Available online at www.sciencedirect.com
SCIENCE DIRECT®
Telematics and Informatics 23 (2006) 196–210
TELEMATICS AND INFORMATICS
www.elsevier.com/locate/tele

Protecting privacy and anonymity in pervasive computing: trends and perspectives

Stelios Dritsas [a,*], Dimitris Gritzalis [a], Costas Lambrinoudakis [b]

[a] *Department of Informatics, Athens University of Economics and Business 76 Patission Avenue, Athens GR-10434, Greece*
[b] *Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece*

Received 27 July 2005; accepted 27 July 2005

Abstract

Pervasive computing is expected to enter our everyday life in the foreseeable future. The capabilities of the devices, which operate in such an environment, as well as the range of services offered to the end-users are expected to be significantly increased. However, this new era is expected to have a serious effect on privacy. In this paper, we first refer to the privacy threats identified in a pervasive environment; then, we present a set of principles for ensuring privacy in this context. In the sequel, we examine a number of privacy protection mechanisms for pervasive systems, with a focus on the level of anonymity offered to the end-users. We identify flaws, these mechanisms suffer by, in terms of the limited anonymity level they offer. We conclude by presenting a set of essential actions one should take into account, in order to ensure user's anonymity in a pervasive computing environment.

Keywords: Pervasive computing; Privacy; Privacy principles; Anonymity

1. Introduction

Some years ago, in an article written by Weiser (1991), it was argued that the most profound technologies are those that "disappear" by weaving themselves into the fabric of

* Corresponding author.
E-mail addresses: sdritsas@aueb.gr (S. Dritsas), dgrit@aueb.gr (D. Gritzalis), clam@aegean.gr (C. Lambrinoudakis).

0736-5853/$ - see front matter
doi:10.1016/j.tele.2005.07.005

people's everyday life, until they become an integrated part of it. Weiser called this vision *Ubiquitous Computing* (UbiComp). For the realization of this vision the underlying technology should reach an acceptable degree of pervasiveness, making the usage of it unconscious from the end-users' perspective.

Imperceptible technology should include low power and inexpensive computational devices, supporting software, as well as the appropriate network infrastructure, thus supporting diverse, autonomous, mobile, and cooperating entities. Pervasive computing refers to the emerging trend toward: *numerous*, *casually accessible*, often *invisible* computing devices, frequently mobile or embedded in the environment, connected to an increasingly ubiquitous network infrastructure composed of a wired core and wireless edges (NIST, 2001).

Besides the concept of pervasive computing, other new concepts have also been proposed, e.g. proactive and autonomic computing, etc. This variety of terms, no matter how short-time realizable might seem, can be quite confusing, in particular because they refer to the future (Satyanarayanan, 2002). In this paper, and for the sake of simplicity, we make use of the terms "Ubiquitous" and "Pervasive" Computing interchangeably.

The most noticeable characteristics of Pervasive computing and its applications, besides the heterogeneity of the underlying supporting environments, are: (a) ubiquity, (b) invisibility, (c) sensing, (d) interconnectivity and co-operation between participating devices, and (e) memory amplification[1] (Langheinrich, 2001; Lahlou et al., 2005; Russell et al., 2005). These characteristics introduce quantitative and qualitative changes to data collection processes in UbiComp, in comparison to current practices. This is true because never before has so much information about individuals been directly available to so many others, and in such a comprehensive way. This exposure can be more straightforward if the above abstract characteristics are implemented and supported by systems, which sense, collect, store, and share, in an unobtrusively and intelligently fashion, large amounts of personal data.

Experience, inter alia, has demonstrated that the advent of new technologies has always been associated with new and increasing risks to privacy. In the case of UbiComp, the association between the services offered and the respective privacy concerns is expected to be more complicated and intractable. Information collection, processing, and sharing is fundamental to pervasive systems; hence privacy and pervasiveness are, by nature, in conflict.

In order to deal effectively with the emerging privacy problems, several mechanisms have been proposed in the literature. In this paper, we first perform a review of state-of-the-art mechanisms, which aim at the protection of privacy. Furthermore, we examine and investigate the weaknesses and vulnerabilities of these mechanisms, while at the same time evaluate the level of anonymity they provide for.

The paper is organized as follows: in Section 2 we discuss the importance of privacy in pervasive environments and, then, we present a set of privacy principles, which should be taken into account during the development of such systems. In Section 3, we examine some representative approaches aiming at privacy protection in UbiComp, while in Section 4 we appraise the drawbacks of these proposals along with the offered level of

[1] The property of memory amplification is related to the enhancement of sensory equipment, combined with the advances in their storage capabilities that will make feasible to perceive memory prosthesis, or amplifiers, which can continuously and unobtrusively record every action, utterance and movement of a user and her surroundings.

anonymity. Finally, in Section 5 we conclude by presenting thoughts and ideas for further research.

2. Privacy in pervasive computing

Pervasive computing, due to its dynamic nature, seems to have an innate conflict with privacy. In order for the environment to be truly invisible and ubiquitous, it is crucial to operate at the users' behalf, without their explicit knowledge and/or interaction. In order to achieve this and to meet the users' needs, the environment should possess a lot of users' personal information, so as to represent them adequately in every situation the user is involved. However, the pervasiveness of the system depends largely on the provision and sharing of users' personal information with the other participated entities, sometimes without the user's explicit consent.

From the users' perspective, the invisible character of UbiComp makes difficult for them to know when and which devices are present and functioning on behalf of them, and what kind of information is being collected and processed. Furthermore, considering the sensing capabilities of ubiquitous sensor networks, in conjunction with the advances in artificial intelligence and in data mining techniques, one can identify the potential tracking and profiling capabilities that information collectors have in such environments. Finally, the ease of collecting personal information, regardless of the existence of an underlying motive for such a collection, completes the picture of privacy violation capabilities in UbiComp.

In general the most profound privacy risks and threats in the case of UbiComp environments are:

- Pervasive computing components will be everywhere and will affect every aspect of our life,
- Many UbiComp components (e.g. sensors) will be invisible and act in a transparent way from the users' perspective,
- The enhancement of storage capabilities will make easier the access and process of personal data,
- The enhancement of sensory equipment, combined with the advances in their storage capabilities, will make feasible to perceive memory prosthesis, or amplifiers, which can continuously and unobtrusively record every action, utterance and movement of us and our surroundings,
- The minimization of sensors, as well as the advances in data mining techniques, will increase the amount and types of personal data that are invisibly captured and analyzed, and
- The communication of the objects in pervasive environments will usually take place by their own initiation and in a way that might disclose personal data to other objects/users, so as to accomplish their intended purpose.

On the other hand we should have in mind that privacy protection, nowadays, enjoys a constitutional status in several countries. Moreover, a series of laws, regulations, recommendations and guidelines have been adopted to protect and ensure privacy. These means aim at protecting some of the following aspects of privacy:

- *Territorial privacy*: The protection of the physical area surrounding a person.
- *Bodily privacy*: The physical protection of a person against undue interference.
- *Informational privacy*: The awareness and control of whether and how personal data can be gathered, stored, processed and communicated.
- *Privacy of communications*: The protection of data communicated among persons, which prevents the monitoring of the transmitted data by third parties.

Since UbiComp may provide for several sophisticated and user-centric services, information about users' location will be essential. Until today, several systems have been developed with an eye towards supporting the tracking of individuals. Such systems (e.g. GPS, cricket, etc.) are improving, in terms of accuracy, availability, and coverage of location discovery services. The improvement of such technologies has led to the introduction of a fifth aspect of privacy, i.e., is *Location Privacy*, which is the ability to prevent other parties from learning a user's current or past location (Beresford and Stajano, 2003).

In most approaches, which aim at privacy protection in UbiComp, a set of privacy principles is adopted (Langheinrich, 2001). These principles, which are based on the well-known Fair Information Practices (OECD, 1980), have been adopted as general rules for the development of privacy enhanced UbiComp systems (e.g. *European Disappearing Computer Privacy Design Guidelines* (Lahlou and Jegou, 2004). These practices are:

1. *Notice*: Users should always be aware of the collection of their personal data.
2. *Choice and consent*: Users should have the choice of carrying out, or not, of their personal data.
3. *Proximity and locality*: The collection of data from a user's device should only occur when the user is present (proximity). Processing and access to these data should only be done within the space they were collected (locality).
4. *Anonymity and pseudonymity*: Whenever the user's identity is not required or whenever the user does not consent, anonymity or pseudonymity services should be provided for.
5. *Security*: There should be security mechanisms, which provide adequate protection for collected data.
6. *Access and resource*: Access to the user's data should only be allowed to authorized persons. There should be regulatory means for the protection of a user against parties that are not complying with this regulatory framework.

Lederer proposed a conceptual model of everyday privacy in Ubiquitous computing. The concept of everyday privacy refers to an individual end-users' ongoing exposure to, and influence over, the collection of their personal information in UbiComp environments (Lederer et al., 2002). The proposed model is based on the *societal-scale model* introduced by Lessig (1998) and on and the *user perceptual model* proposed by Adams (1999). The following formula provides for a qualitative abstract of this model and represents the preferred privacy level of a user, in a given situation:

$$\text{preferred\_privacy\_level} = \text{user}(\text{L}, \text{M}, \text{N}, \text{A}, \text{C}, \text{PI}, \text{IS}, \text{IR}, \text{IU})$$

L stands for Law, M for Market, N for Norms, and A for Architecture (Technology). The former are the actors Lessig used to describe the profile of privacy in a given place and time (e.g. context). These actors are depended with each other, i.e., modification of one of them requires an appropriate adjustment to one or more of the others. PI stands for

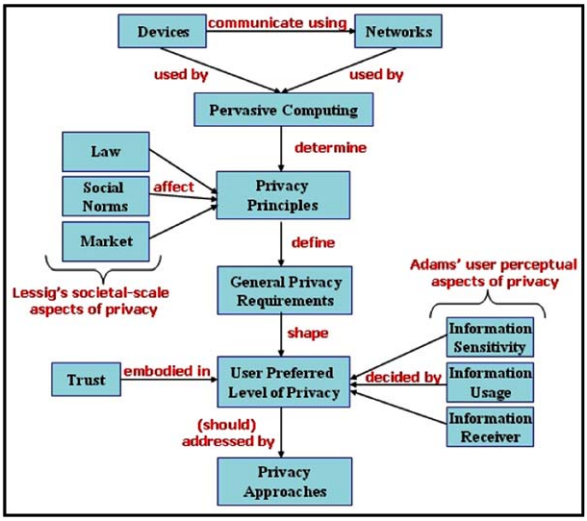

Fig. 1. Modeling privacy with the use of basic concepts in pervasive computing.

the disclosed personal information, and C stands for a set of contextual variables. Finally, IS stands for information sensitivity, IR stands for information receiver and IU stands for the type of information use. An *instance* of the above variables describes the situation a user is involved with. An individual should know the aforementioned parameters, in order to take a privacy-protection decision in the context of a specific pervasive application.

Fig. 1 presents a model identifying the basic concepts and relations regarding privacy in the UbiComp paradigm. The proposed model incorporates the actors (forces and factors) introduced in Lessig's and Adams' model respectively as well as new parameters affecting the user preferred level of privacy that is the focal point of our interest. The relations presented in Fig. 1 are the ones affecting explicitly and clearly the user desired level of privacy. Apparently, there are and other relations that affect, mainly indirectly, devices, networks, etc. which are not presented in our model since is out of the scope of our research work.

In an instance, where a user is involved with, Lederer's model describes each user's preferred privacy level using nine variables. It appears that the most important variables are the contextual ones (e.g. users' location, time, user role in the context of a specific application, etc.). We argue that, for a specific moment $T = T_0$ and in a specific location $L = L_0$, all nine variables of Lederer's type have fixed values. In essence, if we take a "snapshot" of this instance, the variables such as location, law, information use, etc. remain constant.

3. Privacy protection mechanisms

Several mechanisms have been proposed to deal with the privacy threats in pervasive computing environments. These mechanisms range from abstract frameworks to specific protocols and technologies. They are all intended towards fulfilling certain privacy principles. In the following section a review of some indicative such mechanisms is provided for, with an eye towards fulfilling the anonymity principle, which is offered by each

mechanism. It should be noted that out interest is focused on mechanisms and techniques that are focused exclusively on handling privacy requirements in pervasive environments and are widely mentioned in the bibliography of privacy protection in such environments. Finally, it should be stressed that there are many other research works (Fasbender et al., 1996; Leonhardt and Magee, 1998; Kesdogan et al., 1998) related to privacy protection, but are not completely or directly applicable to pervasive computing context.

3.1. Privacy awareness system

The Privacy Awareness System (*pawS*) was introduced by Langheinrich (2002). It was developed in order to provide for a sense of accountability, in a world of invisible services that we will be comfortable living in and interacting with, rather than to provide for security and privacy guarantees. *pawS* aims at offering this sense by allowing data collectors to announce and implement adequate privacy policies, as well as by providing users with the essential means, so that they will be aware of how their personal data are processed.

3.2. Identity management

Another approach for ensuring privacy in a pervasive environment is based on an new architecture, aiming at a context-driven identity management system (Jendricke et al., 2002). Identity management enables users to express and enforce a preferable level of privacy, depending on the situation, which they are involved in. Comparable to the everyday life, the identity manager (which operates in each user device) allows the device to present different subsets of the user's identity, depending on the perceived context.

In UbiComp, the device is expected to interact often with other devices, within its operational environment but without a direct user interaction. With context-driven pervasive identity management, a user may keep under her control the unbidden actions of her device, so as to maintain a high level of privacy. The configuration of the device, in order to present the appropriate subset of users' identities, requires: (a) context sensing, (b) determination of situation, (c) choice of appropriate identity, and (d) setting of authentication and services.

3.3. Mist protocol

Mist is a protocol aiming at ensuring the privacy of a user and the anonymity of her communications (Muhtadi et al., 2002). Through this protocol users communicate with each other and access computing resources through appropriate authentication techniques, while at the same time preventing the disclosure of their physical locations.

Mist's operation is based on *Mist routers* and *Mist circuits*. Mist routers are deployed in a hierarchical fashion. The user can connect directly to a "*Portal*", which is a leaf level Mist router. Portals can detect the presence of the user without identifying her. After connected to a Portal, the user sets up a Mist Circuit, which is a handle-based virtual circuit, preserving privacy of communications between the user and a *Lighthouse*. A Lighthouse is a Mist router that serves as a contact point for the user. A user uses Mist circuits to contact their Lighthouse, which has only partial information on how to route to that user. As a result, the user's Lighthouse will know of her true identity, as well as partial knowledge

on how to route to her, without knowing her exact physical location. On the other hand, the Portal knows the exact physical location of the user, but is not aware of the true identity of the user or her Lighthouse.

As far as the communication between two users is concerned, the Lighthouses of the communicating parties are aware of the identities of the endpoints of the communication but they are not aware of their physical locations. In addition, all intermediate routers are unaware of the endpoints of the communication and, thus, cannot assume the parties' locations, thus preserving their location privacy.

Additionally, the use of session keys in all phases of Mist's operation ensures the confidentiality of the transmitted messages. Finally, it should be noticed that one of Mist basic requirements is that no cameras or microphones should be present in the area that the user is located and uses the services offered (Muhtadi et al., 2002).

3.4. Mix-zones

Location privacy refers to the risk inherent with a situation where an adversary can learn the locations visited by a person and the time of that visit. In order to achieve better location privacy, Beresford and Stajano argue that applications should use pseudonyms rather than true identities (Beresford and Stajano, 2003). Furthermore, in UbiComp, devices and applications are expected to exchange and share information dynamically, thus rendering the use of different pseudonyms in different applications an important issue. Additionally, pseudonyms should be changed frequently and within the same application, in order to avoid the disclosure of the user's identity. In this context, the concept of *Mix-zones* aims at addressing and dealing with the vulnerability of linking old and new pseudonyms by the applications. A mix zone for a group of users is defined as a connected spatial region of maximum size, in which none of the users has registered any application callback. For a given group of users, there might be several distinct mix-zones. The approach proposed by Beresford and Stajano requires a middleware (acting as anonymizing proxy) handling all communication between users and applications in order to protect the disclosure of the identity.

In the case of Mixed Zones, two metrics for measuring location privacy have been proposed. The first is based on anonymity set, which is the group of people who visits a mix zone during a time period t, where this mix zone is the zone that a user u visits during the same time period t. The second metric is based on entropy. By using entropy in the context of mix-zones, a more accurate metric was developed. This metric considers the a priori knowledge that an attacker may have.

3.5. Privacy mirrors

Nguyen and Mynatt define pervasive computing systems as socio-technical systems encompassing three environments: social, technical, and physical (Nguyen and Mynatt, 2002). In this context, they argue that by addressing privacy in only one of the above environments it is not possible to entirely protect privacy in a UbiComp system. As a result of this, they introduced the *Privacy Mirrors* framework for the development of a socio-technical pervasive computing system. Privacy Mirrors expose five characteristics in all of the three different environments, namely: *history* and *feedback* (which provide users with *awareness* and *accountability*) and the *awareness* and *accountability* (which help users to

change one or more of the social, technical, or physical component of the socio-technical system, which they are involved in.

Privacy Mirrors help users deal with the socio-technical parameters of a system and thus be able of making it comply with their privacy needs. In addition, Privacy Mirrors provide users with a better understanding of a system by revealing the system's capabilities and constraints. This way the flow, state, and history of a system are brought in the foreground.

3.6. A conceptual model of privacy in UbiComp

Lederer presented a model for everyday privacy in UbiComp environments using a synthesis of Lessig and Adams privacy models (Lederer et al., 2002). He argues that the most important privacy principles, each UbiComp system should meet, is Notice, Choice and Consent. In this context, he proposed the use of logs, which the user can review later for ensuring the fulfillment of the principle of Notice.

Lederer extended his model by using an interactional metaphor, called *Faces*, which represents the set of permutations of UbiComp privacy preferences an individual is engaged with, within the course of her everyday life. These preferences might include: *identify me only if...*, *record my voice only if...*, *track my location only if...*, where "*only if...*" implies a conditional approval, contingent on situational factors.

As a user is employed in a pervasive application, she "puts on" the appropriate face (e.g. shopper, anonymous, etc.). After reviewing notices in her logs, she could assign the appropriate face to handle future personal information collection by a given recipient (or a class of recipients), in the context of each pervasive application she uses.

3.7. Privacy tagging model

Jiang and Landay proposed the information spaces, an abstraction used for the development of a theoretical model for controlling privacy. Information spaces are repositories of personal data, owned by specific principals, which might stand for a person, a particular device, etc. (Jiang and Landay, 2002). An information space can be restricted by using three types of boundaries, i.e., physical, social, or activity-based; in these spaces specific privacy policies are developed, in order to control the information flow among the spaces.

Since information spaces are an abstraction, and in order to support the desirable for a UbiComp system property of decentralization, Jiang and Landay introduced the privacy tagging approach. Privacy tagging through metadata is used for denoting in which information space a particular object belongs to, as well as for explicating information about privacy controls (i.e., permissions for different types of operations applied to an object). The privacy tagging model is unified in the sense that it can be used to tag both physical and data objects.

4. Evaluation based on anonymity

In this section we examine the weaknesses, vulnerabilities and limitations that the aforementioned mechanisms and approaches suffer by, focusing on the level of anonymity supported by each of them. The evaluation is based on the following criteria:

1. Advantages and limitations of anonymity assurance level as indicated by the researchers of proposing each mechanism.
2. Theoretical justification and specific results concerning the validation of each mechanism in practical scenarios.
3. Consideration of UbiComp characteristics and constraints (i.e., limitation of devices participated in a UbiComp system in terms of computational capabilities, memory, bandwidth, power consumption, etc.).
4. Transparency of the mechanism related to users' participation.
5. Scalability of the proposed model.
6. Response and reaction of the mechanisms by supporting and offering appropriate actions to end-users, when the level of anonymity offered is below a specific threshold.

Anonymity is the state where a user is not identifiable when using a resource or service. The requirements for anonymity provide protection of users' identity. Anonymity is not intended to protect only a user's identity, but requires that other users are unable to determine the identity of a user bound to a subject or operation (ISO/IEC, 1999). Therefore, anonymity is the state of being *not identifiable* within a set of subjects (i.e., the anonymity set) (Pfitzmann and Kohntopp, 2000). An *anonymity set* is further defined as a set of all possible subjects. For example, in the case where a user wishes to send a message, she might be anonymous only within a set of potential senders (i.e., her anonymity set), while the recipient of this message may be anonymous only within a set of the potential recipients. The higher the level of anonymity, the larger the respective anonymity set and the more complex the information flows between the subjects within each set.

A concept related to anonymity is unlinkability. Unlinkability has only meaning, after the system one wishes to describe anonymity upon is defined. Then, *unlinkability* of two or more items (e.g. subjects, messages, actions, etc.) means that these items are no more and no less related within this system than they were based on the a priori knowledge (Pfitzmann and Kohntopp, 2000). Therefore, the probability of the items being related remains steady before (a priori knowledge) and after (a posteriori knowledge of the attacker) the run within the system. When unlinkability decreases, then anonymity decreases, also (Steinbrecher and Kopsell, 2003).

Although there are several methods, which support anonymity, these might not be feasible in the context of pervasive oriented applications. This is mainly due to that the communications between entities participating in a UbiComp system are frequently and dynamically changed, thus preventing direct and instant interactions among them. On the other hand, anonymity offered in a UbiComp environment may suffer by drawbacks from an application point of view. For example, being anonymous prevent one from the use of any application that requires authentication or offers personalization. Although the use of pseudonyms is considered as an alternative to a more fine-grained control of anonymity, there exists a tradeoff between the level of anonymity a user desires and the diversity of services she can use in the pervasive computing context.

4.1. Privacy awareness system

In the case of the *pawS* system, anonymity and pseudonymity are considered as useful tools when they are supported by the infrastructure and not implemented solely. Langh-

einrich did not propose solutions that support anonymity and pseudonymity. However, his approach can adopt anonymous and secure connections when needed, when supported by the underlying infrastructure or in co-operation with Privacy Enhancing Technologies (e.g. anonymizing proxies, mix-nets, etc.).

A major vulnerability of *pawS* is that the suggested privacy solutions suffer by certain weaknesses in respect to UbiComp. For instance, they are either very resource demanding (e.g. mix-nets) or infrastructure-depended (e.g. anonymizing proxies) or they are designed for a completely different operational environment (e.g. for the Internet). Furthermore, *pawS* may suffer by drawbacks regarding the protection of user anonymity. On the other hand, it can adopt anonymity techniques developed specifically for pervasive systems. Therefore, although *pawS* do not offer a high level of anonymity by itself, its effectiveness—regarding the level of anonymity—is proportional to the level offered by the underlying anonymizing solutions adopted by it.

4.2. Pervasive privacy with identity management

Identity Management ensures anonymity either by default or by user's choice. This is done through the concealment of any kind of personal or linkable data related to users. The user can, also, remain anonymous by not having a specific device address (e.g. MAC address). Nevertheless, her identification, when needed, can be achieved by providing her location. For this purpose, Identity Management could use external anonymity networks, like Mist or DC (Dining-Cryptographer (Chaum, 1988; Raymond, 2001)) networks, which sustain users' personal information hidden.

The level of anonymity offered by this approach is limited because the identification of location could compromise user's anonymity, even when using Mist networks, in accordance of the requirement of Mist functionality that was referred in Section 3.3. In the case of DC networks, the technology is inadequate to be used in a pervasive computing context, due to their resource-demanding requirements; therefore their anonymity approaches might be also inappropriate and unacceptable for UbiComp.

Another argument, regarding the inefficiency of identity management for the provision of anonymity services in UbiComp, can be drawn by the definitions of anonymity and unlinkability. As mentioned, an anonymity metric lies with the size of the anonymity set. So, a subject can only be anonymous within a group of other subjects.

In the example with the bus timetable, presented in (Muhtadi et al., 2002), the user's PDA interacts with an appropriate device in a bus stop. The device's task is to announce the timetable to users whenever requested. The communication between the device and the user's PDA is done anonymously through the use of anonymous identity (e.g. anonymous username) by identity management. In this scenario, if we are the only user getting such information, then the size of the anonymity set is 0 and thus we have no anonymity for an external observer, despite the fact that no redundant personal information are concealed. In this example, since the action (getting the timetable) is completely linkable to us, then we have no anonymity.

By using information theory it turns out that the level of anonymity, a system provides for, is given as (Steinbrecher and Kopsell, 2003):

$$d(U) = 1 - \frac{\max(H(X)) - H(X)}{\max(H(X))} = \frac{H(X)}{\max(H(X))}$$

where $H(X) = -\sum_{i=1}^{n} p_i \log_2(p_i)$ stands for the a posteriori entropy of an attacker and $p_i = P_a(X = u_i)$ stands for the attacker's a posteriori probability that user u_i executed the action a. Using the previous example, if we are the only user getting such information, then the attacker's a posteriori probability that we executed this action is $p_i = 1$. Therefore, $d(U) = 0$ and we have no anonymity.

Another drawback of identity management is that the identity manager can determine the current identity of a user by scanning the context. This may imply the misinterpretation of the context, resulting in a situation where a user's identity might be disclosed.

4.3. Privacy preserving through Mist protocol

Mist communications can achieve location privacy and connection anonymity. Alongside, the use of session keys in all phases ensures the confidentiality of messages. In the case of Mist approach, there might be several cases where the anonymity of a user can be compromised. For example:

- If the user's Portal and Lighthouse are the same Mist router, then the location and identity of the user can be revealed. However, because the trust is distributed in the system and the Lighthouses and Portals cover various domains, such collusion may hardly be feasible.
- In the case of two communicating parties, if their Lighthouses collude, then the connection is no longer anonymous.
- In the case of two communicating parties, if the Lighthouse of one colludes with the *lookup* service, then the other's identity can be exposed.

The developers of Mist made the assumption that the spaces that system supports do not contain cameras or voice recognition devices, otherwise the users will have to take additional countermeasures to protect their identity. However, in real life scenarios this is difficult to happen, especially since most users' interactions take place in open environments. Hence, the number of cases in which a Mist can be used for anonymizing connections are significantly reduced. Furthermore, if Mist operates in areas where the aforementioned assumption is not taken into account, then a false sense of anonymity can be provided to the users.

4.4. Protecting location privacy using mix-zones

Mix-zones, when implemented with appropriate parameters (e.g. specific application zones, number of users participate in a zone, the size of anonymity set, etc. (Beresford and Stajano, 2003)), can provide a high level of anonymity. On the other hand, if a mix zone's diameter is larger than the distance a user can cover during one location update period (update of information about mix-zones provided by the middleware, as mentioned in Section 3.4), then mixing of the users may not be adequate. This inadequacy of mixing can lead to a lower degree of anonymity or even to the disclosure of a user's identity.

In addition, frequent alterations of pseudonyms for each application may offer a higher level of anonymity, because the use of the same pseudonym for a long time increases significantly the chances of the user's identification being disclosed.

Table 1
Level of anonymity offered by various approaches in UbiComp

Approach	Satisfaction of anonymity criteria	Comments	Level of anonymity
Privacy awareness system (*pawS*)	①: Low ②: Medium ③: Medium ④: Medium ⑤: High ⑥: None	Flexible design; adoption and co-operation with preferred anonymizing solutions; the level of anonymity is proportional to the adopted anonymizing solutions	Flexible
Identity management	①: High ②: Medium ③: Low ④: Medium ⑤: Low ⑥: None	Level of anonymity offered is highly situational depended; high level of anonymity for specific environments	Medium
Mist protocol	①: High ②: High ③: Medium ④: High ⑤: High ⑥: None	Offers location privacy, connections anonymity and messages confidentiality offered; drawbacks for some specific scenarios and in uncontrolled environments	High
Mix-zones	①: High ②: High ③: High ④: High ⑤: None ⑥: None	Combination of frequent alterations of pseudonyms and mix-zones; its high anonymity level depends on the use of specific parameters of the mix-zones	(Very) High
Privacy mirrors	①: Low ②: Low ③: Low ④: Low ⑤: Medium ⑥: None	Indirect assurance of anonymity; depends on users' knowledge about each system and on their actions; difficult for novice users	Minimum
Faces	①: Medium ②: Medium ③: High ④: Medium ⑤: Low ⑥: None	Abstract model; no implementation proposed; anonymity level depends on each proposed implementation	Flexible
Information spaces—privacy tagging	①: High ②: High ③: High ④: High ⑤: Medium ⑥: None	High level of anonymity in trusted environments; based mainly on the representational accuracy presented by an object	High

Legend: ①: Advantages and limitations of anonymity assurance level as indicated by the researchers of proposing each mechanism. ②: Theoretical justification and specific results concerning the validation of each mechanism in practical scenarios. ③: Consideration of UbiComp characteristics and constraints. ④: Transparency of the proposal related to users' participation. ⑤: Scalability of the proposed model. ⑥: Response and reaction of the mechanisms by supporting and offering appropriate actions to end-users, when the level of anonymity offered is below a specific threshold.

4.5. Privacy mirrors

Privacy mirrors increase the transparency of the system from the users' perspective. This is achieved by increasing the users' awareness of the systems characteristics and of its internals operations (e.g. how the exchange of data takes place). By this way a user could control the personal data "flowed" in the system and thus ensure her anonymity indirectly. However, privacy mirrors do not offer a direct protection of users' Identity and, as such, they do not offer anonymity capabilities.

4.6. A conceptual model of privacy in UbiComp

In the conceptual model of everyday privacy, anonymity can be ensured by the use of faces and, specifically, by the use of the *anonymous* face. However, since its developers did not propose any specific implementation, it may be assumed that the level of anonymity offered is proportional to any implementation of the faces model.

The faces model uses an operational logic, which is similar to the identity management model. This similarity can be demonstrated through the similar approach it adopts, i.e., each user shows a different face/appearance in the different situations in which she is involved. Therefore, the problems of the first model stand for the second, too. Moreover, due to the abstract nature of the proposed model, the level of anonymity cannot be measured through information theory or the formula introduced in (Steinbrecher and Kopsell, 2003).

4.7. Privacy tagging model for privacy control in UbiComp

Information spaces and privacy tagging may ensure a high level of anonymity. This is based on the representational accuracy an object presents (i.e., the simplicity of distinguishing it between other objects, or the level of accuracy in identifying it). The user can exploit this accuracy and achieve intentional ambiguity about his identity by staying anonymous in an identity query. However, this assumption is only applicable in the case when a pervasive system is trusted (especially the agents that protect users and the interactions among them).

Table 1 summarizes the reviewed mechanisms and presents the level of anonymity each approach provides for. As mentioned, the overall anonymity level is evaluated through the anonymity criteria presented in Section 4.

5. Conclusions

Pervasive computing is expected to use invisible devices, acting ubiquitous on behalf of users; as such, it may become a serious threat to privacy. Furthermore, pervasive computing provides an intrinsic contradiction: on one hand a computing environment must be highly knowledgeable about a user, in order to conform with her needs without explicit interactions, and, on the other hand, a system that is truly ubiquitous will include numerous physical locations of users and of and service providers. This situation introduces new privacy risks (e.g. location privacy issues) and makes the development of more effective privacy-protection technologies essential.

Anonymity, a basic tool for privacy-preserving pervasive systems, is an important issue to ignore. In pervasive computing systems, configuration and application behavior change dynamically, as the users make use different devices or move between different physical places. Therefore, even though the technology behind anonymity services is well established, the existing approaches may not be effective in a UbiComp context.

In this paper we examined whether the existing mechanisms are adequate for the protection of privacy in a UbiComp environment, with an eye towards the level of anonymity offered. The evaluation performed was based on specific anonymity criteria, as well as on the difference between the current well-established technologies (e.g. Internet) and the pervasive environments. The most important findings are:

- Although there are mechanisms, which offer an adequate level of anonymity, most of them are theoretical frameworks without specific implementations. On the other hand, wherever specific implementations exist (e.g. Mist), these are limited, in the sense that they do not meet all the privacy principles.
- There are no mechanisms, which can support a user's reaction when the level of anonymity offered is considered not sufficient.
- Scalability is an issue not addressed by the existing mechanisms. The development of a privacy-preserving model should take into account not only the large number of participating entities in a UbiComp system, but also the interactions between several systems.
- Privacy refers to trust; therefore, trust is a basic concept in the context of UbiComp mainly due to the large number of entities operating in such environments. No approach recognizes adequately the importance of trust in UbiComp.

Personal data processing will continue to increase and may erode privacy. What the users need is appropriate means and solutions, which facilitate the emergence of UbiComp, while, at the same time, reduce the risks to the users personal data.

Acknowledgements

The authors would like to thank John Mallios for his helpful comments and suggestions during the initial preparation of this paper.

References

Adams, A., 1999. The implications of users' privacy perception on communication and information privacy policies. In: Proceedings of Telecommunications Policy Research (TPRC), USA.

Beresford, A., Stajano, F., 2003. Location privacy in pervasive computing. IEEE Pervasive Computing 2 (1), 46–55.

Chaum, D., 1988. The dining cryptographers problem: unconditional sender and recipient untraceability. Journal of Cryptology 1 (1), 65–75.

Fasbender, A., Kesdogan, D., Kubitz, O., 1996. Analysis of Security and Privacy in Mobile IP. In: Proceedings of 4th International Conference on Telecommunication Systems, Modelling and Analysis, Nashville, TN.

ISO/IEC 15408, 1999. Information Technology—Security Techniques—Evaluation Criteria for IT Security.

Jendricke, U., Kreutzer, M., Zugenmaier, A., 2002. Pervasive privacy with identity management. In: Proceedings of the Workshop on Security in Ubiquitous Computing, UbiComp 2002, Sweden.

Jiang, X., Landay, J., 2002. Modelling privacy control in context-aware systems. IEEE Pervasive Computing 1 (3), 59–63.

Kesdogan, D., Reichl, P., Junghðrtchen, K., 1998. Distributed temporary pseudonyms: a new approach for protecting location information in mobile communication networks. In: Proceedings of 5th European Symposium on Research in Computer Security, Lecture Notes in Computer Science, vol. 1485, pp. 295–312.

Lahlou, S., Jegou, F., 2004. European Disappearing Computer Privacy Design Guidelines (Version 1.1), Ambient Agoras Programme Report (IST-2000-25134). Disappearing Computing Initiative.

Lahlou, S., Langheinrich, M., Rocker, C., 2005. Privacy and trust issues with invisible computers. Communications of the ACM 48 (3), 59–60.

Langheinrich, M., 2001. Privacy by design—principles of privacy—aware ubiquitous systems. In: Proceedings of the 3rd International Conference on Ubiquitous Computing, Lecture Notes in Computer Science, vol. 2201, pp. 273–29.

Langheinrich, M., 2002. A privacy awareness system for ubiquitous computing environments. In: Proceedings of UbiComp 2002. Lecture Notes in Computer Science, vol. 2498, pp. 237–245.

Lederer, S., Dey, A., Mankoff, J., 2002. A conceptual model and a metaphor of everyday privacy in ubiquitous computing environments. Technical Report CSD-02-1188, University of California, Berkeley, USA.

Leonhardt, U., Magee, J., 1998. Security considerations for a distributed location service. Journal of Network and Systems Management 6 (1), 51–70.

Lessig, L., 1998. The architecture of privacy. In: Proceedings of the Taiwan NET '98 Conference, Taipei, Taiwan.

Muhtadi, J.Al., Campbell, R., Kapadia, A., Mickunas, M., Yi, S., 2002. Routing through the mist: privacy preserving communication in ubiquitous computing environments. In: Proceedings of the International Conference on Distributed Computing Systems (ICDCS 2002), Austria.

National Institute of Standards and Technologies (NIST), 2001, About Pervasive Computing. Available from: <http://www.nist.gov/pc2001/about_pervasive.html> (retrieved 2 April 2005).

Nguyen, D., Mynatt, E., 2002. Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems, Technical Report GIT-GVU-02-16, Georgia Institute of Technology, USA.

Organisation for Economic Co-operation and Development (OECD), 1980. Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data.

Pfitzmann, A., Kohntopp, M., 2000, Anonymity, unobservability and pseudonymity—a proposal for terminology, In: Proceedings of the International Workshop on the Design Issues in Anonymity and Observability, International Computer Science Institute (ICSI), Berkeley, California, USA.

Raymond, J.F., 2001. Traffic analysis: protocols, attacks, design issues and open problems. In: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, Lecture Notes in Computer Science vol. 2009, pp. 10–29.

Russell, D., Streitz, N., Winograd, T., 2005. Building disappearing computers. Communications of the ACM 48 (3), 42–48.

Satyanarayanan, M., 2002. A catalyst for mobile and ubiquitous computing. IEEE Pervasive Computing 1 (1), 2–5.

Steinbrecher, S., Kopsell, S., 2003. Modelling unlinkability, In: Proceedings of the 3rd International Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science, vol. 2760, pp. 32–47.

Weiser, M., 1991. The computer for the 21st century. Scientific American 265 (3), 94–104.