Security, Privacy and Trust Issues in Smart Environments

P A Nixon, W. Wagealla, C. English, S. Terzis

The Global and Pervasive Computing Group
Department of Computer and Information Sciences
University of Strathclyde, Glasgow, Scotland.
{Paddy.Nixon@cis.strath.ac.uk}
http://www.smartlab.cis.strath.ac.uk/

1 Introduction

Recent advances in networking, handheld computing and sensor technologies have driven forward research towards the realisation of Mark Weiser's dream of calm and ubiquitous computing (variously called pervasive computing, ambient computing, active spaces, the disappearing computer or context-aware computing). In turn, this has led to the emergence of smart environments as one significant facet of research in this domain.

A *smart environment, or space,* is a region of the real world that is extensively equipped with sensors, actuators and computing components [1]. In effect the smart space becomes a part of a larger information system: with all actions within the space potentially affecting the underlying computer applications, which may themselves affect the space through the actuators. Such smart environments have tremendous potential within many application areas to improve the utility of a space. Consider the potential offered by a smart environment that prolongs the time an elderly or infirm person can live an independent life or the potential offered by a smart environment that supports vicarious learning.

So smart environments, by definition, are designed to exploit rich combinations of small distributed sensing/computational nodes to identify and deliver personalized services to the user when they are interacting and exchanging information with the environment. Within such environments there is a high demand on solutions to users to be secure, private and trustworthy. Security describes the cryptographic techniques used to secure the communications channels and required data. Privacy in this context encompasses reasoning about trust and risk involved in interactions between users. Trust, therefore, controls the amount of information that can be revealed, and risk analysis allows us to evaluate the expected benefit that would motivate users to participate in these interactions. In this chapter we endeavour to survey selected work in these three disparate, but related, areas and to situate them in the unique problems of smart environments

In particular this domain of technology has at its core the collection of assorted contextual sensing information, such as the computers context, user context, and physical context [2], that is subsequently used for the delivery of personalised services. A typical example of context gathering would be the placement of sensors in rooms and offices to enable the collection of data such as location of the smart space inhabitants. The vast amounts of personal information collected by such systems has led to growing concerns about the security, privacy and trustworthiness of such systems and the data they hold. This is a core problem as users concerned about their private information are likely to refuse participation in such systems; and so slow or stop the deployment of smart environments. Therefore, in this chapter we consider the broad issues of security, privacy and trust in smart environments. We start by considering the characteristics that make smart environments unique in the requirements they place on security, privacy and trust.

1.1 What makes it different?

In [3] the following question is asked in respect of privacy – *what makes ubiquitous computing any different from other computer science domains.* Langherich goes on to identify four key motivators:

1. **Ubiquity:** The infrastructure will be everywhere consequently affecting every aspect of life.
2. **Invisibility:** The infrastructure will be cognitively or physically invisible to the user – the user will have no idea when or where they are using the *computer*.
3. **Sensing:** Input to the ever-present invisible computer will be everything we do or say, rather than everything we type.
4. **Memory amplification:** Every aspect of these interactions, no matter how personal, has the potential to be stored, queried and replayed.

The descriptions of these four elements show how ubiquitous computing, and smart environments, will be characterised by massive numbers of almost invisible miniature sensing devices that can potentially observe and store information about our most personal and intimate experiences. It is worth noting that these observations are not merely an amplification of the current concerns of Internet users with desktop computers. These observations show the deep societal impact that such technology will have.

From a technological perspective they also highlight a fundamental change. In most areas where security, privacy and trust are investigated we can clearly identify the intended interaction end points. In an e-commerce transaction it may be ones web browser and the shops web site; in a targeted online communication it may be between two or more specific people. However in a smart environment the interaction end points could simply not be cognitively or physically visible; in essence the user may have no idea that they are engaging in a computer –mediated communication. In these situations a password spoken aloud in an empty room could be a security hazard. We can imagine more personal and intimate situations in everyday living that would be equally uncomfortable and which would destroy our privacy or undermine our trust.

In addition to these operational characteristics there are a number of technology related characteristics that compound the problem. A smart environment [4] can be viewed as a composite space made from many individual objects. These objects will be either fixed or mobile and for our purposes can be broken down into the following categories:

- **Fixed sensors:** These are items that do not have computational or processing ability but that have state, which can be ascertained using sensors[1]. Examples go from simple door and window sensors (that can be open or shut), lights sensors (on, off or dimmed), and thermostatic controls to rich sensors such as video surveillance. Such fixed sensors are used to provide a given environment its core *sense* of its surroundings.
- **Mobile sensors:** We differentiate fixed from mobile sensors for two reasons. Certain sensing must be done on the move – such as gathering locational information from GPS-like sensors. Secondly, an individual or device may want to distinguish the sensed information they gather from that supplied by a given environment.

[1] http://www.sensormag.com has a comprehensive list of off-the-shelf sensors.

- **Fixed computing elements:** This set of elements comprises of objects which have processing and data storage ability but no method of moving. The more obvious examples would include servers, printers, desktop computers, coffee machines, photocopiers, air conditioners, etc.
- **Mobile computing elements**: These objects exhibit the properties of fixed computing entities but also have the freedom of movement. Examples include mobile communicators (phone/pda), intelligent wheelchairs, mobile personal computers, vehicles, and task specific robots.

Campbell et al [5] also identify a similar set of issues and characteristics. We have highlighted these four types of objects as these emphasise the contrasting elements of fixed computation with the mobile computation and sensing that are now core, rather than peripheral, elements of the problem. Moreover, in identifying these characteristics we hint at a fundamental part of the technology problem; in any given smart environment no one part of the systems has full knowledge or has full control over what is stored, sensed or communicated. In the following sections we will consider each aspect of security, privacy and trust in the light of these observations.

2 Security

2.1 Motivation

The motivation for security in smart environments is identical, at some level, to the motivation in all other computing systems. Simply put, to ensure that information is not stolen, modified or access to it denied. The recurring argument we present in this chapter that differentiates smart environments is the massive diversity of information that can now be misused and thus needs to be protected. In these environments, the carrier of a device with sensing and wireless network capabilities can become an unwitting spy by carrying information from one environment to another or by collecting information about third parties unintentionally. A comparable observation is also made in [6] about the increased context of operation for smart environments; it referred to as the *trust context space* (Figure 1). In subsequent sections we address design and good practice aspects for respecting privacy, and decision process to identify trustworthy interactions. However, in this section we review some basic principles of security that must underpin the whole process.

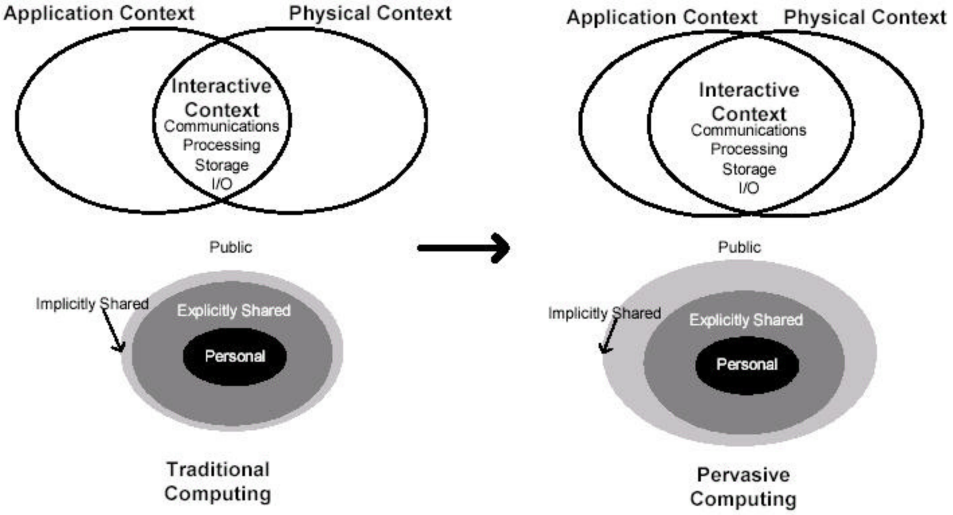

Figure 1: Trust Context Space [6]

2.2 Definitions

Security is not merely about cryptography [7,8], but is about assessing the risk of bad things happening in a given environment or situation and developing safeguards and countermeasures to militate against these risks. In this chapter we have taken a couple of security concerns, privacy and trust, and extracted them as important elements in their own right. However, security encompasses these and other issues. In its broadest definition security is widely accepted [7] to cover the three main properties of Confidentiality, Integrity, and Availability. Confidentiality is concerned with protecting the information/service from unauthorised access; Integrity is concerned with protecting the information/service from unauthorised changes; and Availability is concerned with ensuring that the information/service remains accessible. In the following section we consider each of these aspects of the security problem and highlight a very small subset of the technologies. The interested reader is referred to [7,8] for broader coverage of technologies and the state-of-the-art in security in pervasive computing respectively.

2.3 Security in Smart Environments

Confidentiality and Integrity are essentially about encryption and decryption. Smart's book on cryptography [8] provides a thorough and detailed perspective on the many and varied cryptographic techniques. Encryption, decryption and hence authentication in a smart space are complicated by the characteristics of the environment. Key to these environments is the largely decentralised and dynamic nature of the principals[2] and their interactions, due to the transient nature of relationships among principals roaming between administrative domains. For authentication, Public Key Infrastructures (PKI) rely on a certification authority (a trusted third party) hierarchy that can verify the principal carrying the key is the owner of the key. The rigid structure of this fixed hierarchy of authorities has limitations for a decentralised environment where two entities' certification hierarchies may not intersect. An approach to solving this problem originated with Pretty Good Privacy (PGP) [9], a tool intended to provide the general public with reliable email cryptography by removing the need for hierarchies of certification authorities (CAs). The approach is a decentralised 'web of trust' where individuals sign the key certificates of others, recommending that the key in the certificate belong to the person stated. These signatories, called 'introducers', are allocated specific trust levels with regard to their status as introducers, allowing for fine-grained evolution of the 'trust in introducer' relationship. Chains (possibly multiple chains) of certificates can be formed based on these introducer relationships between entities, thereby propagating trust in the validity of the key in question from one end of the chain to the other. These intersecting chains of trust relationships form the web of trust. Local policies are defined in terms of the quantity of each trust level required before a key certificate is considered valid. For example, two fully trusted introducers and one marginally trusted introducer claiming the validity of a key certificate may suffice to indicate that key is valid. In this sense, each of these introducer trust relationships constitutes a piece of evidence or a recommendation for the validity of a key.

It is important to note, as pointed out by Germano Caronni [10], that although the web of trust approach is useful as a more generic solution than the hierarchical approach, it is potentially more difficult to manage. As a more dynamic approach to authentication, there are no hard and fast rules regarding the formation of individual relationships. In PGP, this is done offline through user intervention, a principle at odds with Mark Weiser's dream of 'calm

[2] Principal is the term used in security to signify the entities (people, agents, devices…) of interest.

technology'. The provision of automated reasoning capabilities is hampered by the fact that portable devices may have limited processing and storage capabilities, a factor that also affects the ability to provide suitable cryptographic security for confidentiality. In [11] it is also identified that the web of trust does not solve the problem of security for smart environments. In these environments there may be no immediate recourse to the global infrastructure to establish trust in the introducers and hence all introducers drop to a base trust value of unknown. Furthermore, as Phil Zimmerman, the creator of PGP, points out, "Trusting a key is not the same as trusting a key's owner", implying a shortcoming of PGP and PKIs; that trust in the identity of a principal is not the same as trust in that principal's behaviour. This is a key issue in environments that may be inhabited by principals unknown to the system. These are open problems that highlight the need for more dynamic models of security/confidentiality that better reflect the properties of smart environments.

Security has traditionally focused on the integrity of messages in transit. Many techniques for this have been developed, and despite mobile device limitations, cryptography to all intents and purposes deals with this problem. While this obviously still holds for any smart environment, there are additional problems introduced by the increasing use of wireless technologies within smart environments [12]. With these technologies being used for multiple access and dynamic connections, it becomes much more difficult to prevent eavesdropping on communications. Coupled with this level of physical insecurity of the communication medium, many wireless protocol implementations fail to implement the security features of the protocol specification. Even when these are implemented properly, the security protocols are not very resistant to attacks, as documented in work on Bluetooth's wireless security [13]. Concerns arise both for the security of wireless networks against attack from roaming devices and the security of the roaming devices against a wireless network capable of malicious behaviour. Furthermore, tracking malicious users becomes difficult in the case of mobile devices. Additional problems arise as computing becomes more invisible, and it becomes more difficult to ensure it is fulfilling the security needs of a user that may be unaware of its existence. Indeed, users are increasingly unaware of the security implications of such technology. To address these concerns, security configuration should be removed from the user as far as possible, to avoid misunderstood security configurations causing problems for smart space integrity, allowing devices to be compromised.

Further security issues are evident in terms of the integrity of the devices themselves; the devices are mobile and may arrive in a given smart environment from an unknown domain. The problem arises that even if this device has been seen before it may have been altered during its absence. Theft of a device implies theft of the identity that the device represents, and as such, a known device may behave very differently when controlled by a different and possibly malicious user. Consequently no claims can be made about the device's integrity. Furthermore, there are concerns about the integrity of sensors. While cryptographic measures can be taken to protect data between the sensor and application, preventing a malicious user masquerading as a sensor, the problem of protection against false information entering the sensor itself must be addressed. This type of attack might be carried out much more easily if measures such accurate biometric authentication are not used.

Availability also suffers from new problems in the smart environment domain. As well typical denial of service attacks that might affect the communication channel Stajano [7] observes that resource limitations on devices, such as limited battery power, could be the target of *sleep deprivation*. In this attack the server or device maybe kept awake until battery power is dissipates completely. Intermittent service failure is likely on wireless connections, and many wireless protocols do not require re-authentication [12], such that short denial of service attacks may lead to man in the middle attack vulnerabilities.

It should be clear from the discussion in this section that there is a need for new security mechanisms to provide a more dynamic view of security for the dynamic environments under consideration here. There are some promising approaches being considered in this area. In contrast to static access control lists, these approaches essentially classify users into categories based on certain properties, separating security policy from the allocation of users to categories, and simplifying the policy definition. An example of this is Role Based Access Control, where traditionally users are categorised according to their position in an organisation's hierarchy. One approach that has been suggested to extend this paradigm into the smart environment setting is that of Covington et. Al. [14]. Instead of using organisational roles, they introduce the notion of 'environmental roles', categorising users according to security relevant environmental context, such as location and time, in conjunction with user information. Thus policies can vary dependent on, for example, which other users are in the same location, or access requests outwith normal working hours. Another similar approach proposed by Mostéfaoui [15] is the use of adaptive, flexible smart security policies, where contextual information is used as a constraint for real-time re-configuration of policies. The user's preferences can be taken into consideration, but the user need not be directly involved in complex security decisions. These approaches provide access control, while permitting access from any location, thus supporting user mobility. Furthermore, they demonstrate that even given the security and privacy implications of a sensor network, it is possible to use the contextual information that they provide to enhance security for smart environments.

A very promising approach, which we concentrate on in the later sections of this chapter, is that of trust management, and the application of trust and risk analysis to security problems in dynamic and decentralised environments comprising unknown entity interactions. We will provide a detailed analysis of this approach later in the chapter.

3 Privacy

3.1 Motivation

As already discussed in the introduction to this chapter the very features that allow smart environments to be personalised and dynamic are the features that contribute to the privacy problem. A smart environment will collect data from sensors and from users. The manner of collection will not necessarily be obvious or active. The potential for collection and misuse of information is massive. As pointed out by Campbell [5] – this information could be used by the malicious or simply curious, for instance, to track and stalk unsuspecting users. A sentiment echoed in [3] when we are reminded of the Orwellian Big Brother Nightmare. Because of this the demand for privacy is obvious – perhaps even more so than for security or trust. Without notions of individual privacy users will simply not engage with the technology. Research in this area is very important for smart environments where even previous solutions for privacy in online systems are inadequate.

3.2 Definition

According to Alan Westin [16] "*privacy*[3] *is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information is communicated to others*". Privacy on its own is about protecting users' personal information. Considering the advances technology in ubiquitous computing, the concern over privacy is greatly increased. The challenging question, which researchers have begun to tackle recently is how to control and manage users' privacy. Privacy control, as the term states, encompasses the notion of privacy and the notion of control or management. It not only relates to the process of setting rules and enforcing them, but also to the way privacy is managed/controlled adaptively

[3] The word *privacy* originates from the latin word *privatus*, which means "apart from the public life".

according to changes in the degree of disclosure of personal information or user mobility from one smart space to another. The main emphasis is that any good privacy solution should combine these two notions as control is about justification of privacy and plays a role in the management of privacy [17].

As observed by Langeheinrich [3], the issues of privacy have been addressed in a number of domains. Langeheinrich [3] identifies the significant recent historical aspects of privacy showing its evolution as an issue for public concern from early arguments of privacy in the 19th century, notably by Warren and Brandeis [18], to constitutional and legal impact in the late 1970's. He also points to the key open issue in privacy – information privacy. Information privacy is at the core of the privacy problem for smart environments. Westin [17] identifies this problem and refines some principles of fair information practices, and these are summarised as [3]:

1. **Openness and transparency**: No secret record keeping.
2. **Individual participation**: The subject should be able to see the records.
3. **Collection limits**: Record collection should be appropriate for the application.
4. **Data quality**: Record collection should be accurate and relevant to the application.
5. **Use Limits**: Records should only be used for specified purposes and by only by authorised people**.**
6. **Appropriate security**: Reasonable efforts should be made to secure the records.
7. **Accountability**: Record keepers must be accountable.

These principles perfectly cover the smart environment problem space. There is only one minor modification to be observed. These principles have an implicit assumption of one-way interaction (system records user). This is not the case in smart environments were all parties in the process are both record keepers and the subject of record keeping; although this does not change the validity of these seven principles. Furthermore, there is an issue of "awareness" from the user point of view, in the sense that users should be aware about the availability of interactions.

3.3 Privacy in smart environments

Privacy has been studied in the context of the Internet, with the most evident technology being the platform for privacy preferences (P3P) [19]. P3P aims to enhance user control by the design of an open standard for a given website to describe how it uses personal information it collects during a session. This then allows P3P enabled browsers to interpret this machine-readable description, thus providing the user with a way of making decisions about how they use the site by reference to their own *privacy preferences*. This technology focuses on the service provider annotating their *information* privacy policies and making these available. In addition to the standardization and adoption of P3P, there is a recent trend towards developing privacy-enhancing technologies, which enhance user privacy management. These also provide solutions to the related problems of security and privacy, enabling information collectors and users to manage personal privacy in a flexible manner. The main concept behind these solutions is to use technical and organisational concepts to protect users' personal identities. Cryptographically this is achieved through the use of digital signatures. Such solutions as P3P and privacy-enhancing technologies are aimed at facilitating control of privacy concerns in e-commerce, online systems, and Internet browsers. So far, these technologies have not been successfully applied to smart environments, in part due to the bi-directional relationships between multiple principals and the difficulty of balancing the privacy requirements of all principals with the functionality of the smart space. This highlights a fundamental problem with privacy (and security in general) that is also observed in [3]. Namely, we cannot achieve total privacy in any given system. It also identifies that openness is the only way forward in developing a generic privacy infrastructure.

With this in mind Langeheinrich [3] outlines a number of privacy guidelines for the design of ubiquitous computing systems (*sic* smart environments) inspired by the Westin's principles. In describing these, rather than focus on the malicious invasion of privacy, he focuses on the more typical everyday aspects of accidental invasion of privacy.

3.3.1 Notice

From a very human perspective it may simply be sufficient to make the user aware of the existence and activity of a smart environment. By announcing, or giving notice, to the user in a clean open manner we can devolve many of the privacy decisions to the user; which is the main aim in any case. This is essentially the approach taken in the P3P project. A P3P compliant node announces its policies through a policy specification located at a well-known place. Such a service in a smart environment would have to include not only the environment policies but also the device policies (covering the fixed and mobile entities) because mobile devices may be collecting data that will leave the domain of control of the specific smart environment. It seems obvious that such an *awareness infrastructure* is a base line technology for smart environments.

3.3.2 Choice and Consent

As pointed in [3] legislation in some domains requires that explicit consent be obtained from a user before data is stored. Many of us, depending on our country of residence, never give any thought to the fact that we have consented to the logging of our web activity or email traffic in the work place. However as already identified, the potential intrusiveness of the sensing smart environment requires more careful consideration. This second guideline is simple in essence: having notified the user of the activity in a space, give the user a choice whether to engage and if they do interact seek their consent. Tavani [20] stated that consent is a means of control that manages privacy and justifies what without it would be an invasion of privacy. Choice and consent are the main aspects of individual control and they define a necessary trade-off in the human interaction with the smart environment. The premise of smart environments is *invisible* technology and *natural* interaction. But to answer the users privacy concerns we have to make them *less invisible* and *less natural.*

3.3.3 Anonymity and Pseudonymity

An often-used solution to circumvent this trade-off and avoid seeking explicit consent is to provide mechanisms to hide or obviscate the identity of a user. This guideline argues for offering anonymity but not mandating it. The problem encountered in smart environments is that the techniques used in the Internet context to provide anonymity[4] will not suit the highly dynamic, real-time world activity. Moreover, the devices themselves may not have the computational power or network complexity to support such techniques. One system that addresses aspects of this is the Mist service of GAIA [5]. Finally, anonymity is again a trade-off in the privacy debate as it may inhibit one of the core aims of a smart environment – to provide personalised interactions.

3.3.4 Proximity and Locality

[4] http://www.anonymizer.com

This guideline corresponds to the notion of filtering and multicasting in network communications; only distribute announcements of data or sensors to the interested parties that match some rules. The rules in this case are distance metrics from the source. In doing this the guideline is suggesting a common sense optimisation of the pervious three guidelines.

3.3.5 Adequate Security

The obvious answer to many aspects of privacy – encrypt the data in a manner that enforces the *provider's* privacy preferences. However, this again is a difficult trade-off. Simple, low power devices simply will not be able to use robust encryption techniques because of the computational overhead. This guideline sensibly encourages the proportionate use of encryption in a given environment.

3.3.6 Access and Recourse

This guideline echoes the Westin's principles 3, 5, 7, namely collection limits, use limits, and accountability. Essentially it is a process and purpose guideline, rather than a technology guideline, which encourages good practice in the collection and dissemination of collected data or records.

In [21] a broadly similar set of guidelines are described. Interestingly, these guidelines draw out the user focus very strongly and one additional element. The notion of *making risky operation expensive* makes explicit the risk assessment that happens implicitly in most, if not all, interactions. This key point is echoed in the trust community and revisited in section 4.

To summarise, this section has taken a guideline perspective on privacy rather than a technology implementation perspective. Essentially, although there are examples of privacy technologies in ubiquitous computing in general [5,21,22,23,24], these are at an early stage and but on careful inspection embody elements of the guidelines above.

4 Trust

As already identified (in section 1.1) mobile entities in a smart environment benefit from the ability to interact and collaborate in an ad-hoc manner with other entities and services within the environment. Such entities and services may be from unfamiliar administrative domains and therefore be completely unknown *a priori*. To safely take advantage of the whole range of possibilities such an environment creates it is essential to provide support for secure autonomous decision-making by its constituent entities. In such systems, spanning multiple administrative domains, autonomous operation is an essential characteristic of entities that cannot rely on specific security infrastructures or central control to help in security related decisions. Entities will have to deal with unforeseen circumstances ranging from unexpected interactions to disconnected operation, often with incomplete information about other principals and the environment. While security technologies such as cryptography can protect data and privacy concerns can be addressed, we are still left with the problem of deciding when a trust relationship between two or more principals should be initiated.

We take the view that the process of decision-making for the principals involves the estimation of likely behaviour; not explicitly catered for by traditional security measures that focus on the identification/authentication of principals involved in an interaction. In addition to this unsuitable focus on identity, the hard coded approach to centrally managed security domains is inflexible for environments with unpredictable composition. The responsibility therefore falls to the entities themselves to make security-related decisions, for example to protect their resources from misuse or ensure payment is received for service. Trust management attacks this part of the security problem - the process of decision making within a smart environment [11].

4.1 Definition

Beyond the basic dictionary definition, trust is notoriously difficult to define with definitions challenging philosophers, psychologists and sociologists. In his seminal thesis, Marsh [25] examines many of these perspectives and determines certain generalities and principles of trust, in a step towards his goal of a computational model for trust.

Firstly, trust is subjective and situation specific, based on observations made by an entity and evidence made available to the entity within a particular situation or environment. Secondly, trust is inherently linked with risk, such that higher risk means co-operation is less likely to occur, although the benefits of interaction are often worth the risk. This presupposition of risk is perhaps what differentiates trust from confidence or assurance. Thirdly, Marsh identifies trust as *intransitive*; if A trusts B and B trusts C this does not necessarily imply A trusts C. This however does not rule out the possibility of the transfer of trust information. It merely states that trust is not implicitly transitive, thus when passing information, it is important to be sure that any trust in the information is explicit. The idea of the complex evolutionary nature of trust is also speculated on, in that trust is self-reinforcing such that above a threshold, trust will not decrease below that threshold and below a threshold, trust will not increase above that threshold.

McKnight et al [26] define six trust-related constructs, which capture significant portions of the conceptual meaning of trust and help differentiate between trust and its consequences. These constructs are Trusting Intention, Trusting Behaviour, Trusting Beliefs, System Trust, Dispositional Trust and Situational Decision to Trust.

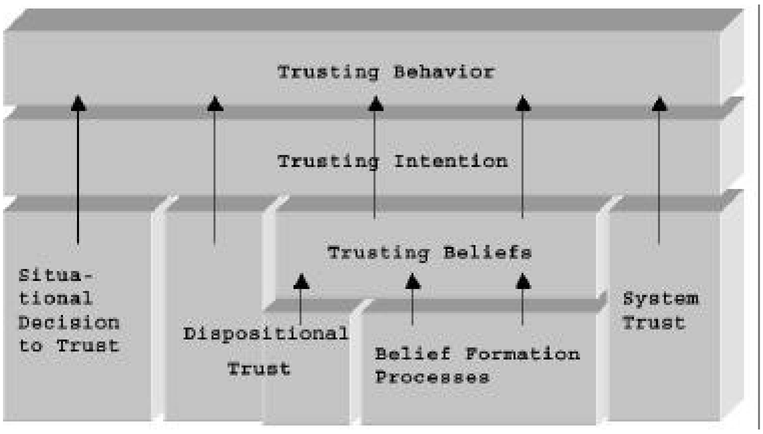

Figure 2. McKnight and Chervany’s Six Trust Constructs and Interactions [26]

The diagram in figure 2 shows how the constructs are related to one another such that beliefs lead to intentions, which in turn manifest in behaviours or the taking of the trusting path in a decision situation. The view is taken that belief in another is based on benevolence, honesty, competence and predictability, forming a solid foundation for trusting intention. From a system point of view it is therefore necessary to observe such characteristics to provide information to the formation and evolution of such trusting beliefs. Predictability here again implies the necessity for risk to be present before trusting is necessary, that perfect information is not available to base a decision upon. Important aspects of trust are included in the Situational Decision to Trust, the Dispositional Trust and System Trust. System trust is the belief that the proper system measures are in place to encourage successful interactions, such as monitoring and dealing with improper behaviour. Dispositional Trust relates to an entity's general expectations of the trustworthiness of others and should be consistent across a range of situations and entities. The disposition of an entity is an interesting idea in terms of trust dynamics also, and might be used to determine how much an entity is affected by the available evidence. The Situational Decision to Trust construct highlights the situation specific nature of trust and the formation of a trusting belief in relation to a specific entity. The constructs are deemed to have heuristic value rather than dictate a specific definition of trust itself, by providing a means to discuss trust across a wide range of situations.

Other work by McKnight et al. [27] highlights that many of the definitions of trust in the literature are not explicit about the dynamic aspects, such as the formation of trusting relationships, instead focussing on what trust is used for in a static fashion. The paper focuses on the initial meeting between two parties that are dependent on one another, before they have interacted and built up experience between them. At first, interaction is supported by dispositional trust (particularly through lack of other support), a situational decision to trust (perhaps irrespective of beliefs, because there is no other choice), system trust and categorisation and illusionary mechanisms. Categorisation and illusionary mechanisms underlie trust through their effects on trusting belief. In a new relationship, the authors claim that three types or categorisation can occur; unit grouping (grouped due to common goals), reputation categorisation (regarding the individual or group) and stereotyping (general biases). The authors claim that human trust is not only based on rational mechanisms, but also on illusions when information and logic to support categorisation is not available. As such, a high level of overconfidence (not justified by the available evidence) about an entity may exist, if we have great need of their help. While the paper makes it clear that trust formation can be supported in many ways, it also points out that initial trust can be fragile and that if experience and observation proves the initial trust incorrect, it may be rapidly revised downwards. The authors further argue that trust is emotional and modelling an emotional concept is not well understood. For this reason it may prove more suitable to attempt to model the behaviour of trust [25] rather than trust itself when considering trust in smart environments.

4.2 Trust management in smart environments

Matt Blaze et al. [28] define trust management as "a unified approach to specifying and interpreting security policies, credentials and relationships that allow direct authorisation of security-critical actions". In such trust management systems, trust is viewed implicitly through the delegation of privileges to trusted entities via the use of credentials or certificates, which can be chained to represent the propagation of trust between entities. Examples of this type of trust management system are Blaze et al's PolicyMaker [28] and its later incarnation, Keynote [29], applications that bind a key directly to access rights, moving away from identity-based certificates and static access control lists. Requestors of a service in a smart environment can prove directly that they hold the correct credentials to authorise the requested service, integrating specification of policy with key to privilege binding. Polices and credentials (assertions) are application specific, essentially autonomous programs that do not communicate with or depend on one another or externally defined data structures [30]. These systems appear much like a database query engine to applications, accepting input of local policy statements, sets of credentials and descriptions of the proposed actions. These are evaluated by a compliance checker [31] to provide a yes or no answer or conditions to be met before proceeding, or in the case of Keynote, an application-defined string for flexible decision making capabilities.

There have been extensions to this model of trust management. For example, the REFEREE Trust Management System [32] places all security-related decisions under direct policy control, including evaluation of compliance with policy. The dynamic loading of new credentials is made possible by making a trust management decision about the downloaded code. This allows credential discovery mechanisms to be developed, increasing the applicability of this approach to smart environments, by seeking the necessary credentials to support access to some service. Lalana Kagal et al's work on security in ubiquitous computing [33] extends trust management with the notion of conditional delegation (imposing constraints), negotiable delegation, prohibition and delegation requests, to improve the evolutionary capabilities of trust relationships. Trust negotiation [34] takes trust management a step further by allowing the bilateral exchange of credentials between the negotiation participants as required to progress towards successful completion of the negotiation. The response to a request will communicate the required credentials to achieve the next step of the negotiation. Measures should be in place to allow credential chain discovery if locally cached credentials do not satisfy policy. Li and Mitchell [35] have developed the RT role based trust management framework for large decentralised systems, combining role-based access control with trust management through a logic-programming approach based on Delegation Logic [36]. RT also incorporates credential chain discovery [37] and uses a goal-directed evaluation procedure for compliance checking and trust negotiation. Cross-domain vocabulary agreement ensures the correct permissions are delegated, by globally uniquely identified Application Domain Specific Documents, declaring data types and role names (termed a vocabulary), allowing strongly typed credentials and policies, supported by a typed credential storage system.

In summary, all of these credential-based systems described in this section provide valuable insights into trust managements, and are useful in their own rights, although not for the type of smart environments of interest here. Despite the advances outlined above, the systems are not flexible enough for general-purpose trust reasoning, and basically describe measures for the exploitation of trust relationships for distributed security policy management. The fact that policy is evaluated with respect to delegation credentials means that if the necessary credentials cannot be discovered, the access cannot be granted. This is a real problem in an environment where unknown mobile entities cause only partial views of the system to exist and we cannot rely on a fixed security infrastructure. Furthermore, the implicit trust relationship established via credentials relies on entities with explicit knowledge of the trust subject to delegate privileges, assuming they have the authority to do so. There is no consideration of how relationships at this level are formed and at some stage this comes down to administrative intervention, which is not consistent with calm computing. Given the limitations of credential based trust management for our environment of interest, we advocate the use of trust management paradigms, which more closely mimic the nature of human trust, based on historical evidence evaluated from a subjective viewpoint.

4.3 A new approach to trust based security in smart environments

Based on the properties of trust discussed in section 4.2, it is clear that the credential based approaches above are not sufficiently flexible for smart environments, due to their reliance, at least at some level, on complete information for policy evaluation. A new approach that is being actively researched is to defined security policies in terms of a more humanly intuitive notion of trust. Due to the vast amount of current research in this area we can only briefly describe a few of the important contributions to the area.

Stephen Marsh [25] made some early attempts to formalise the notion of the trust for computational use in interactions between two autonomous agents. This approach takes into account many of the widely accepted aspects of trust as seen in the literature, defining basic or dispositional trust, general trust in another entity and situational trust in another entity, combined with the notions of utility, risk and importance. From this, simple linear equations allow the formation of trust values, which are represented in the range [-1, 1) to allow for reasoning about distrust. Trust information (values representing payoff) from past interactions of an agent is stored, allowing evolution of trust, albeit in a rather arbitrary manner. More detailed evidence would be more useful in terms of evolution. The concept of a threshold for trusting behaviour based on the perceived risk and competence in the situation, demonstrates the important relationship between trust and risk. Although the model incorporates many of the important features of trust, implementations encountered several problems, due to the use of overly simple linear equations failing to intuitively model trust. This work makes several useful contributions to dynamic computational trust, but is limited by a very basic trust model, which fails to cope with certain values in a limited trust domain.

Abdul-Rahman [38] proposes a more comprehensive approach to decentralised trust management incorporating distinct trust levels and dynamics. The work focuses on the formation and evolution of trust rather than exploitation. Formation of trust relationships is based on reputation, comprising recommendations from third parties and experiences of the truster itself. The model defines 'direct trust relationships', which take a trust degree with locally defined semantics. At any given time, trust in an agent is evaluated from the relevant subset of experiences based on context. An experience is the result of either evaluating an interaction or relying on a recommendation from an agent, and takes a value corresponding to the trust degree. By storing a count of each type of outcome, the direct trust can be evaluated according to the trust degree that corresponds to the most frequent type of experience. 'Recommender trust relationships' represent the belief that an agent provides good recommendations within a certain context, and 'recommender trust' can give a weighting for recommendations based on 'semantic distance' of experience from recommendation. Context of a recommendation can be direct or a lead to a recommender, which means that chains can be omitted by contacting the final recommender directly. Recommendations can be combined from various sources. This work provides many valuable insights into the evaluation of trust, particularly the subjective evaluation of recommendations, a useful process for determining the trustworthiness of unknowns entering a smart environment. However, a notion of risk is not considered, which is important when determining likelihood of desirable behaviour.

Josang describes Subjective Logic [39] as a logic that operates on subjective beliefs (opinions) about the world using standard and non-standard logical operators. The representation of trust is based around probability metrics able to represent a degree of uncertainty in beliefs represented as propositions. Logical operators are defined for propositional conjunction and disjunction for two propositions from distinct binary frames of discernment, and for propositional negation. Two non-traditional operators are defined that depend upon belief ownership. These allow discounting of opinions based on an opinion of the advice and for reaching consensus between two opinions. It is only possible to reach consensus with somebody who retains some uncertainty (which can be introduced via discounting). An alternative representation of uncertain probabilities with respect to the evidence space is defined using probability density functions derived from the amount of evidence supporting the event and the amount of evidence supporting its negation. A mapping is easily defined between the evidence space and the opinion space to allow the use of results from one in the other. Propositional conjunction and disjunction is defined on the evidence space, as is the combination of evidence from two observers as if one entity had collected all of the evidence. This forms the basis for the opinion space consensus operator. This constitutes very important work in the area of subjective reasoning, in particular due to the fact that opinions can be represented with some uncertainty.

Jonker and Treur [40] have carried out some interesting work regarding the dynamics of trust in light of personal experience. Each event that can influence the degree of trust in a subject is interpreted as either trust negative or trust positive, reducing or increasing trust respectively, although the degree to which the trust is changed depends on the trust model used by the agent. Trust dynamics affect how the agent is influenced by trust positive and trust negative experiences. For example, agents can be defined as slow-positive-fast-negative, meaning it takes a lot of positive evidence to build trust, and little negative evidence to reduce it. The dynamics of trust can be formalised by a trust evolution function, which relates sequences of experiences to trust representations, or in an inductive manner a trust update function, which relates a current trust representation and a current experience to a new trust representation. This formal framework enables a variety of dynamic models to be developed to capture the individual characteristics of agents. This framework is not meant as a coherent approach to trust management, but rather an analysis of trust dynamics, and as such does not address how trust might be used for decision making.

Grandison and Sloman [41] define a general-purpose trust management system developed as a trust specification that can be analysed and evaluated for many uses. Example uses include a starting point for deriving Ponder security management policies or to make trust-based authorisation decisions. SULTAN (Simple Universal Logic-oriented Trust Analysis Notation) is a notation with associated tools for specification, analysis and management of trust relationships for Internet applications. SULTAN's trust management has several components. Trust Establishment defines protocols for negotiation and exchange of the evidence and credentials. Trust Analysis evaluates the trust and recommendation specifications to determine conflicts and implicit relationships. A Specification Server (with a Specification Editor) holds all the trust and recommendation specifications for the domain, while a Monitoring Service updates a State Information Server with state information for the scenario and system, experience information for direct alteration of trust levels (e.g. number of successful interactions), and risk information. The Risk Evaluation Service retrieves risk information from the state information server and performs a risk calculation using a list of common risks and their probabilities with a list of action dependencies and risk thresholds. The SULTAN framework is to be used both as a decision support tool to aid human managers or automated manager agents, and to support on-line trust queries for security policy decisions. The model makes good use of context for effective use of evidence, considers risk factors and allows propagation of trust through recommendations.

After we examined some of the influential trust management approaches, it is clear that there are some problems remaining to be addressed. In the systems considered, problems arise due to reliance on a global view of the system (through central storage or broadcast messages), which we assume cannot exist even if desirable from the privacy perspective. Furthermore, the provision of some form of centralised infrastructure such as storage or trust analysis engine is common, which can be a problem for principals roaming between smart environments. An simple notion of evidence is used in most systems, such as quality of service feedback by the user, which leads to missing a great deal of information that could be gained from interaction via, for example, network monitoring. Furthermore, this simple evidence is not evaluated with respect to the trust value used to initiate a decision, and thus does not consider the behaviour we expected to see. Limited evidence also leads to limited dynamics in terms of initial formation and evolution capabilities. In the exploitation of trust values, few systems take risk into account when making decisions, which is counterintuitive for trust-based decision-making.

To address these inadequacies, a more comprehensive framework is required, such as that being developed in the SECURE project [42]. A comprehensive general framework is necessary to gather and evaluate detailed observational evidence [43] in an automated manner and propagates source-weighted recommendations in a context aware fashion. SECURE incorporates a general trust model [44], allowing application specific trust domains to be used, and providing the capability of incorporating many dimensions of trust, hence being less restrictive as a framework. The trust model also incorporates a notion of uncertainty to cope with unknown principals. Through the incorporation of uncertainty in our trust values, it is possible to assign unknown trust to a new principal, yet still afford them the possibility of interaction. SECURE retains this notion of uncertainty throughout the dynamic lifecycle of trust, even into the decision process, where the exploitation of trust occurs to facilitate risk assessment as part of a general risk model [45], also capable of representing uncertainty. This decision process based on the relationship between trust and risk allows the separation of policy evaluation from trust reasoning, in that trust is used to categorise principals. By defining policy in terms of trust and risk, flexibility of decision-making is retained, facilitating interaction in a smart environment even in the absence of full knowledge of a principal.

Furthermore, trust in SECURE is based on patterns of historical behaviour rather than just separate pieces of evidence and the trust evolution mechanisms essentially allow all the history to remain at some level within the trust values, albeit with depleting influence over time. By explicitly modelling trust it is possible to form and evolve trust relationships more intuitively based on observations and recommendations, whether negative or positive. Therefore we can incorporate a range of opinions as evidence without leading to policy violations. This focus on evidence currently available for evaluation to predict the likely behaviour, coupled with risk analysis to incorporate other factors of the interaction leads to an intuitive subjective notion of trust, supporting fine-grained trust evolution. Moreover, gathering evidence of past behaviour can be automated and thus requires no user intervention, such that the principals of calm technology are maintained. Also, the same evidence can influence a variety of decisions through context mappings, although perhaps not to the same degree.

5 Discussion

In this chapter we have attempted to give a perspective on the background and current status of security, privacy and trust in smart environments. It is a fundamentally difficult task, as for each aspect of the problem space there are a massive number of issues. Consequently there are many areas we have simply not covered: Access Control, Identity Management, Legal and Socio-technical Issues, and Biometric aspects to name a few.

In considering security we have been rather prosaic in revisiting the traditional definitions and reusing these. However, this is the area perhaps best understood (although not yet solved) with much of the technology useable in some form or another in smart environments. However, because of the characteristics of the environments new versions of old problems occur, such as denial of service attacks on battery power as well communication channels. The key problem identified is the lack of global reference so all secure interactions have to potentially take place in a zero knowledge environment [11].

In considering privacy we focused not on the technology aspects but on the guidelines for design derived from significant historical debate: these are exemplified by [3, 21]. These demonstrate very clearly the importance of openness and accountability in establishing a privacy-preserving environment. One aspect we highlight from [28] is the importance of risk assessment, both implicit and explicit, in determining whether a user engages in an activity. This aspect is reflected in some detail in our discussion on trust management.

Trust Management is a key area for smart environments because of the user centric nature of these systems. Encouraging users to engage while providing them with the ability to control their exposure to the system is a critical requirement. Existing trust management systems are not sufficient for the purposes because they do not address fine-grained dynamic trust evolution. This is a consequence of the lack of explicit models and representations for trust behaviours. Recent work [5,11,22,23,46] has begun to address this from a number of perspectives. However, we believe that trust, as a core enabling infrastructural, is the next step to balance the complex trade-offs demanded by security and privacy in smart environments. In particular, each decision about encryption, access control, or information exchange implies a decision process. Trust based infrastructure provide the mechanisms for users and systems to base this decision process on their perspective of the risks and benefits involved.

It is the author's belief that the issues of security, privacy and trust are now among *the* most important challenges for smart environment research and we hope this chapter contributes to understanding in the area.

Acknowledgements

This work was supported partly supported by the **SECURE project** (Secure Environments for Collaboration among Ubiquitous Roaming Entities, IST-2001-32486) and the **GLOSS Project** (Global Smart Environments, IST-2000-26070), both funded by the EU FET Programme.

6 References

[1] Paddy Nixon, Gerard Lacey and Simon Dobson (eds), Managing interactions in smart environments, Springer Verlag Press, pp. 243, December 1999.

[2] Bill Schilit, Norman Adams, and Roy Want. Context-aware computing applications. In Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pages 85-90, Santa Cruz, California, December 1994. IEEE Computer Society Press.

[3] Marc Langeheinrich, Privacy by Design – Principles of Privacy Aware Ubiquitous Systems, in UBICOMP 2001, LNCS 2201, pp 273 291.

[4] Paddy Nixon, Gerard Lacey, and Simon Dobson, Managing Smart Environments in proceedings of Workshop on Software Engineering for Wearable and Pervasive Computing, June 2000.

[5] Roy Campbell, Jalal Al-Muhtadi, Prasad Naldurg, Geetanjali Sampemane, M. Dennis Mickunas, "Towards Security and Privacy for Pervasive Computing." in Theories and Systems, Mext-NSF-JSPS International Sympsoium, ISSS 2002, Tokyo, Japan, November 2002. pp. 1-15, G. Goos, J. Hartmanis, and J. vanLeeuwen (editors) in Lecture Notes in Computer Science.

[6] Philip Robinson, Michael Beigl, "Trust Context Spaces: An Infrastructure for Pervasive Security", in Proceedings of First International Conference on Security in Pervasive Computing, Springer Verlag Press, 2003.

[7] Frank Stajeno, Security for Ubiquitous Computing, Wiley Press, 2002.

[8] Nigel Smart, Crytopgraphy, McGraw Hill Press, 2003.

[9] A. Abdul-Rahman: "The PGP Trust Model" , Technical report, Department of Computer Science, University College London, 1996.

[10] Germano Caronni, "Walking the Web of Trust", Proceeding of WETICE, IEEE Computer Society Press, 2000.

[11] V. Cahill, B. Shand, E. Gray, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. A. Nixon, C. Bryce, G. Serugendo, J. Seigneur, M. Carbone, K. Krukow, C. Jensen, Y. Chen, and M. Nielsen, "Using Trust for Secure Collaboration in Uncertain environments," IEEE Pervasive Computing Magazine, 2003.

[12] Anup K. Ghosh , Tara M. Swaminatha, Software security and privacy risks in mobile e-commerce, Communications of the ACM, v.44 n.2, p.51-57, Feb. 2001

[13] M. Jakobsson and S. Wetzel. Security Weaknesses in Bluetooth. In Proc. of the RSA Cryptographer's Track (RSA CT '01), LNCS 2020, pages 176 191. RSA Data Security, Springer-Verlag, 2001.

[14] Michael J. Covington, Wende Long, Srividhya Srinivasan, Anind K. Dev, Mustaque Ahamad, Gregory D. Abowd: Securing context-aware applications using environment roles. SACMAT 2001: 10-20

[15]] Ghita Kouadri Mostéfaoui: Security in Pervasive Environments, What's Next? Security and Management 2003: 93-98

[16] Alan F. Westin. Privacy and Freedom. Publisher: Bodley Head.

[17] Tavani, H.T.: 1999, "Informational Privacy, Data Mining, and the Internet." Ethics and Information Technology, vol. 1, 2.

[18] S Warren, L Brandeis, “The right to privacy”, Harvard Law Review, 4:193-220, 1890.

[19] http://www.w3.org/P3P/ and http://www.w3.org/2002/01/P3Pv1

[20] Tavani, H. T. and J. H. Moor: 2001, 'Privacy Protection, Control of Information, and Privacy-Enhancing Technologies'. ACM SIGCAS Newsletter 31(1), 6-11.

[21] S Lahlou, F Jegou, “Privacy Design Guidelines, Ambient-Agoras Project Deliverable D15.4, 2003.

[22] Waleed Wagealla, Sotirios Terzis and Colin English, Trust-based model for privacy control in context-aware systems, in UBICOM Worhsop on Security in Ubiquitous Computing, 2003.

[23] Lalana Kagal, Jeffrey Undercoffer, Filip Perich, Tim Finin “A Security Architecture Based on Trust Management for Pervasive Computing Systems”. In Proceedings of Grace Hopper Celebration of Women in Computing 2002.

[24] M. Langheinrich, “A Privacy Awareness System for Ubiquitous Computing Environments”, in UBICOMP 2002, LNCS 2498, pp 237-245, 2002.

[25] S. Marsh: “Formalising Trust as a Computational Concept”. Ph.D. Thesis, University of Stirling, 1994.

[26] D. McKnight and N. Chevany: “The Meanings of Trust”. working paper, Carlson School of Management, University of Minnesota, 1996.

[27] D. McKnight, L. Cummings and N. Chevany: “Trust Formation in New Organisational Relationships”. Carlson School of Management, University of Minnesota, 1995.

[28] M. Blaze, J. Feigenbaum, and J. Lacy: “Decentralized trust management”. In Proceedings of the 1996 IEEE Symposium on Security and Privacy, pp.164-173, May 1996.

[29] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis: “The KeyNote Trust Management System - Version 2”. Internet Engineering Task Force, September 1999. RFC 2704.

[30] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. "The Role of Trust Management in Distributed Systems Security." Chapter in *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, (Vitek and Jensen, eds.) Springer-Verlag, 1999.

[31] M. Blaze, J. Feigenbaum, and M. Strauss: “Compliance checking in the policymaker trust management system”. In R. Hirschfeld, ed., Financial Cryptography, volume 1465 of Lecture Notes in Computer Science, pages 254--274. Springer Verlag, Berlin, 1998.

[32] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss: "REFEREE: Trust Management for Web Applications," World Wide Web Journal, 2 (1997), pp. 706-734.

[33] Lalana Kagal et al: “A Security Architecture Based on Trust Management for Pervasive Computing Systems”. In Proceedings of Grace Hopper Celebration of Women in Computing 2002.

[34] K. E. Seamons, M. Winslett, T. Yu, B. Smith, E. Child, J. Jacobson, H. Mills, and L. Yu: “Requirements for Policy Languages for Trust Negotiation” In 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY 2002), Monterey, CA, June 2002.

[35] Ninghui Li and John C. Mitchell: “RT: A Role-based Trust-management Framework”. In Proceedings of The Third DARPA Information Survivability Conference and Exposition (DISCEX III), Washington, D.C., April 2003. IEEE Computer Society Press, Los Alamitos, California, pp. 201--212.

[36] Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum: “Delegation Logic: A Logic-based Approach to Distributed Authorization” In ACM Transactions on Information and System Security (TISSEC), volume 6, number 1, pp. 128-171, February 2003.

[37] Ninghui Li, William H. Winsborough, and John C. Mitchell: “Distributed Credential Chain Discovery in Trust Management” In Journal of Computer Security, volume 11, number 1, pp. 35-86, February 2003.

[38] A. Abdul-Rahman, S. Hailes: “Supporting Trust in Virtual Communities" In Proceedings Hawaii International Conference on System Sciences, 33. Maui, Hawaii, 4-7 January 2000.

[39] A.Jøsang: “A Logic for Uncertain Probabilities”. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 9(3), pp.279-311, June 2001.

[40] C. M. Jonker, J. Treur: “Formal Analysis of Models for the Dynamics of Trust Based on Experiences” Modelling Autonomous Agents in a Multi-Agent World 1999 European Workshop on Multi-Agent Systems. pp. 221-231, 1999.

[41] Tyrone Grandison and Morris Sloman: “Trust Management Tools for Internet Applications”. In Proceedings the First International Conference on Trust Management, Heraklion, Crete, 28-30 May 2003.

[42] SECURE website: http://secure.dsg.cs.tcd.ie.

[43] S. Terzis, W. Wagealla, C. English, and P. Nixon. The SECURE collaboration model. Technical report 03. University of Strathclyde, department of Computer and information sciences.

[44] M. Carbone, O. Danvy, I. Damgaard, K. Krukow, A. Møller, J. B. Nielsen, M. Nielsen: “SECURE Deliverable 1.1: A Model For Trust”, December 2002.

[45] J. Bacon, N. Dimmock, D. Ingram, K. Moody, B. Shand, A. Twigg: “SECURE Deliverable 3.1: Definition of Risk Model”, December 2002.

[46] P. A. Nixon and S. Terzis, "Trust Management," in *Lecture Notes in Computer Science*, vol. 2692: Springer-Verlag, 2003.