tag, so that if the document is not in the safe or not on the person a security event is activated. This might mean that a biometric agent also has a printer associated with it and that the distance between the document being printed and the biometric is minimal. Motorola had been developing a product called 'BiStatix', a smart label that attempts to combine document tracking and identification to prevent copying of marked documents. This showed some promise in providing a solution to the problem of securing paper documents but in 2001 Motorola closed down this project (from Schaumburg 2001). BiStatix was a form of radio frequency identification where the traditional RFID antenna coils are replaced by carbon ink electrodes that can be printed on paper.

## 7 Summary

Like all new technologies pervasive computing and biometrics are far from perfect. Many biometric devices use proprietary techniques in the storage and exchange of data (though institutes such as the National Institute of Standards and Technology are attempting to reach industry consensus on common biometric exchange file formats). Most biometric devices lack any sort of formal accreditation and manufacturers must be trusted that their false acceptance and false rejection statistics are accurate. Having said this some biometrics clearly emerge to be more secure, though usually also more intrusive, while others that are less secure are more user friendly (see Jain et al 1998). Because the user-friendly aspect of a pervasive environment is paramount, we cannot ignore

this fact when looking at biometric devices. Apart from this, a face biometric device, which may not be as trusted as an iris biometric device, would be more suited to surveillance.

As we have noted when it comes to securing a pervasive environment there are some areas where technology seems a long way from being able to provide a solution. The point is that the availability of these devices for use in a pervasive environment, where we have the coming together of two different security domains, should not make us forget that there is no silver bullet when it comes to security. We must not let a technology such as biometrics that enables us to more accurately identify someone in the physical realm or PKI that allows us to be more certain of who we are dealing with in cyber space, cause us to overlook the more fundamental problems that are encountered when attempting to build a secure environment.

In a traditional environment where physical and information security are used, a typical scenario might proceed as follows: When you enter the front door or gate of your place of work you have a key or swipe card that gains you entry (something you have), you enter your office without being questioned because people recognise your face (something you are) and you then login to your computer or unlock your safe with your password (something you know). These three traditional forms of identification haven't changed much - all that is different is that the something you are is now automated and used for authentication in a way that more closely complements the other forms of authentication and in places where authentication was not previously enforced (e.g. exiting room). This more closely coupled form of authentication, using different types of identification, is still in keeping with the defence-in-depth principle but, by more closely binding the various forms of identification in a way that provides continuous authentication, the system becomes more trusted.

This paper has investigated the issue of security in a pervasive computing environment, as well as suggesting a possible architecture within this environment. Access to information in this environment is via authentication and authorisation, using a combination of biometric and smart card technology, coupled with the use of a document filtering prototype application. A person must first be authenticated and then access to information is granted depending on what their attributes permit them to see. Within our environment, we require every bit of information manipulation that is executed to be undeniably linked to someone who can be identified. This may not seem that onerous a task, but in the age of Information Technology and pervasive computing it is still non-trivial.

## 8 References

BLADES, A. (1997): Principles of Security and Risk Analysis - online journal at: <http://www-some.cowan.edu.au/units/scy1102/website/default.html>. Accessed 24 August 2002.

BROOKS, R.A. (1997): The Intelligent Room Project. *IEEE journal Cognitive Technology*, 1997. Humanizing the Information Age. Proc. Second International Conference **2**: 271-278.

JAIN, A.K., PANKANTI, S. and BOLLE, R (1998): *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers.

KAGAL, L., FININ, T. and JOSHI, A. (2001): Trust-Based Security in Pervasive Computing Environments. *IEEE journal* **34**(12):154-157.

MATSUMOTO, T., MATSUMOTO, H., YAMADA, K. and HOSHINO, S. (2002): Impact of Artificial "Gummy" Fingers on Fingerprint Systems. Proc. SPIE **4677**: Optical Security and Counterfeit Deterrence Techniques IV.

McCARTHY, J and THREDGOLD, J. (2002): Modelling smart security for classified rooms with DOVE. This paper appeared at the Workshop on Formal Methods Applied to Defence Systems, Adelaide, Australia. Proc. Conferences in Research and Practice in Information Technology, Adelaide, Australia, 12, L.M. Kristensen and J. Billington, Eds.

MINSKY, M.L. (1986): *The Society of Mind*. New York; Sydney, Simon & Schuster.

National Institute of Standards and Technology: Accessed 20 August 2002.

RADCLIFF, D (2001): companies move to combine physical IT security efforts. From COMPUTERWORLD online journal. Accessed 24 August 2002.

SCHAUMBURG, I. (2001): Press Releases in Transponder News – online journal at: <http://rapidftp.com/transponder>. Accessed 23 August 2002.

TULENKO, P. (2002): Small business: Why audit? in [naplesnews.com](http://www.naplesnews.com) at: <http://www.naplesnews.com/02/05/business/d329109a.htm>. Accessed 21 August 2002.

WHELAN, P. and MOLLOY, D. (2001): *Machine vision algorithms in Java: techniques and implementation*. London, Springer.