Mobile Identity Management

Uwe Jendricke, Michael Kreutzer, Alf Zugenmaier
Institute of Computer Science and Social Studies, Department of Telematics
Albert-Ludwigs-University of Freiburg, Friedrichstrasse 50, D-79098 Freiburg, Germany
Tel.: +49-761-2034964, E-Mail: {ujendric, mkreu, zugenmai}@iig.uni-freiburg.de

This work was presented at the Workshop on Security in Ubiquitous Computing, UBICOMP2002

Abstract

Privacy is a severe problem facing mobile computing. The fundamental question arises: Who gets to know personal data stored on handhelds? Most of current handhelds (personal digital assistants, mobile phones, etc.) are equipped with wireless communication interfaces like bluetooth or infrared. However they only have access controls for the user of the device, but do not consider which personal data is offered at different locations. This is a privacy problem because the information offered already allows the generation of various profiles of the device's user, for example location profiles. To improve the user's privacy, we propose an identity-based control over the data published and the services offered. Comparable to "normal life", this identity management *allows the device to present different subsets of the user's identity depending on the perceived (wireless) communication context.*

1 Introduction

Many users fear that their privacy is invaded by the collection of personal data when using it-systems. Privacy in this context is the concept of restricted access to personal data [18]. With mobile computing, where devices leave data traces at different locations by using wireless communication, privacy is jeopardized even more. The devices belonging to the user potentially communicate with the wireless environment all the time, thus revealing the whereabouts and identity of the user (indirectly through the device address).

A reference scenario illustrates this point: going to the shopping mall, one does not normally hand out personal data to every person one meets. One may choose to transfer personal data to carefully selected persons for example when entering a transaction to a local bank clerk, or when conducting a business transaction to a local retailer, or on a peer to peer basis when visiting a trade show. Even here, different sets of personal data are handed out. In the mobile computing world, this differentiation of publishing personal data is jeopardized because the devices advertise their identity irrespective of their communication partners.

We propose mobile identity management, which is a concept that allows the user to keep his or her privacy depending on the situation. By using identity management, the user's devices "behave" in a similar way to the user: In different contexts (i.e. wireless "environments"), the user presents a different "appearance". Devices controlled by identity management change their "behaviour" similar to the way in which a user would.

This paper is organized as follows: The next section describes the concept of identity management and the related work. In Section 3 we present privacy principles for mobile identity management build up on the principles of multilateral security. Section 4 introduces the concept of identity management in the mobile computing world and describes our prototype. The paper concludes with a summary.

2 Identity Management

While using information technology (IT-) systems, everybody discloses some degree of information about himself or herself and the used computer system. Web browsers, for example, allow the server to obtain the user's IP address, the operating system used, or the web page that has been previously visited.

The server's operators can use this personal data to generate profiles of the users. This data may be very informative, especially for e-commerce providers. Users can be traced in all their actions, e.g. surfing through a web catalog. Together with the data which is often added by the user (names, addresses, or other identifying data), a detailed profile of the user can be generated and extended over time.

During everyday life, everybody is used to managing the appearance and disclosure of his or her personal data to others. In a brick-and-mortar shop, for example, people do not disclose much personal data. In most cases (e.g. when using cash), payment is anonymous and several shopping transactions cannot be linked to one customer. However, this habit changes by using credit cards, debit cards, and reward schemes.

We define *identity management* as a concept that enables each user to express and to enforce his or her privacy and security needs in IT-systems depending on the situation the user is in. The situation is determined by the context. The user selects a subset of his or her personal data (the identity) to which access is granted for each situation. The communication is based on secure mechanisms to enable anonymity and confidentiality.

In order to use an identity management, the user needs an appropriate tool to facilitate the management of the disclosure of personal data. As early as 1985, David Chaum [2] considered a device that helps the user with (payment) transactions and upholds the user's privacy. Roger Clarke [4] proposed the "digital individual", the individual's data shadow in the computer system which can be compared to the user's identity as defined above. In 1995, John Borking [19] published a report about the "Identity Protector" that should help to protect the user's data. The "reachability manager" [17, 7] realized an identity management system for telephone reachability. Based on this work, we proposed the concept of *generic identity management*: a usable and secure way for the user to protect his or her privacy [10, 11][1]. We implemented the identity manager for the Internet as a prototype application. This prototype is a usable security tool that helps even the inexperienced user to manage his or her general security needs when using the Web. Other actual research about identity management can be found at [5] with an emphasis on infrastructures needed for credentials and other accountability mechanisms.

An identity manager allows the user to determine the personal data that is offered in a situation. This set of personal data represents the user in the given situation, and therefore constitutes the user's (partial) *identity*. In our Internet prototype, situations are specified by different URLs or substrings of URLs. The situation is recognized by comparing the context to predefined settings or rules. User defined rules are derived from user actions, such as explicitly choosing a particular (partial) identity in a given situation. When a user returns to a situation later, the system uses the same identity that was used before and the user knows which data has already been offered to this communication partner. In new, undefined situations a default identity is used, which enables anonymous communication.

Technically, an identity management system is based on an anonymity service which allows the user to be anonymous to the communication partner and to third parties. To a trustworthy communication partner the identity is revealed by the user who selects the appropriate partial identity dependent on the situation. In addition, the system has to use mechanisms to establish a confidential communication, e.g. by using secure socket layer SSL, or PGP. A database stores the personal data, the identities, and the situations of the user.

Other systems offer some parts of the described functionality. Form fillers like Gator[2] automatically fill out web forms with previously defined personal (or fake) data. The Lucent Personalized Web Assistant [8] allows the user a pseudonymous use of personalized web sites by offering different aliases for the user. These aliases are managed by a trusted intermediary. The Freedom Premium Service[3] offered an anonymizing infrastructure and the usage of several pseudonyms for web browsing but did not utilize the concept of identity management for all Internet services. P3P [6] is a standard that allows the user to specify preferences about his or her privacy preferences. These preferences are compared by the system to the server's policy. In case of conflict, the user or the system have to decide how the conflict can be solved. P3P is helpful as an add-on for an identity management system: each identity may contain its own privacy preferences.

3 Privacy Principles of Mobile Identity Management

In this section we describe how privacy principles for the Mobile Identity Management can be derived from the requirements of multilateral security [16, 15].

Confidentiality: *c1 Message contents:* To achieve confidentiality in information and communication technology, cryptography is "classically" regarded as the main mechanism that also may achieve integrity of the messages. The identity manager should support cryptography (symmetric and asymmetric): Whenever the mobile device is capable of running cryptographic algorithms and key

[1] Current information about our work and further publications can be found at http://www.iig.uni-freiburg.de/telematik/atus/

[2] http://www.gator.com/

[3] http://www.freedom.net/, closed 10/2001

exchange protocols are available, the identity manager automatically should use an encrypted connection [10, 11].

c2 Anonymity and Pseudonymity: This is another aspect of confidentiality: Communication Data should not be able to be linked to individuals and one should be able to conceal one's true identity. The identity management system, by default should reveal no identity: the user's appearance is anonymous. As devices are highly mobile, new anonymity mechanisms must be introduced [21]. When authentication is needed, the user can configure his or her device to reveal authentication data only in well-defined situations and to well-defined communication partners. Moreover the user should be capable to act under a pseudonym whenever identification is obligatory but not the revealing of the true identity.

c3 Protection of location information: The determination of the current location of a mobile terminal should either be done with the consent of the user or the location information should not be linkable to the user and the device.

Integrity: Manipulation of messages must be detected. This can be done with cryptographical mechanisms as already described in c1.

Availability: Using wireless communication, potentially there are more undesired connection aborts than using wired systems. A possible workaround for the identity management may be a transaction concept known from databases [14] to ensure that important actions are withdrawn either correctly or not at all.

Accountability: Concerning the need of proving the sending and receiving of messages, cryptographical mechanisms like digital signatures can be used.

Notice: This point addresses the attention of the user [15]: Whenever devices carry out or observe security-related actions, the people concerned should be informed. For example an IT-system can be configured to show all log-in events instantly on the console window. In the case of identity management, the device should demand the attention of the user when a situation arises that affects privacy and that needs user interaction. These situations requiring user interaction must be pre-configured to meet demands of the user concerning his or her security needs and to minimize disturbance. It is conceivable that notice may also be allowed in the case of a paid advertisement [17, 7]: the user determines the amount of money which must be given to him or her in order that he or she reads an advertisement.

However, for usability reasons, notice must be reduced to a minimum [15]. Automation is a good compromise between usability and security (i.e. disturbance in the case of notice) as long as it does not incapacitate the user.

Data Collection: This is an extension to the concept of multilateral security. As stipulated in the various guidelines on data protection, it is not sufficient just to inform people about data collection. The users should be able to actively decide, whether and which data about them is being collected [6] and also be able to have access to the data, to alter or erase it.

The identity management system supports this aspect of privacy in so far as it restricts the communication partner's access to the personal data of the user. The main task of the identity management system is to give the user control over which personal data he or she gives away. As a consequence, the system only authenticates itself when the user explicitly allows it to do so or when preconfigured situations arise. Thus, the user has full control over the data that is revealed to communication partners.

Alongside the principle of data minimization, data should only be collected for a specific purpose. This emphasizes the possibility of objection and of recourse in the event of conflict. Non-repudiation mechanisms are required for this. The realization of these demands is not guaranteed even in the spontaneous networking environment. These problems become still more pressing in mobile computing.

The principle of recourse cannot be assured by the identity management system because this principle can only be handled by mechanisms that go beyond the configuration of the user's hardware and software. To enable recourse, the identity management can be widened by a tele-witness system [12] which is under the control of the user.

Identity management fulfills all principles that do not rely on third parties. This has the advantage that identity management can be implemented completely on the user's device and does not require access to services in the network. These services or an access to these services may not exist in every network. Restricting the transfer of sensitve data that are handed out to communication partners to other (third) parties only can be achieved by using external mechanisms and requires non-technical solutions to arbitrate disputes.

4 Realization of Mobile Identity Management

Identity management, as described in Sect. 2, helps the user to maintain control of his or her personal data. This results in a higher level of privacy for the user. In the world of mobile computing, the user and the user's devices encounter some new vulnerabilities, because the user and the hardware change location and offer (and use) new services and data in ad hoc networks. In these networks, the device may even interact spontaneously with its environment, often without direct user interaction. With mobile identity management the user may overcome these vulnerabilities to keep a high level of privacy.

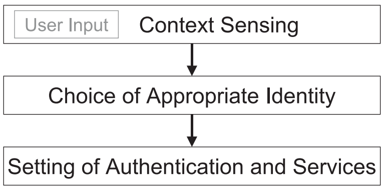

Figure 1. Flow chart of mobile identity management

In Fig. 1, the procedure of configuring the device is shown. First, the system senses the current context, as will be described in Sect. 4.1. This context, which optionally includes user input, is used for the determination of the appropriate identity. With these identities, the offered services, and the access to the personal data are configured as will be described in Sect. 4.2.

4.1 Context of a PDA

The following hierarchy of context information refers to a current multipurpose personal digital assistant[4].

1. *The task.* The application chosen by the user reflects his or her goal. This application is the fact that best represents the user's intentions and therefore it is the most important context in this case.

2. *The infrastructure (surrounding computing and interaction environment).*
   The ability to communicate is crucial for the device described. A personal device without communication interface to other devices only has an impact on privacy when it falls into the wrong hands. The most important communication interfaces in mobile computing are the various kinds of wireless interfaces.

3. *The physical environment, especially the location.*
   Apart from guidance systems, location can be used as an additional security feature. It is not only possible to use location for improved authentication [9] but also to reach higher trust using accountablity mechanisms [20].

[4]We have chosen this kind of device as it is presumably the scenario with the highest relevance concerning privacy (cf. also Sect. 4.3).

However, it is clear that not all PDAs actually can determine the last item. Some special-purpose devices may even have only a single source of context information. In addition, not all context data is useful for a specific task. As a result of this, the concept of context sensing in identity management must be implemented in an application- and device-specific way.

To recognize the context, a data structure must be defined which derives the identity from the context information. As shown in [3] this determination is application-specific and can be done in manifold ways (using key-value pairs, an object-oriented approach, tagged encoding, a logic-based model etc.).

When a user visits a bank, for example, the system may receive the location information and the wireless services that are offered by the bank. In a logic based model, one rule may be "when location is 'in the range of own bank' and wireless service is 'ATM', then propose 'Customer' identity to the user". The determination process may be defined by the user, by the manufacturer, or even by the service provider. A banking smart card may contain context configurations that activate the "Home Bank Authentication" on the card when the owner enters the bank. When a foreign bank is visited (at another location, with different wireless services), the "Foreign Bank Authentication" will be selected on the card.

When communicating with several communication partners at once, each session with one of the partners is matched to one identity. Because of the confidentiality of the communication (see identity management basics in Sect. 2), it is not possible for attackers to get the communication data of the other communication partners.

4.2 Components of a Mobile Identity Management System

When the context changes, the user may want to present a different appearance to the appropriate communication partners or servers. Thus, each context is combined with an identity. This identity determines the "appearance" of the user in such a way that the user's devices are configured individually. For this, the identity from the identity management of Sect. 2 is extended by configuration data for the device's services. Thus, the identity manager has an impact on the *personal data* and *services* offered. In the bank, for example, the user's devices may offer all the financial data and no services ("Home Bank Identity"). On the street they may offer only a nickname and a service to find people that are nearby and are friends of the user ("Outside Identity") or filled with more or less identifying information or even "Anonymous", i.e. no identity. For being anonymous, the user should not offer any personal or linkable data. Depending on the technology there are some possibilities to be anonymous even in a world of mobile computing, for example to have no device address and being identified only by the location [21]. Location addressing ensures that no information attributable to a specific device is required for communication on the link level and network level of the protocol stack. Service discovery relies on a broadcast of the service provider, the device does not have to become active and thus does not reveal its presence just for discovering services the user may not be interested in. Other possibilities to completely hide the identity of the user are by using external anonymity networks like Mist [1], or DC networks [2]. As a result, switching identities allows the user to operate in the spectrum between anonymity and identification.

This changing of identities can be compared to the user's "appearance" in every-day life. The user changes the degree of publicity and information offered when changing location (and communication partners). By using this well-known model of switching identities, the user can easily understand the basic concept of the system which results in better usability.

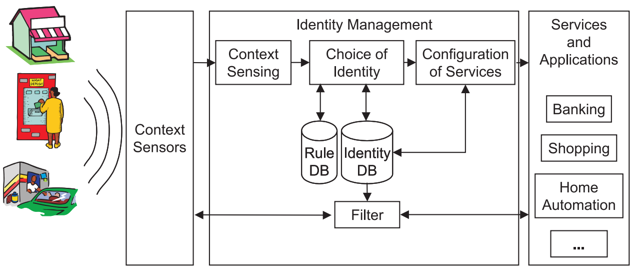

Figure 2. Components of a mobile identity management system.

The components of a mobile identity manager are shown in Fig. 2. The wireless interface and the location sensor acquire the context data according to our prototype, but the context sensors may be more general for more powerful applications. This context data is used to determine the proper identity which is retrieved from the identity database. This database contains all identities and for each identity the appropriate system configuration. Thus, with each identity a specific configuration of the device's services can be performed. In our prototype this configuration consists of simple rules of the form: "if identity A was selected, offer services X and Y and use the bank authentication data". In addition, the system uses a filter to scan the outgoing data for personal data that is not allowed (by the current identity) to be published. When the user accidentally offers such data, the system warns the user about the security violation.

For each recognized context, the device has to be configured to know which identity to use and which services and authentication information (and/or protocol) is combined with this identity. The configuration may be predefined by the manufacturer, predefined by the user, or the user could "train" his or her device in the situation by configuring it at the moment the situation is first detected. The right way of configuring the device is application-specific, however, two objectives should be taken into account: the privacy needs of the user and the usability of the user interfaces.

4.3 Evaluation

To see how this concept could be implemented on a multipurpose PDA, we implemented a simulation as a local Java application. In this simulation, a user with a PDA can be moved through different environments. During movement, the PDA of the user receives the appropriate context information. As described previously, the PDA changes the identity of the user and offers the appropriate applications. A screenshot of the demonstrator is shown in Fig. 3.

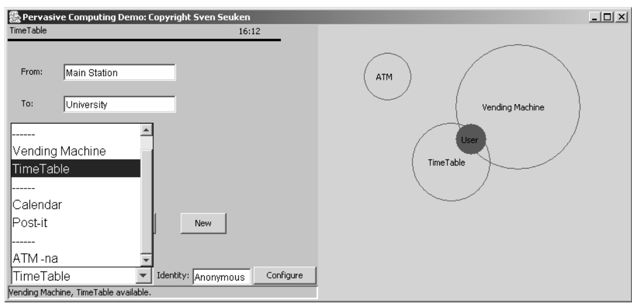

Figure 3. Screenshot of the demonstrator when communicating with the time-table application.

Moving the user and using the PDA can be done independently so as to simulate a roaming user moving and operating his or her PDA. The simulation visualizes the range of the wireless interfaces of other devices by circles in the right part of the window. The circles may intersect, as shown in Fig. 4: when the representation of the user is inside this intersection it simulates the user being in more than one wireless LAN at the same time. The PDA shows the available services in the status line at the bottom of the window.

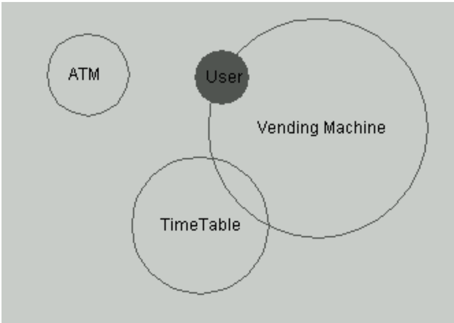

Figure 4. User strolling.

A result from the work with our Identity Manager prototype for the Internet is to prevent the user from selecting identities because of the usability. Better is the selection of a web site or an application. Transferred to our scenario, we have the assumption that a selection of services or runnable applications in a given context offers a better usability than a selection of identities. Thus, the system offers the applications to the user which are possible to use in a context (e.g. banking is not usable at the grocery store). In addition, the user can start applications with a "start" menu, as known from window-based operating systems. The start menu contains, in addition to the context-specific applications, general applications that may be used everywhere (e.g. a calendar or a todo list), as shown in Fig. 3.

When the user explicitly wants to map a context with a new or other identity, he or she can do so by pressing the configure button.

4.3.1 The Scenario:

In our scenario, the "PDA" interacts with three devices and associated authentications:

- a vending machine at work
- banking activities at an ATM
- getting the bus timetable at the bus stop

For the vending machine, the device automatically chooses the "work" identity, as it contains the correct authentication data in this case and fits the context. Using this identity, the vending machine offers its goods on the display of the PDA and the user can buy a drink or a snack, as shown in Fig. 5. The billing simply is tracked by a tally sheet under the control of the vending machine.

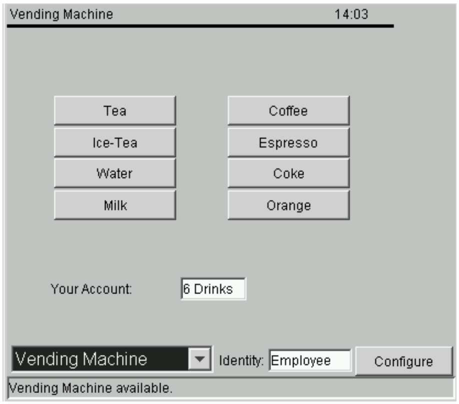

Figure 5. Screenshot of the "PDA" when communicating with the vending machine.

For the banking activities an authentication protocol runs first in order to find out whether the ATM is trustworthy. In the case of a positive result, the ATM application appears on the user interface as an offered service. Only after the user has chosen to interact with the ATM does the encrypted authentication data of the user leave the device.

When getting the timetable at the bus station (Fig. 3), the user remains anonymous. This is shown to the user by the name of the presently used identity.

4.3.2 Experiences

For a further improvement of the mobile identity management system we performed a usability test with different inspection methods [13] of our simulation with 5 people. In addition to some small usability problems (e.g. misunderstandable button labels) we found the following facts:

- Each time the device leaves the range of the sender the connection is broken. In the case of a financial exchange, as it is the case in the banking activities, transaction management is crucial. This can be done in the same manner as with chipcards, obeying the ACID[5] criteria.

[5]Atomicity, Consistency, Isolation, and Durability. [14]

- When many contexts are sensed simultaneously, the status line of the PDA shows all of them. When too many contexts are sensed, a hint to press the start button ("...") is introduced in this case.

- The order of the available applications shown when pressing the start key reflects the pre-defined priority.

- Positive for the usability is the pre-selection of the offered applications. Applications that have no possibility to communicate for the moment (e.g. banking at the vending machine) are offered with a mark (n.a.) but can be runned for configuration reasons.

- Negative for the usability is the reduction of the display size because of additional control elements. This led to the reduction of the identity manager to an adapting start menu and a (small) identity status display and configuration button.

- Some users liked the possibility that an application start automatically when the appropriate identity is selected, e.g. the banking application starts when the user enters the bank building. Others did not like that functionality at all. Thus, this function should be offered optionally.

4.4 Limits and Vulnerabilities

Privacy can be divided into the areas of access control and control of published data [18]. Our system allows adjustable access control of personal data and services offered. Naturally, it offers no control over the data after publication. For this, other mechanisms would be helpful: The user could be provided with approved information on what the offered personal data will be used for. With this information, the user can decide to publish personal data or not and to configure the offered services adequately. For this, adequate legal enforcement is required to ensure the provider's compliance to the policy.

The identity management determines the current identity by scanning the context. This implies the problem of misinterpretation of the context. The context information of an unknown (or attacking) location A may be similar to the context of another location B, which is well known to the user. When the user enters location A, the system sets the identity of location B. Now, attackers at location A may have access to data and services that the user did not want to publish at location A. This problem must be solved by the context recognition system.

Usability may be a problem too. No user likes to be bothered by a lot of configuration effort. What happens when a bank offers a new service and the identity management system does not recognize the identity anymore? Strategies must be found so that the identity manager does not constantly ask the user about new identities or unfamiliar context.

5 Summary

With identity management, a new concept to achieve privacy in mobile computing has been presented. We define the term "(partial) identity" and we show how the identities are determined by the device. Moreover, we suggest the components for the identity management system in mobile computing. A simulation verifies the validity of the concept. We also address the issue of limits and vulnerabilities of our proposals.

Using the context-dependent approach to identity management relieves the burden on the user and therefore makes a usable tool for protecting the user's privacy. We expect more acceptance of mobile computing by introducing identity management because the privacy of the users is respected.

Acknowledgements

We thank Jason Bechtel and Julia Bär for their helpful comments on readability and Sven Seuken for implementation work. This research has been partly supported by the Deutsche Forschungsgemeinschaft (DFG) and the Kolleg "Living in a Smart Environment" of the Gottlieb Daimler- and Karl Benz-Stiftung.

References

[1] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi. Routing through the mist: Privacy preserving communication in ubiquitous computing environments. In *Proceedings of ICDCS 2002*, July 2002.

[2] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, Oct. 1985.

[3] G. Chen and D. Kotz. A survey of context-aware mobile computing research. Technical Report TR2000-381, Dept. of Computer Science, Dartmouth College, November 2000.

[4] R. Clarke. Computer matching and digital identity. In *Proceedings of the Computers, Freedom & Privacy Conference*, San Francisco, 1993.

[5] S. Clauss and M. Köhntopp. Identity management and its support of multilateral security. *Computer Networks*, (37):205–219, 2001.

[6] L. Cranor, M. Langheinrich, M. Massimo, M. Presler-Marshall, and J. Reagle. The platform for privacy preferences 1.0 (p3p1.0) specification. http://www.w3.org/TR/P3P/, Jan. 2002.

[7] H. Damker, U. Pordesch, and M. Reichenbach. Personal Reachability and Security Management – Negotiation of Multilateral Security. In G. Müller and K. Rannenberg, editors, *Technology, Infrastructure, Economy*, volume 3 of *Multilateral Security in Communications*, pages 95–111. Addison Wesley Longman Verlag GmbH, 1999.

[8] E. Gabber, P. B. Gibbons, Y. Matias, and A. Mayer. How to make personalized web browsing simple, secure, and anonymous. In *Proceedings of Financial Cryptography 97*, LNCS 1318. Springer Verlag, February 1997.

[9] D. Gollmann. *Computer Security*. John Wiley & Sons, 1999.

[10] U. Jendricke and D. G. tom Markotten. Usability meets security – the identity-manager as your personal security assistant for the internet. In *Proceedings of the Annual Computer Security Applications Conference*, December 2000.

[11] U. Jendricke and D. G. tom Markotten. Identitätsmanagement: Einheiten und systemarchitektur. In D. Fox, M. Köhntopp, and A. Pfitzmann, editors, *Verlässliche IT-Systeme - Sicherheit in komplexen Infrastrukturen*, pages 77–85. Vieweg, Wiesbaden, September 2001.

[12] D. O. Keck, M. Kabatnik, M. Kreutzer, and A. Zugenmaier. Multilateral security in intelligent networks. In *Intelligent Network Workshop, IN 2000, Cape Town, South Africa*. IEEE, May 2000.

[13] J. Nielsen. *Heuristic Evaluation*, chapter 2. John Wiley and Sons, Inc., 1994.

[14] P. O'Neil. *Database – Principles, Programming, Performance*. Morgan Kaufmann Publishers, 1994.

[15] K. Rannenberg. Multilateral security? a concept and examples for balanced security. In *Proceedings of the 9th ACM New Security Paradigms Workshop 2000*, September 2000.

[16] K. Rannenberg, A. Pfitzmann, and G. Müller. *IT Security and Multilateral Security*, pages 21–29. Multilateral Security in Communications - Vol. 3 Technology, Infrastructure, Economy. Addison-Wesley, 1999.

[17] M. Reichenbach, H. Damker, H. Federrath, and K. Rannenberg. Individual management of personal reachability in mobile communication. In L. Yngström and J. Carlsen, editors, *Information Security in Research and Business; Proceedings of the IFIP TC11 13th International Information Security Conference (SEC '97): 14-16 May 1997, Copenhagen, Denmark*, pages 163–174, London, 1997. Chapman & Hall.

[18] H. T. Tavani and J. H. Moor. Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Newsletter*, 31(1):6–11, March 2001.

[19] H. van Rossum, H. Gardeniers, and J. B. et. al. Privacy-enhancing technologies: The path to anonymity, August 1995.

[20] A. Zugenmaier, M. Kreutzer, and M. Kabatnik. Enhancing applications with approved location stamps. In *Intelligent Network Workshop, IN 2001, Boston, MA, USA*. IEEE, May 2001.

[21] A. Zugenmaier, M. Kreutzer, and G. Müller. Location addressing: Technical paradigm for privacy and security in a ubiquitous world. Technical report, Hitachi, August 2001.