To appear in the Proceedings of the International Conference on Availability, Reliability and Security (AReS), IEEE CS Press, Vienna, Austria, April 2007

Privacy in Pervasive Computing and Open Issues

Pankaj Bhaskar and Sheikh I Ahamed
Dept. of Math., Stat. and CS, Marquette University, Milwaukee, WI, USA
{pankaj.bhaskar, sheikh.ahamed}@marquette.edu

Abstract

Privacy appears as a major issue for pervasive computing applications. Several models have been proposed to address privacy challenges. Successful design requires awareness of the technology's users and that their desires and concerns are understood. This is difficult as few empirical researches exist about potential pervasive users that designers can use. Complicating design further is the fact that pervasive systems are typically embedded or invisible, making it difficult for users to know when these devices are present and collecting data. As users have a limited understanding of the technology several privacy, design, and safety issues are raised. This paper discusses how privacy might be preserved in a pervasive computing environment. It presents some research developments in these areas to address privacy concerns. Open issues and challenges are also examined.

Keywords: Pervasive Computing, Trust, Privacy, Security, Location Privacy

1. Introduction

With the increase of handheld devices and wireless networks, pervasive computing has become integral part of our life. A pervasive computing environment unobtrusively and transparently supports the human beings with its embedded computation and communication [1]. This embedding ensures transparent interaction of the devices with the users [2].

Privacy can be defined as “the privilege of users to determine for themselves when, how, and to what extent information about them is communicated to others” [3]. Thus privacy in pervasive computing can be perceived as an entitlement of users for control over collection and dissemination of information related to them. These users can be individuals, groups, or organizations.

To protect privacy a user can be notified of requests for information. But for pervasive technology to become truly ubiquitous, it should merge into the background and become a part of everyday life. Researchers [1-5, 47] have recognized that embedded technology's unobtrusiveness both hinders and supports its capability for development and use of potentially invasive applications [4]. Users’ inability to see a technology makes it difficult for them to understand how it might affect their privacy. Unobtrusiveness however is a reasonable and required goal because pervasive systems should minimize the demands on users.

Location privacy is a particular type of information privacy that can be defined as “the ability to prevent other parties from learning one’s current or past location” [5]. Until recently the concept of location privacy was unknown as reliable and timely information about the exact location of others was not available. Most people did not perceive any privacy implications in revealing their location except in certain situations but with pervasive computing the scale of the problem has changed considerably. It is a major concern if someone can inspect the history of all past movements of a user that has been recorded continuously. This “change in scale of several orders of magnitude is often qualitative as well as quantitative and is a recurring problem in pervasive computing” [5]. With increase in location-based applications protecting personal location information has become a major challenge [5, 6, 47]. To address this challenge a mechanism is required that lets users control their location information automatically [6, 47].

With growing concern about privacy in pervasive computing environments, considerable research has been conducted focusing on various aspects. Solutions and models put forth by this research address specific challenges of the problem. In this paper, the discussion will focus on the characteristics of the problem and how the works done in this field addresses these challenges.

Section 2 will discuss the background for privacy. Section 3 will explore characteristics of the problem domain. Section 4 will list some challenges for protecting privacy in pervasive computing. Section 5 will explore related works along with a comparison of their strengths and weaknesses vis-à-vis the challenges. Section 6 will present a comparison table for challenges addressed by various research works. Section 7 will describe some of the open issues for further research.

2. Background

Several countries have laws that provide privacy as a right to their citizens [5]. One of the first pieces of privacy legislation is England's 1361 Justices of the Peace Act, under which eavesdroppers and stalkers could be arrested. The Fourth Amendment to the US Constitution provides privacy rights to citizens. The United Nations stated in its 1948 Universal Declaration of Human Rights that everyone has a right to privacy [7]. This declaration has served as a guiding principle for later legislations regarding privacy. The Global Internet Liberty Campaign identifies four categories for privacy: information privacy, bodily privacy, communications privacy, and territorial privacy [5, 8].

3. Characteristics of the Problem

Research in pervasive computing has focused on developing applications that enable users to collect, communicate, save, organize, and reuse information [18]. Pervasive services are provided through countless invisible devices embedded in the user environment that might be work related or personal. This continuous information collection exposes personal behavior, habits, preferences, aversions, and associations [10]. Privacy and security of this information has not been given enough consideration. In addition pervasive computing applications rely heavily on mobile and wireless communications that brings up new privacy issues.

The privacy breach can be due to misuse by a pervasive service provider or network traffic analysis by an intruder [11]. Privacy sensitive information is available to pervasive service providers continuously making it difficult to protect it. Stealing sensitive information through analysis of traffic might be constrained with use of cryptography but it is still possible to glean some information like identity, location and activities. Under any situation it is important to ensure that users don't feel they are being spied on and using the services exposes them to unexpected threats and misuse of context and private information. The challenge here is to provide a service that is based on location and context without revealing identity which in some ways is paradoxical. New technologies like RFID (Radio Frequency Identification) have on one hand made pervasive computing a reality but on the other hand have caused concerns about privacy as users are tracked when they move around. Laws such as the Patriot Act are also causing concerns that not only can hackers but also law enforcement agencies can intrude on the privacy of individuals. Protection of private and sensitive information is mandated under laws such as HIPAA (Health Insurance Portability and Accountability Act) and the European Union's Data Protection Directive, but their implementation in the Pervasive Computing realm is complicated [9, 12].

Privacy of location information deals with controlling access to the huge amount of sensitive information that might be generated when location systems continuously track users [5]. The user would not want to stop all access because some applications can use this information to provide critical services like public safety, transportation, emergency response, and disaster management [13], but there is a need for the user to be in control [5].

4. Challenges to Privacy Protection

4.1. Unobtrusiveness

The goal of pervasive computing is to be unobtrusive. For this purpose, technology is embedded into everyday objects that transmit and receive information. This "embedding" reduces the visibility of the pervasive computing environment surrounding the user and makes the technology more friendly and acceptable [33]. Ironically, the same characteristic makes it possible to invade the privacy of the user without the user realizing it. This leaves the users with limited control over their own privacy and also adds the responsibility that they do not intrude on privacy of others. This invasion and responsibility cannot be managed or imposed through social and organizational controls [18].

There is a need to find a balance between usability and privacy. Traditional models requiring explicit user input have to be replaced with models that can sense information securely and automatically from the context and environment, and exchange it seamlessly with communicating devices and users [14]. A single-sign on feature to enable single-step authentication to multiple applications can be a solution. The extension of such models to truly pervasive environments still remains a challenge.

4.2. Location Dependency

Pervasive computing applications make use of location information to provide services including local information access (traffic reports, news, navigation maps) and nearest-neighbor services (locating nearby restaurants) [15]. To utilize these location-based services, the users have to make their location known to the service provider. The access to location information about a user can provide opportunity for its misuse. Location is privacy-sensitive information that is available readily making its protection a challenge. There is also the added requirement for the services to be flexible enough to support different location privacy policies based on situation. For example a user might want location privacy but change this need in case of an emergency to pinpoint and communicate the exact location [14].

4.3. Context Dependency

Pervasive computing applications also depend on context information. This information can include the type of wireless device used by the application, GPS coordinates, user profiles, user preferences, current time, etc. [16]. The ability to use contextual information to enhance traditional user attributes is important for making privacy protection less intrusive [14]. Providing sufficient protection for context information is difficult as context-aware systems deal with sets of information that might have different privacy requirements due to variance in sensitivity and user preference [17]. However there is a lack of protocols and infrastructure for securely collecting, validating, and using contextual information [14].

4.4. Amount of Data Collection

Compared to current computing technology, pervasive computing implementation relies on an increased amount, quality, and accuracy of data generated and collected. This is also enhanced by increasing capabilities to process and analyze the data. This sheer amount of data collection and processing leads to users frequently ignoring or being deprived from the decision of release of personal data.

In addition, pervasive computing environments have a majority of wireless devices. These devices have limitations for processing power, bandwidth, throughput, memory etc [14]. These factors put a resource limitation on elaborate models and protocols for privacy protection that might depend on extensive use of these resources.

4.5. Role of Service Provider

The role of the service provider as maintainer and preserver of the privacy sensitive data is critical. There are numerous opportunities for misuse of data passing through the devices of the service provider. The Platform for Privacy Preferences (P3P) of the World Wide Web Consortium (W3C) provides a specification that can be used to ensure that each data request by the service providers also specifies purpose, retention, and recipients of the data [10]. In the real-world ensuring that all service providers follow the rules is difficult.

4.6. Lack of ownership

Resources in a traditional computing system have ownership and access control. On the other hand pervasive computing environments “permit looser and more dynamic couplings between people and resources, thereby invalidating the usual approaches to ownership and control of resources” [17]. For example a user has no control over a camera recording activities in a room where the user is. It is difficult to implement privacy control when ownership cannot be easily determined.

5. Related Works

Several projects and models have already addressed the concerns of privacy protection in pervasive computing. Some of these works are discussed here along with their strengths and weaknesses.

5.1. PSIUM

Privacy Sensitive Information Diluting Mechanism (PSIUM) is a model that tries to eliminate the misuse of user data by the service providers [11]. The model achieves this by reducing the usefulness of the data collected by the service providers without affecting the service provided to the users. A PSIUM-enabled device sends multiple location-based service request messages to the service provider. All but one of these messages contains the true location. On return of service information the device knows to utilize the correct information and make it available to the user. PSIUM maintains false data that appears realistic so that it is difficult to distinguish it from the actual true data. This false data is created from locations previously used by the user. The strength of PSIUM is in preventing misuse of users’ data by a service provider without reducing the quality of the service. Its weakness is that

it increases the cost of obtaining results from the service provider as the number of queries is increased.

5.2. Mix Networks and Mix Nodes

A mix network is a store-and-forward network that offers anonymous communication facilities [5]. The network contains normal message-routing nodes alongside special mix nodes. Even hostile observers who can monitor all the links in the network cannot trace a message from its source to its destination without the collusion of the mix nodes. In its simplest form, a mix node collects *n* equal-length packets as input and reorders them by some metric before forwarding them, thus providing unlinkability between incoming and outgoing messages. The number of distinct senders in the batch provides a measure of the unlinkability between the messages coming in and going out of the mix. The advantage of this model is that it provides privacy protection even when data flowing through the environment is compromised. Its weakness lies in its vulnerability of communication between the user device and the service provider.

5.3. Pseudonyms and Mix-Zones

Traffic analysis attacks can be used to analyze encrypted messages due to the vulnerability of the communication path between a client device and the service provider. This analysis can lead to inference of the identity, location and activities of the users [11]. To address this problem the concept of frequently changing pseudonyms and mix zones is introduced [24]. To enhance anonymity users change pseudonyms frequently and adopt unused pseudonyms for each application with which they interact. Even changing Pseudonyms might be compromised through tracking. To address this vulnerability mix zones are used. Mix-zones are defined as "connected spatial regions of maximum size in which none of these users has registered any application callback" whereas an application zone is defined as an "area where a user has registered for a callback" [11]. Users are made to pass through mix zones through usage of the mix zones and application zones. The transactions between the users and the applications are suspended inside a mix zone that causes unlinking with user's new pseudonym. The strength of this model lies in its ability to protect privacy in the communication between user device and service provider. On the contrary this is a complex model that is difficult to design and implement.

5.4. Feedback and Control for Privacy in RAVE

EuroPARC's RAVE system used principles of Feedback and Control for enhancing privacy [18]. Control is defined as "Empowering people to stipulate what information they project and who can get hold of it". Feedback is defined as "Informing people when and what information about them is being captured and to whom the information is being made available". Users of the RAVE system can control who can connect to them and what kind of connections each person is allowed to make. Feedback provided by the RAVE system makes the users aware of what data is being sent to the system and who has access to use that data. The success of this system is in enabling people to orient themselves to the technology. Its main drawback is that the boundaries between awareness, privacy, and intrusion are easily breached.

5.5. Information Space Model

Information Space organizes information, resources, and services around privacy-relevant contextual factors [19]. Information spaces define different boundaries and have owners that determine its permissions. With the boundaries and permissions information spaces provide for information, resources, services, and authorizations management in context-aware systems. For privacy control an information space boundary acts as a trigger to enforce permissions defined by owners of that space. This model protects sensitive information through control of the information through trusted owners. It is this same trust that is a weakness in this model as the assumption of trustworthiness of the metadata as well as the software component that processes the metadata can be problematic for large-scale decentralized systems.

5.6. LocServ

LocServ supports various location-based applications and is a middleware service that lies between location-based applications and location-tracking technologies [6]. By unifying location tracking technologies LocServ lets location-based applications use multiple positioning systems. Users can specify a location query using various symbolic or geometric location models and the service can resolve the queries using various underlying technologies. Such a service requires mechanisms for controlling access to users' location information without repeated user intervention. This gives users control over the release of their location information and provides a general framework that lets users apply policies to control distribution of their information. Various factors are

used to make this model work. These include the type of organization or application requesting the data together with its information retention and distribution policies and, a mechanism for consulting external entities such as application-specific modules before releasing information. This system protects the location privacy of a user when arbitrary third party location-based applications query the location server.

5.7. Mist

Mist is a communication infrastructure that aims to preserve privacy in pervasive computing environments [20]. It achieves this by separation of location from identity and thus allowing authorized users of the system to access services while protecting their location privacy. Mist works through a privacy preserving hierarchy of specialized routers that form an overlay network. This network provides private communication by routing packets in a hop-by-hop, handle-based routing protocol. Public key cryptography is used in the setup of these handles. Using this mechanism the communication is made untraceable to hackers and unintended parties.

Mist provides a customizable level of privacy. Its usefulness however is defined by the choice of the user and if the user chooses a connecting router at a lower hierarchy then the protection is lower too.

5.8. Interaction History

Pervasive Computing environments lack trust between different component parties making it difficult to use identity-based authentication and public key infrastructure [21]. This method proposes to address the privacy problem by authenticating based on the interaction history of the entities. This history will be made of credentials that show that interaction took place. A credential is created after each interaction and it is later used to prove the interaction. The credential is encrypted and can be accessed only by the credential creator and other trusted members of the environment. To maintain privacy the credential creator cannot trace users through the created credentials. Blind signatures can be used to ensure that signatures are not recognized. Using this mechanism privacy of user information is maintained. The history of user interactions can be used when communicating with the service provider or a trusted partner without the users being linked to previous event and without revealing their identity. This makes untraceability and anonymity possible.

5.9. Geopriv

The Internet Engineering Task Force (IETF)'s Geopriv working group has focused on the need to "securely gather and transfer location information for location services, while at the same time protecting the privacy of the individuals involved" [6]. The Geopriv model involves creating location objects that encapsulate user location data and associated privacy requirements. These location objects can be made tamper resistant by digitally signing them making it similar to digital rights management schemes that protect digital media from illegal distribution. Geopriv's coupling of data and privacy metadata offers accountability when location information has been passed between multiple applications.

5.10. pawS

*pawS (P*rivacy Awareness System) [46] provides users with tools that let them protect their personal privacy and help others respect that privacy. This system is based on respect and social and legal norms rather than rigorous technical protection of private information. In a pawS enabled system when a user enters an environment in which services are collecting data, a privacy beacon announces the privacy policies of each service in the environment. A user's privacy proxy checks these policies against the user's predefined privacy preferences. If the policies agree, the services can collect information and users can utilize the services. If the policies don't agree, the system notifies the user, who can choose not to use the service in question or leave the area in which the information collection is occurring.

5.11. Spirit

Spirit [5] provides applications with a middleware event model through which entities entering or exiting a predefined region of space generate events. Applications register their interest in a particular set of locations and entities that can be located. The applications receive callbacks when the registered events occur. Current location-aware middleware provides open access to all location events, but this architecture can be enhanced to let users control the dissemination of their own location information.

5.12. Quality of Privacy

Quality of Privacy (QoP) [22] allows balancing the trade-off between the amount of privacy a user is willing to concede and the value of the services that can be provided by a pervasive application, in a similar

way as that of Quality of Service (QoS). QoP is based on five elements; location, identity, access, activity, and persistence. Based on this a user can demand a certain level of QoP to the pervasive environment using a qualitative measure. The perception of anonymity is then mapped by the system to certain values of one or more contextual elements. This provides an agent-based architecture that adapts the behavior of the pervasive application to the users' context, in order to satisfy the level of QoP that both the application and the user have agreed upon.

6. Comparison of Related Work

The discussed research works address some of the challenges of privacy protection. Table 1 presents a comparison of the challenges addressed.

Table 1. Challenges addressed

	Unobtrusiveness	Location Dependency	Context Dependency	Amount of Data Collection	Role of Service Provider	Lack of ownership
PSIUM [11]	X	X	X	X	√	X
Mix networks and Mix Nodes [5]	X	X	X	X	√	X
Pseudonyms and Mix-Zones[24]	X	√	√	X	√	X
RAVE [18]	√	X	X	X	X	√
Information Space Model[19]	X	X	X	X	√	√
LocServ [6]	√	√	X	X	√	√
Mist [20]	√	√	√	X	√	X
Interaction History [21]	√	X	X	X	√	X
Geopriv [6]	X	√	X	X	√	√
pawS [46]	√	X	X	X	√	√
Spirit [5]	√	X	X	X	√	√
Quality of Privacy[12]	√	√	√	X	√	X

The comparison illustrates that extensive work has been done to address the Role of Service Provider. Unobtrusiveness, Lack of Ownership, and Location Dependency have also been given considerable attention. Amount of Data Collection and Context Dependency appear to be the difficult areas with none or little focus.

7. Open Issues

The challenges in the area of privacy protection are being addressed by research work in pervasive computing. Still there are open issues that need future work.

7.1. Insufficient Privacy Response

The problem is to model the user's response to the level of privacy falling below a certain threshold. The applications will become unresponsive if the service provider stops providing information. Alternatively the user might be presented with many messages or will just believe that they are still receiving service when they are not [5]. This reconciliation of privacy with application functionality is an open problem.

7.2. Scalability

Most of the research work has been done on experimental data from controlled environments, covering a relatively small area and user population. These models developed in the test environment still have to prove scalability when they are applied to a wider area and larger population [5].

7.3. Changing Environment

Users will typically move between different pervasive computing environments and interface with different devices and applications [14]. As users roam from one environment to another their data and in some cases their applications may also move with them. It is a challenge to design models and services that support this mobility including the scenario that users might also pass through zones of no service.

7.4. Private Information Retrieval

Some applications or users require services without providing or using any user identifiable information. This constitutes a problem similar to domain of private information retrieval (PIR) protocols [11]. This provides data retrieval with queries that require user information without disclosing the same information. Developments of applications that provide private information retrieval have not been given sufficient attention in pervasive computing.

7.5 Avoiding Privacy Violation for Resource Sharing

Availability of information regarding users may lead to privacy violations while communicating with others for services and resources. Providing a model to resolve this issue in pervasive computing environment is a major challenge to achieve ubiquity.

8. Conclusion

In this paper, the various aspects of privacy preservation in pervasive computing have been discussed. This is an area that had not been given much attention earlier but recent research has addressed some of the challenges. The interest in privacy issues has been caused by legal mandates and concerns raised by users. Several works in this area were presented and their strengths and weaknesses evaluated. Key open issues that need further work have also been discussed. Privacy is a real concern in pervasive computing and it should be considered appropriately and made a part of design for acceptance of pervasive technologies in everyday life.

9. References

[1] J. Seigneur, C. D. Jensen, "Ubiquitous computing (UC): Trust enhanced ubiquitous payment without too much privacy loss", *Proceedings of the 2004 ACM symposium on Applied computing*, March 2004

[2] M. Haque, S. I. Ahamed, "Security in Pervasive Computing: Current Status and Open Issues", *International Journal of Network Security*, Volume 3, November 2006, pp. 203-214

[3] J. I. Hong, J. A. Landay, "Support for location: An architecture for privacy-sensitive ubiquitous computing", *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, June 2004

[4] R Beckwith, "Designing for ubiquity: the perception of privacy", *Pervasive Computing*, IEEE Volume 2, Issue 2, April-June 2003, pp. 40-46

[5] A. R. Beresford, F. Stajano, "Location Privacy in Pervasive Computing", *Pervasive Computing*, IEEE, Volume 2, Issue 1, Jan-Mar 2003, pp. 46-55

[6] G. Myles, A. Friday, N. Davies, "Preserving privacy in environments with location-based applications", *Pervasive Computing*, IEEE Volume 2, Issue 1, Jan-Mar 2003, pp. 56-64

[7] D. Henrici, P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, March 2004, pp. 149-153

[8] D. Banisar and S. Davies, "Privacy and Human Rights", www.gilc.org/privacy/survey

[9] V. Stanford, "Pervasive health care applications face tough security challenges", *Pervasive Computing*, IEEE, Volume 1, Issue 2, April-June 2002, pp. 8-12

[10] J. Cas, "Privacy in pervasive computing environments - a contradiction in terms?", *Technology and Society Magazine*, IEEE, Volume 24, Issue 1, Spring 2005, pp. 24-33

[11] H. S. Cheng, D. Zhang, J. G. Tan, "Protection of Privacy in Pervasive Computing Environments", *International Conference on Information Technology: Coding and Computing*, 4-6 April 2005, pp. 242-247

[12] A. R. Jacobs, G. D. Abowd, "A Framework for comparing perspectives on privacy and pervasive technologies", *Pervasive Computing*, IEEE, Volume 2, Issue 4, Oct-Dec 2003, pp. 78-84

[13] C. K. Lee, W. C. Lee, H. V. Leung, "Nearest Surrounder Search", *IEEE International Conference on Data Engineering*, April 2006

[14] R. K. Thomas, R. Sandhu, "Models, protocols, and architectures for secure pervasive computing: challenges and research directions", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 14-17 March 2004, pp. 164-168

[15] D. L. Lee, J. Xu, B. Zheng, W. C. Lee, "Data Management in Location-Dependent Information Services", *Pervasive Computing*, July-September 2002, pp. 65-72

[16] D. F. Ferguson, "Web Services Architecture: Direction and Position Paper", *W3C Web Services Workshop*, April 2001

[17] K. Henricksen, R. Wishart, T. McFadden, J. Indulska, "Extending context models for privacy in pervasive computing environments", *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, 8-12 March 2005 pp.20-24

[18] V. Bellotti, A. Sellen, "Design for Privacy in Ubiquitous Computing Environments", *Proceedings of 3rd European Conference on Computer Supported Cooperative Work*, 1993, pp. 77-92

[19] J. Xiaodong, J. A. Landay, "Modeling privacy control in context-aware systems", *Pervasive Computing*, IEEE, Volume 1, Issue 3, July-Sept. 2002, pp. 59-63

[20] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, M. D. Mickunas, "Towards Security and Privacy for Pervasive Computing", *Proceedings of International Symposium on Software Security*, 2002

[21] L. Bussard, Y. Roudier, R. Molva, "Untraceable secret credentials: trust establishment with privacy", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 14-17 March 2004, pp.122-126

[22] M. Tentori, J. Favela, M. D. Rodriguez, V. M. Gonzalez, "Supporting Quality of Privacy (QoP) in Pervasive Computing", Sixth Mexican International Conference on Computer Science, 26-30 Sept. 2005, pp. 58-67

[23] D. M. Konidala, D. N Duc, L. Dongman, K. Kwangjo, "A capability-based privacy-preserving scheme for pervasive computing environments", *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, 8-12 March 2005, pp. 136-140

[24] A. R. Beresford, F. Stajano, "Mix Zones - User Privacy in Location-aware Services", *International Workshop on Pervasive Computing and Communication Security*, IEEE, Mar 2004

[25] M. Jacobsson, I. Niemegeers, "Privacy and anonymity in personal networks", *Third IEEE International Conference on Pervasive Computing and Communications Workshops*, 8-12 March 2005, pp. 130-135

[26] L. Bussard, Y. Roudier, R. Molva, "Untraceable secret credentials: trust establishment with privacy", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 14-17 March 2004, pp. 122-126

[27] M. Hazas, A. Ward, "A high performance privacy-oriented location system", *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, 23-26 March 2003, pp. 216-223

[28] U. Hengartner, P. Steenkiste, "Avoiding Privacy Violations Caused by Context-Sensitive Services", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, 13-17 March 2006, pp. 222-233

[29] Z. Feng; M. W. Mutka, M. Lionel, "The Master Key: A Private Authentication Approach for Pervasive Computing Environments", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, 13-17 March 2006, pp. 212-221

[30] K. Henricksen, J. Indulska, "A software engineering framework for context-aware pervasive computing", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications*, 2004, pp. 77-86

[31] Z. Feng, M. W. Mutka, L. M. Ni, "A Private, Secure, and User-Centric Information Exposure Model for Service Discovery Protocols", *IEEE Transactions on Mobile Computing*, Volume 5, Issue 4, July-Aug. 2006, pp. 418-429

[32] A. Applewhite, "What knows where you are?" *Pervasive Computing*, IEEE Volume 1, Issue 4, Oct.-Dec. 2002, pp. 4-8

[33] D. Hong, M. Yuan, V. Y. Shen, "Social communication: Dynamic privacy management: a plug-in service for the middleware in pervasive computing", *Proceedings of the 7th international conference on Human computer interaction with mobile devices & services*, September 2005

[34] M. S. Ackerman, "Privacy in pervasive environments: next generation labeling protocols", *Personal and Ubiquitous Computing*, Volume 8 Issue 6, November 2004

[35] G. Iachello, G. D. Abowd, "Privacy 1: Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing", *Proceedings of the SIGCHI conference on Human factors in computing systems*, April 2005

[36] B. Dragovic, J. Crowcroft, "Ubiquitous computing: Information exposure control through data manipulation for ubiquitous computing", *Proceedings of the 2004 workshop on New security paradigms*, September 2004

[37] J. A. Halderman, B. Waters, E. W. Felten, "Physical privacy: Privacy management for portable recording devices", *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, October 2004

[38] C. Schmandt, M. Ackerman, "Personal and Ubiquitous Computing: Issue on privacy and security" *Personal and Ubiquitous Computing*, Volume 8 Issue 6, November 2004

[39] N. Davies, N, "Introduction security and privacy", *Pervasive Computing*, IEEE, Volume 2, Issue 1, Jan-Mar 2003, pp. 20-20

[40] R. J. Bayardo, R. Srikant, "Technological solutions for protecting privacy", *Computer*, Volume 36, Issue 9, Sept. 2003, pp. 115-118

[41] M. Gruteser, L. Xuan, "Protecting privacy, in continuous location-tracking applications", *Security & Privacy Magazine*, IEEE, Volume 2, Issue 2, Mar-Apr 2004, pp. 28-34

[42] S. Pankanti, A. Senior, L. Brown, A. Hampapur, T. Ying-Li, R. Bolle, F. Almenarez, A. Marin, M. C. Campo, R. C. Garcia, R. V. Kranenburg, "Security, privacy, and health", *Pervasive Computing*, IEEE, Volume 2, Issue 1, Jan-Mar 2003, pp. 96-97

[43] R. Kui, L. Wenjing, "Privacy enhanced access control in pervasive computing environments", *2nd International Conference on Broadband Networks*, Oct 2005, pp. 384-393

[44] M. R. Stytz, "Protecting Personal Privacy: Hauling Down the Jolly Roger", *Security & Privacy Magazine*, IEEE, Volume 3, Issue 4, July-Aug 2005, pp. 72-74

[45] P. Osbakk, N. Ryan, "A Privacy Enhancing Infrastructure for Context-Awareness", *UK-UbiNet Workshop*, September 2003

[46] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments", *Ubicomp*, Lecture Notes in Computer Science, volume 2498, pp. 237-245, Springer, 2002

[47] A. Görlach, W. W. Terpstra, A. Heinemann, "Survey on Location Privacy in Pervasive Computing", *Book chapter of Security and Trust within the Context of Pervasive Computing*, Volume 780, Springer Netherlands, 2004