Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments

Stefan G. Weber, Andreas Heinemann, Max Mühlhäuser
Telecooperation Group
Technische Universität Darmstadt
Hochschulstrasse 10, 64289 Darmstadt, Germany
{sweber,aheine,max}@tk.informatik.tu-darmstadt.de

Abstract

Privacy Preservation has been identified as an important factor to the success and acceptance of Ubiquitous Computing systems. Traceability, i.e. attributing events and actions to those who caused them, seems to be a directly contradicting goal. However, harnessing sensitive data collected by Ubiquitous Computing infrastructures for traceability applications in a privacy-respecting manner may clearly bring further benefits, for different concerned parties. Automated working hours recording and personalized insurances are first examples of such applications. To contribute to this matter, this paper presents an architecture that allows for balancing between privacy and traceability in Ubiquitous Computing environments. We describe its foundations and components and illustrate its benefits. Moreover, we discuss important existing research approaches on privacy protection and traceability applications in Ubiquitous Computing settings.

1. Introduction

Ubiquitous Computing (UbiComp) denotes "a powerful shift in computation, where people live, work, and play in a seamlessly interweaving computing environment" [27]. This vision, coined more than 15 years ago by Mark Weiser, brings along a fundamental confluence of real and digital worlds, influencing "an unprecedented share of our public and private life" [17]. In forthcoming UbiComp settings, people will work and carry out their personal everyday actions supported and observed by computers of different form and shapes. Those computers are meant to provide unobtrusive support to individuals in their everyday life tasks. One the one hand, the continual observation by Ubiquitous Computing infrastructures causes severe concerns on how individuals' privacy can be guaranteed. On the other hand, once a personal action can be comprehended by the surrounding computing facilities, it may potentially have legal or financial consequences. One can think of automated working hours recording based on employee tracking, or on charging based on a pay-per-action basis. In all these cases, an individual's right to have privacy has to be traded off against its responsibility and obligations. Especially, in the first mentioned scenario, this might be stated in a contract between an employee and his employer and illustrates a typical tradeoff between privacy and traceability. Ubiquitous Computing infrastructures that are able to document everyday life activities become a key instrument in this area of interest. One can clearly see, that there are widespread and conflicting interests concerning the use and deployment of UbiComp technologies for traceability applications. The pursuit of goals that are inherently present in real life situations among different parties of a society, i.e. individuals, organizations and the society as a whole, may be supported by these technologies. We believe that, in this context, a challenge is to investigate how UbiComp environments can be designed, in a way that allows for balancing between conflicting goals. In this paper, we especially focus on the balance between privacy and traceability. Privacy issues have been identified as one of the greatest barrier to the long term success of Ubiquitous Computing [21]. Throughout the last years, notable research efforts have been taken to understand and tackle privacy concerns of Ubiquitous Computing settings [15, 16, 2, 13, 14]. Several techniques have been proposed so far (e.g., temporal pseudonyms [2], distributed access control mechanisms [5], transparency management [16]). Yet, it remains unclear how to balance between personal privacy protection and traceability goals.

In this paper, we contribute to this matter by presenting the foundations of an architecture that allows to balance between the conflicting goals of privacy and traceability in UbiComp settings.The remainder of this paper is structured as follows: in Section 2, we outline characteristics and chal-

lenges of privacy protection in UbiComp environments. In Section 3, we discuss traceability conceptions and applications. The tradeoffs between privacy and traceability are illustrated in Section 4, by describing two scenarios. Afterwards, in Section 5, we describe the foundations of an architecture, that allows users to customize their preferences between privacy and traceability. In Section 6, we discuss related work. We draw our conclusions afterwards, in Section 7.

2 Privacy

The vision of Ubiquitous Computing bears (among others) an obvious problem: privacy - i.e. "the capability to determine what one wants to reveal and how accessible one wants to be" [1] - is under great risk. Ubiquitous Computing essentially relies on intensive collection, processing and dissemination of large amounts of data. Much of this data is related to users and can be very sensitive or of great value for several parties.

Langheinrich [15] has identified four key properties of the UbiComp vision in this context:

- **Ubiquity:** UbiComp technologies are constantly present in every aspect of life;
- **Invisibility:** Computers disappear in the environment, becoming invisible to the users;
- **Sensing:** Sensors constantly perceive sensible aspects of the environment and its users;
- **Memory Amplification:** Any collected data can be stored and made accessible later.

Several technical threats to privacy protection arise from this setting. Due to the invisibility, concrete sensor activity cannot be easily detected and thus controlled by an user. This fact may be exploited for observation and surveillance purposes. Even worse, manipulated sensor data can cause a severe privacy violation, by distorting personal data [11], e.g., incorrectly delivering location data. The operators of the sensor infrastructure may exploit their global view in their respective spheres of data collection. By this, building user profiles may be possible, while, superficially, protection mechanisms against attacks on a higher layer, e.g., access control mechanisms, may appear to be effective. Due to the memory amplification, aggregation and interpretation of acquired data can generate profiles describing in detail everyday activities of users.

Clearly, privacy is a social, ethical and legal issue, beyond technical threats. In order to establish acceptance of the UbiComp vision, protecting the privacy of users is of central importance. If those privacy concerns are not addressed appropriately, the continuous surveillance through countless sensors may be perceived as a serious downside for those living and working in smart environments.

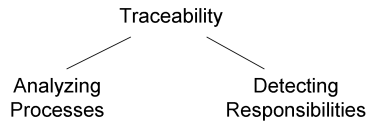

Figure 1. Basic applications of traceability

3 Traceability

Generally speaking, traceability refers to the ability to attribute events and actions to its cause or source, i.e. an object, place and/or entity. On the one hand, traceability concepts may be used for managing and analyzing processes, e.g., in the case of product traceability [19]. On the other hand, a different application is to employ traceability for detecting responsibilities of actions conducted by real persons in a UbiComp setting. This is the focus of this paper. Figure 1 illustrates those two basic fields of application.

In order to provide some level of traceability, the following basic functionalities have to be supported by a traceability system of the second kind:

1. detecting actions and events
2. identifying persons resp. their digital identities
3. attributing action to identities

In a UbiComp setting, traceability can be provided by harnessing the sensor inputs and security facilities of the environment. The quality of data processed in the detection, identification and attribution steps, moreover the trustworthiness of the process itself, determines possible consequences. Even more, the stronger goal of accountability can be given if a party can enact specific consequences for specific actions [3]. Especially, for some applications, legal validity may be granted, if some kind of non-repudiation can be guarranted for the evidences generated by the traceability system [8]. Consequently, any daily-life action conducted in a UbiComp environment, that is able to acquire sensor data of a certain quality, may potentially have juridical or financial consequences. We assume that acceptance of smart environments of that kind will depend on the level of control available to the individual users.

4 Privacy-Traceability Tradeoff

In a closer sense, privacy refers to a personal control over the unlinkability of one's identity and personally committed actions. Traceability is a directly contradicting goal, it

hinges on attributing actions to identities. At lot of applications can be based on traceability concepts, e.g., individual accounting, personalized insurances and attestation services [26, 20]. We next describe two scenarios that illustrate the advantages, arising from the user's ability to customize his UbiComp environment between traceability and privacy preferences in a fine-grained manner.

4.1 Scenario 1 - Smart Workplace

John is an employee of a company, which uses several kinds of smart Ubiquitous Computing technologies at the work place. His employer grants John flexible working hours, as long as he is convinced that his employee is at work for a contractually fixed time. Therefore, John agrees to be tracked regularly by the smart workspace on a coarse level. It generates only a binary record for his employer, that indicates if he is present at work accordingly. Because John does a lot of telephone conversation everyday, he enjoys to use the automatic dialogue summarization service [18] provided by his smart working environment. This helps him to keep track of his working duties. Moreover, in project meetings, he and his colleagues regularly choose a high level of traceability. Especially, if decisions of importance have to be made, the decisions are non-repudiable captured. However, these logs are only made accessible for special purposes. Sometimes it is difficult for John to avoid doing some personal things at work, even though he has flexible working hours. Especially, his children regularly ask for his parental advice. Then John does some longer private phone calls, in his office room. In these cases, John decides to disable the dialogue summarization services and the time tracking service as well.

4.2 Scenario 2 - Flexible Car Insurance

On his way back home, John enjoys to use one of the pay-per-drive cars that are available at the parking station of his company. Being able to lend a car flexibly on demand, he does not need to buy an own car. In order to be covered by an insurance for his way back home, John has agreed to pay on a usage basis. Moreover, John participates in a toll collection for the roads he travels on, the same way. Unfortunately, on this day, John is involved in a serious accident. His car is hit by a vehicle whose driver did not guide priority. So, he passes out. This emergency causes a security unit of the car, that regularly detects his vital signs, to call for help. Fortunately, John has preconfigured his current medical record to be released to the doctors in case of emergency, so they can provide fast and adequate help to him. John recovers quickly, but he has to get in contact with his insurance company. Harnessing the local log system of the car, John is able to attest that he did not drive too fast. Therefore, he is in a good mood that he will not be charged to pay for the irreparably damaged car.

The scenarios indicate that situation, environment and activity can have a large impact on how people set personal preferences on privacy protection [7], and which data people like to provide for traceability applications. Generally speaking, we assume that users want their privacy to be kept on an individually chosen level. In order to do so, one basic mechanisms is to allow users to use pseudonyms to communicate with the surrounding UbiComp infrastructure. However, in many everyday activities legal and financial issues are inherently involved. In these cases, a user has to remain responsible for his actions, even though he normally prefers to be anonymous. Then, third parties may trace back the specific user, or he may himself access the traceability system for his personal and legal interests as well or may delegate the access. We are aware that several competing interest are involved in traceability applications that harness personal data, along with ethical and social questions that need to be considered [26]. Especially, technologies that allow for tracing everyday life activities must indispensably be adopted in a responsible manner.

5 Towards an Architecture

Our goal is to develop a generic architecture for balancing the conflicting goals of privacy and traceability in UbiComp settings. First of all, this architecture shall provide a user the ability to configure his personal preferences for privacy preservation and traceability functionalities and services, once he enters a UbiComp environment. The further development and implementation of this architecture is ongoing work. In this paper, we describe the foundations of this architecture, ommiting technical details. Its design is based on an analysis of various approaches to privacy protection for UbiComp settings (cf. Section 6). The architecture consists of the following main components, illustrated in Figure 2.

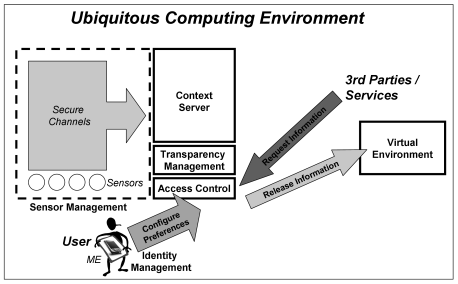

Figure 2. Architecture

Sensor Management: UbiComp environments are sensor-rich. The sensor management component focuses

on integrating various sources of sensor data into the whole system in a trustworthy manner. Therefore, this component detects the available sensors, and provides secure channels to the central component, i.e. the context server. In combination with this part, the sensor management component provides mechanisms for tolerating and detecting manipulations to protect delivered sensor data streams.

Context Server: This component provides the processing of sensor data in order to generate context, i.e. information characterizing the situation of the users. This allows adapting the system's behavior accordingly. Especially, the tasks of this component are filtering and aggregation of sensor data, classification and anonymization of personal data. This way higher level context is generated and provided in several levels of granularity (cf. Figure 3). Sensor data and context that was acquired and processed is stored, temporarily or permanently. A permanent retention can be required due to legal constraints, e.g., specific data protection frameworks.

Access Control: On top of the context server, flexible fine-grained access control mechanism are devised. Those mechanisms, that allow for selective, context-dependent access are a crucial part, since a main challenge of the actual integration of privacy protection mechanisms into a context middleware is to enable context-awareness while protecting personal data. Especially, automation and delegation of access are considered in this component, and in its interplay with the identity management.

Identity Management: This component enables and manages the digital representation and identity of users in a UbiComp environment. We assume that each user is equipped with a personal trusted device, a so called Minimal Entity (ME) [12]. The ME provides the main interface between the user and the environment. It allows a user to configure privacy and traceability preferences, to use pseudonyms, enables non-repudiation via digital signatures, provides configuration support and feedback mechanisms to the user about his current level of privacy.

Virtual Environment: Once access to sensitive data is granted to a third party or service, its further distribution needs to be controlled. Therefore, we devise a virtual environment component. It provides information flow control using trusted computing [23], thus uncontrollable profiling and linking of digital data is prevented.

Transparency Management: The transparency management component audits and documents any access to personal data in an accountable manner. It is a necessary component for traceability and privacy protection systems [16]. Parties and services that are allowed to access private data in specific cases should not routinely abuse this ability [3].

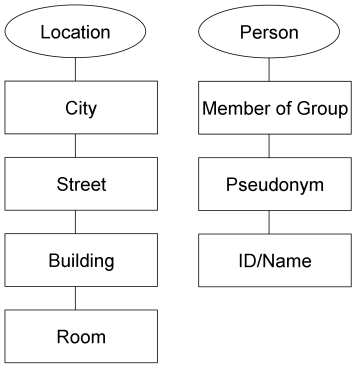

Figure 3. Location and Person Granularity

5.1 Balancing Privacy and Traceability

Our architecture under development provides customizable privacy protection on several levels. The sensor management component ensures, that data related to persons is acquired in a trustworthy manner. The context server allows to provide data in several levels of granularity and anonymity (cf. Figure 3), comparable to the work of Wishart et al. [28]. Building on this, the access control component ensures, that personal data can only be accessed by authorized parties or services. Once data is disseminated, the virtual environment component provides appropriate information flow control. The identity management component ensures, that users may be pseudonymous against the UbiComp infrastructure.

The traceability facilities are interwoven with the privacy protection mechanisms, they are part of the access control, identity management and transparency management components. The access control mechanisms are designed to support fine-grained specification and delegation of access to personal data. Users are enabled to grant and to delegate access to groups and hierarchies of parties or services, enabling a distribution of responsibilities. The identity management enables temporal pseudonyms, that may be traced back to a core identity, or to a group membership (cf. Figure 3). In order to be able to balance between privacy and traceability, users must be able to express their preferences about which data to disclose in which circumstances, in a fine-grained manner. For this purpose, fine-grained resolution of context data, of identity information, and of access rights are provided.

6 Related Work

In this section we discuss important approaches to privacy protection for UbiComp settings. We first discuss

some technical means for preserving location privacy. Afterwards, we describe policy based approaches. Finally, we discuss some existing work on traceability applications.

6.1 Location Privacy

A lot of research has been dedicated to protect location information, which is a primary context information. We next sum up concepts for pseudonym management, access control and de-personalization of location data. Those approaches assume that the location information was collected in a trustworthy manner.

6.1.1 Mix Zones

In [2], Beresford and Stajano propose to protect location privacy by two techniques: first, users of location based services do use changing pseudonyms to receive and request those services. Second, they introduce so-called mix zones, i.e. service-free zones, in which the actual change of pseudonyms is done, in order to prevent profiling by a service provider. Beresford and Stajano argue that, since users change their pseudonym before entering the next application zone, the identities of all users present in a mix zone are undistinguishable mixed. The degree of anonymity provided hinges on the number of users present. Unfortunately, using only short-time pseudonyms does not allow to receive personalized services. Moreover, restricting service usage to application zones contradicts to the basic idea of using services everywhere.

6.1.2 Spatial and Temporal Cloaking

In [10], Gruteser and Grunwald present an approach to de-personalized disclosure of location information to service providers. Before requested data is actually disclosed, together with an identity or pseudonym, they propose to reduce the spatial and temporal resolution of location information (so called cloaking), until an anonymity criteria based on k-anonymity [24], is met. Here, k-anonymity means that the location information released cannot be used to distinguish an individual from at least $k-1$ further co-located individuals. Users are able to chose a k value globally. As drawbacks, only one fix level of granularity is provided, which may be too inaccurate for some applications. Temporal cloaking may lead to delays of data delivery, especially in sparsely populated areas. Moreover, computing the k-anonymity criteria here requires a global view of one trustworthy component, which can be a threat to privacy in itself.

6.1.3 Share The Secret

The Share The Secret (STS) architecture, described by Delakouridis et al. [5] addresses the problem of storing and accessing sensitive information in a privacy-preserving, decentralized manner. They propose to split the information to be protected according to the (k, n)-threshold secret sharing principle [22], and to distribute those shares on several servers, addressable via pseudonyms. Here, secret sharing guarantees that only a coalition of at least k servers can actually access the information. This approach ensures that no single server may compromise private information stored in this way. As severe drawbacks, distributing the access responsibilities leads to extensive storage and communication overheads.

6.2 Policy based Approaches

Privacy policies are contractual agreements between a user and a party receiving personal data. A policy can be considered as meta-data attached to the actual information, specifying its allowed usage. Beyond location information, policies can be used to deal with further kinds of context information. We discuss important approaches next.

6.2.1 Confab

In [13], Hong and Landay propose Confab, an architecture for privacy-sensitive UbiComp. They assume that a user is in control of his context data, by devising an infrastructure, that captures, stores, and processes personal information on the users devices. In case a user decides to disseminate personal data, e.g., his location determined by his GPS system, to a third party, he specifies his privacy preferences and attaches them as metadata. Here, the policy language allows to specify granularity levels, e.g., a location can be disseminated on a accurate ("street") or more coarse level ("city"). Moreover, Confab implements a social component of privacy protection, i.e. users are able to provide white lies ("Requested data unknown"), to hide their real privacy preferences. Hong and Landay call this ability plausible deniability. As a severe drawback, the Confab architecture does not address the cases, in which context is acquired by external sensors. This underlying assumption does not hold for the vision of smart UbiComp environments.

6.2.2 pawS

In [16], Langheinrich proposes pawS, a privacy-awareness system. In this approach, each user is equipped with a personal trusted device, called privacy assistant. Using this device, the user specifies and negotiates his privacy preferences with a surrounding UbiComp environment. Beyond

establishing a limited user control over the sensor configuration of the current environment, Langheinrich's approach provides some degree of transparency on the collection and usage of sensitive personal information. Privacy-aware databases store any data access and usage, enabling a user to verify the details later. The privacy policies are specified in a machine-readable XML format. Even though Langheinrich argues that, providing transparency is a key factor for privacy protection in UbiComp settings, the pawS approach exhibits some problems. It relies on policies, which cannot be enforced rigorously, without some form of additional digital rights management or compliance mechanisms. So manipulation of log entries in the privacy-aware databases cannot be detected, yielding only a superficially degree of transparency. Moreover, it is a hard task for a user to verify the large amount of XML logfiles provides by pawS.

6.2.3 Virtual Walls

Kapadia et al. [14] describe the concept of virtual walls, i.e. usable policy abstractions. Like a physical wall controls physical access, a virtual wall controls access to acquired sensor data. Users are enabled to setup their privacy preferences using three predefined levels of configuration, namely transparent, translucent and opaque. Those levels correspond to intuitive levels of privacy. By this, Kapadia et al.'s approach provides an initial support for users in setting their preferences. As a clear drawback the translucent level, which allows some private data to be accessed from outside, preferably chosen in most cases, does certainly need adjustment to personal demands. So, the initially provided usability support is not sufficient for standard users.

6.3 Traceability applications

In this section, we sketch some work on traceability applications. Especially, we distinguish between attestation applications, i.e. service that allow users prove actions, presence or absence in dispute cases, damage or loss, and confirmation applications, i.e. fine-grained warranty and accounting services (cf. [26]).

6.3.1 Attestation services

Zugenmaier et al. [29] describe attestation services that are based on so called location stamps. This approach builds on cellular networks and mobile phones. Here, location stamps are basically digitally signatures that are used to prove that a mobile phone under the control of a certain user has been at a certain time at a certain location.

Extending these concepts, Gonzales-Tablas et al. [8, 9] additionally take movement of users into account. They propose path stamps, and furthermore address automation aspects [9]. We believe that, additionally, the collection and generation of evidences can benefit from the large amount of data collected by a variety of different sensors in UbiComp environments.

6.3.2 Confirmation services

In [25], Troncoso et al. describe PriPAYD, an approach towards a privacy friendly pay-as-you-drive insurance system. PriPAYD aggregates the information for billing, i.e. the time and position a car has been, locally. Thus, it only gives out the minimum information necessary to bill the client to the insurance company.

Similarly, Coroama [4] proposes the Smart Tachograph. This system allows to bill drivers in a pay-per-use or pay-per-risk manner. Coroama discusses several variations concerning the degree of privacy provided. A local data processing model is chosen, to aggregate billing information. Only the total sum is transferred to the accounting authority.

Both approaches [25, 4] suffer from the same drawback as the approach of Hong et al. (cf. Section 6.2.1), they rely on the assumption that data is only collected locally. We believe that this is an unrealistic assumptions in UbiComp settings.

6.4 Discussion

We described several approaches to protect privacy and to realize traceability applications in UbiComp settings. Even though concepts for customizing between privacy and traceability preferences have not been considered under realistic assumptions, yet, the related work provides valuable insights on how to design customizable mechanisms. Temporal pseudonyms, k-anonymity, context granularity and access control mechanisms are important parts of our architecture.

7 Conclusions and Outlook

Protecting privacy of users of UbiComp technology obviously poses severe problems. This fact has been noticed from the beginning of the UbiComp vision. On the one hand, misuse of sensitive information collected and processed by sensors and computers present in every aspect of life is a fundamental barrier to the acceptance of UbiComp. On the other hand, once personal data of a certain quality can be acquired, traceability is a natural interest, leading to several new kinds of applications.

In this paper, we presented our initial approach to deal with this issue. We described the foundations and components of an architecture, that allows a user to customize and balance between the conflicting interests of privacy and

traceability. Its design builds on an analysis of various approaches to privacy protection for UbiComp settings. Such an architecture requires appropriate protection mechanisms for the collection, access, usage and dissemination of personal data. Additionally, transparency and usability issues have to be taken into account. Here, both the configuration of privacy and traceability preferences and feedback about the current state of privacy are critical. The so chosen state has to be intuitively understandable, i.e. its implications need to be conveyed to the user as clearly and simply as possible. We believe that, the users are the first concerned party that should be able to actually exercise the control on the balance between privacy and traceability. Nevertheless, it is important to determine, in which situations further interests need to be balanced, and therefore which parties may be allowed to exercise control on this balance. This is an important legal, social and ethical discussion. One can think of sites, e.g., airports, that demand some higher degree of traceability, while a smart home shall undoubtly remain the hideaway of its inhabitants.

Technologists may contribute to this matter by providing customizable solutions. We expect that such customizable technologies will shape and create new forms of socially acceptable UbiComp applications, interactions and services, while mitigating the inherent privacy concerns.

In the next steps of our research, we will further develop and implement the discussed architecture, and evaluate it in challenging real world settings. Especially, we intend to test it in scenarios with high privacy demands, e.g., smart homes, and scenarios with high traceability demands, e.g., mission-critical meeting and control rooms [6].

References

[1] V. Bellotti. Design for Privacy in Multimedia Computing and Communications Environments. *Technology and Privacy: The New Landscape*, pages 63–98, 1997.

[2] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 02(1):46–55, 2003.

[3] M. Burmester, Y. Desmedt, R. N. Wright, and A. Yasinsac. Accountable Privacy. In *Security Protocols Workshop 2004*, pages 83–95, 2004.

[4] V. Coroama. The Smart Tachograph - Individual Accounting of Traffic Costs and its Implications. In *Proceedings of Pervasive 2006*, pages 135–152, May 2006.

[5] C. Delakouridis, L. Kazatzopoulos, G. F. Marias, and P. Georgiadis. Share The Secret: Enabling Location Privacy in Ubiquitous Environments. In *LoCA*, pages 289–305, 2005.

[6] F. Flentge, S. G. Weber, A. Behring, and T. Ziegert. Designing Context-Aware HCI for Collaborative Emergency Management. In *Int'l Workshop on HCI for Emergencies in conjunction with CHI 2008*, 2008.

[7] M. Friedewald, E. Vildjiounaiteb, Y. Puniec, and D. Wright. Privacy, Identity and Security in Ambient Intelligence: A Scenario Analysis. *Telematics and Informatics*, 24(1):15–29, 2007.

[8] A. I. González-Tablas, B. Ramos, and A. Ribagorda. PathStamps: A Proposal for Enhancing Security of Location Tracking Applications. In *CAiSE Workshops*, 2003.

[9] A. I. González-Tablas, L. M. Salas, B. Ramos, and A. Ribagorda. Providing Personalization and Automation to Spatial-Temporal Stamping Services. In *DEXA Workshops*, pages 219–225, 2005.

[10] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys*, 2003.

[11] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald. Privacy-Aware Location Sensor Networks. In *Proceedings of HotOS'03: 9th Workshop on Hot Topics in Operating Systems*, pages 163–168, May 2003.

[12] A. Hartl, E. Aitenbichler, G. Austaller, A. Heinemann, T. Limberger, E. Braun, and M. Mühlhäuser. Engineering Multimedia-Aware Personalized Ubiquitous Services. In *IEEE Fourth International Symposium on Multimedia Software Engineering (MSE'02)*, pages 344–351, Dec. 2002.

[13] J. I. Hong and J. A. Landay. An Architecture for Privacy-Sensitive Ubiquitous Computing. In *Proceedings of The Second International Conference on Mobile Systems, Applications, and Services (MobiSys 2004)*, 2004.

[14] A. Kapadia, T. Henderson, J. J. Fielding, and D. Kotz. Virtual Walls: Protecting Digital Privacy in Pervasive Environments. In *Proceedings of the Fifth International Conference on Pervasive Computing (Pervasive)*, pages 162–179. Springer-Verlag, May 2007.

[15] M. Langheinrich. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001)*, pages 273–291. Springer-Verlag, 2001.

[16] M. Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In *Proceedings of the 4th International Conference on Ubiquitous Computing (UbiComp 2002)*, pages 237–245. Springer-Verlag, Sept. 2002.

[17] M. Langheinrich. Privacy Invasions in Ubiquitous Computing. In *Workshop on Socially-Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing*, 2002.

[18] M. Mieskes, C. Müller, and M. Strube. Improving Extractive Dialogue Summarization by Utilizing Human Feedback. In *AIAP'07: Proceedings of the 25th IASTED International Multi-Conference*, pages 627–632. ACTA Press, 2007.

[19] J. M. Myerson. *RFID in the Supply Chains: A Guide to Selection and Implementation*. Auerbach Publications, 2006.

[20] C. Patrikakis, P. Karamolegkos, A. Voulodimos, M. H. A. Wahab, N. S. A. M. Taujuddin, C. Hanif, L. Pareschi, D. Riboni, S. G. Weber, A. Heinemann, S. ching Samson Cheung, J. Chaudhari, and J. K. Paruchuri. Security and Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 6(4):73–75, 2007.

[21] M. Satyanarayanan. Privacy: The Achilles Heel of Pervasive Computing? *IEEE Pervasive Computing*, 2(1):2–3, 2003.

[22] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[23] F. Stumpf, M. Benz, M. Hermanowski, and C. Eckert. An Approach to a Trustworthy System Architecture Using Virtualization. In *Proceedings of the 4th International Conference on Autonomic and Trusted Computing (ATC-2007)*, pages 191–202. Springer-Verlag, 2007.

[24] L. Sweeney. k-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[25] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel. PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance. In *Workshop on Privacy in the Electronic Society 2007 (WPES '07)*, 2007.

[26] S. G. Weber, S. Ries, and A. Heinemann. Inherent Tradeoffs in Ubiquitous Computing Services. In *INFORMATIK 2007*, volume P109 of *LNI*, pages 364–368. GI, September 2007.

[27] M. Weiser. The Computer for the 21st Century. *Scientific American*, 265(3):94–104, 1991.

[28] R. Wishart, K. Henricksen, and J. Indulska. Context Obfuscation for Privacy via Ontological Descriptions. In *LoCA*, pages 276–288, 2005.

[29] A. Zugenmaier, M. Kreutzer, and M. Kabatnik. Enhancing Applications with Approved Location Stamps. In *Intelligent Network Workshop (IN 2001)*, pages 140–147, 2001.