Providing Personalized Privacy Support in Public Places

Carsten Roecker
Fraunhofer IPSI, AMBIENTE – Smart Environments of the Future
Dolivostrasse 15, D-64293 Darmstadt, Germany

In this paper we present a system that provides personalized privacy support for large public displays based on the current social situation and individual privacy profiles. We first present the results of a user study that was conducted to derive the requirements for the design of the system. In the second part of the paper, we describe the developed system consisting of a program for privacy-enhancing information management and a small personal artefact for an easy adaptation of the privacy settings to the local context.

Keywords: Large Public Displays, Active User Support, Privacy Enhancing information Management

Introduction And Goal

A continuous trend towards higher mobility is observable in most companies, leading employees to spend considerable time away from their own desk, working in meeting rooms, other offices or in the hallway [1]. According to estimations white-collar workers spend between 25% and 70% of their daily working time in conferences or meetings with colleagues [2,3] As large-screen displays are becoming increasingly prevalent in public spaces [4], several projects address this evolution by providing "walk-up-and-use" applications on large screens in public or semi-public areas. "Blue Board" [5], for example, is a large plasma display with touch sensing and a badge reader to identify individuals. The onboard software is designed for personal use (access of private calendar) as well as small group collaborative use (creating and sharing of content). While "Blue Board" requires users to set up their content ahead of time and thus gives the user control over the information that is displayed, other systems, like "IM Here" [6], are intended for more spontaneous workgroup interaction. "IM Here" is a shared instant messaging system running on a large public display designed to facilitate informal communication while away from the desktop. Similar to [7], upcoming privacy problems are eluded by restricting the use to small group of users.

While most developers rely on social protocols or do not address privacy questions at all, there are very few approaches to actively support privacy on large public displays. In most cases, e.g. [8,9], additional private displays are used to generate and present personal information, while public information is displayed on a shared large display. A different approach using a stereographic display and special shutter glasses is described in [10]. Personal privacy is maintained through the filtering of the information on the shared display. Users wearing shutter glasses will see the public information as well as their own private information, while other person's private data is not visible to them.

Although these systems support individual privacy in an adequate way, they always require additional personal devices, like PDAs or shutter glasses. Since most public displays are intended for "walk-up-and-use" applications, like quickly accessing the personal calendar or email, the existing solutions are not very suitable. Our goal is to give users the freedom to spontaneously work on large public displays without the fear of privacy infringements through passers-by. This seems to be of particular importance, since recent studies [11] showed, that even given constant visual angles and similar legibility, individuals are more likely to read sensitive text on a large display than on a small one.

User Needs And Privacy

To obtain a deeper insight of the requirements for privacy in multi-user situations and as a basis to develop an appropriate solution we started addressing this topic by investigating the demands of potential users. The emphasis of our survey was on privacy-related questions, especially on the importance of privacy and the acceptance of system-controlled privacy measures. Since the majority of future users will lack a detailed technical knowledge about the environment they inhabit, we aimed at a target group outside the research community to get representative results. During an open house day at our institute n=131 visitors participated in an questionnaire-based survey. Being asked about their computing skills, 51.1 % rated themselves as advanced, 42.2 % as experts und 6.9 % as beginners.

The survey shows that 45.0% of all users rate privacy "important" and 32.8% as "very important", while at the same time over one third (36.6%) never change their passwords. The results stress again the important role of privacy in ubiquitous computing environments [12], but also indicate a large discrepancy between users' desire to protect privacy and their willingness to take relevant measures.

Context-Dependent Information Disclosure

To guarantee satisfactory privacy protection and at the same time to minimize interruptions during the work process, it is essential to know which information should be hidden from whom and when. Protecting work-related information from colleagues passing-by might not be necessary and doing so would most likely result in an unintended interruption of the ongoing task. But the situation is fundamentally different, when accessing private information while other people approach the display. In the second part of the questionnaire the participants were confronted with different types of information and asked which information they would be willing to provide to whom.

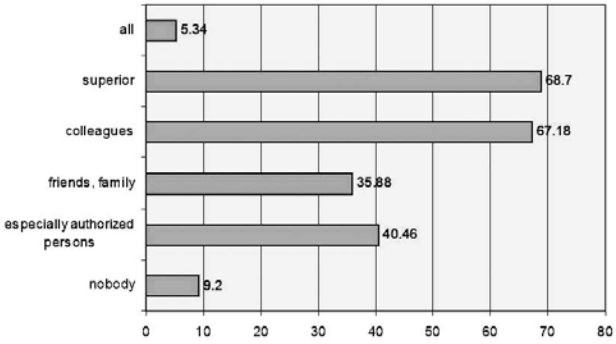

Fig. 2. Professional appointments: number of participants [%] who would provide calendar information about professional appointments to different recipients.

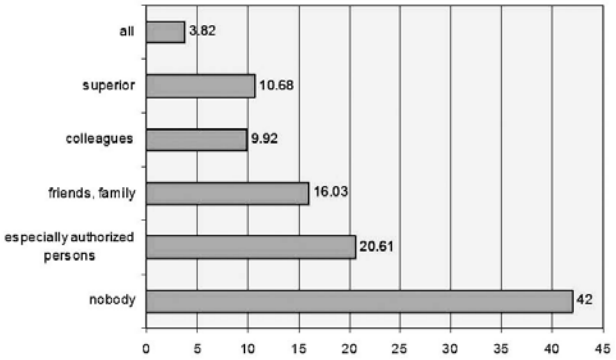

Fig. 3. Accessed web pages: number of participants [%] who would provide information about accessed web pages to different recipients.

The results indicate that the willingness to provide information varies widely with the type of information and the information receiver. Figure 1 and 2 show two examples for these findings.

Active User Support

Moreover, we investigated the acceptance of automated privacy support in group situations as well as the desired degree of system support regarding privacy protection. Our aim was to understand if and how users want to be supported in protecting their privacy in dynamically changing group situations.

Therefore, we asked the participants to imagine a situation where they work with personal data on a large public display and other users are approaching the public display area. In such a situation, 83% of all users would appreciate an automatic reaction of the system helping to protect their privacy. Out of this 83%, one third favors to be warned and would like to take necessary steps on their own, while the other two thirds prefer a system that automatically hides private data (see figure 3).

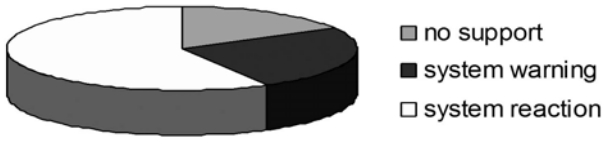

Fig. 3. Desired system support regarding privacy protection in group situations.

While automated privacy support seems to be favored by the majority of users, most of them are very reluctant to provide all the necessary information to auto-configure their privacy settings. For example less than 10% of the users would accept the collection of biometric information even if it is used to reduce their workload. The results show, that system developers must not rely on active user participation when implementing measures to safeguard user privacy, but should aim at designing easy and intuitive ways to handle personal privacy in everyday situations.

Approach

The demand for active privacy support led us to the development of a system that enhances privacy in group situations based on the current context and individual predefined trust settings. We aimed to develop a system that automatically hides information which is not intended to be seen by others while providing users with an easy interface to dynamically adapt the automated privacy support to their current needs. This is achieved by

the combination of a program for automated privacy management based on user-defined preferences and a small personal artefact which enables users to easily adapt their privacy settings to the local context. In the following section, we will describe both components as well as the underlying sensing infrastructure. Both prototypes were developed in the EU-funded "Disappearing Computer"-project "Ambient Agoras: Dynamic Information Clouds in a Hybrid Worlds" [13,14,15].

Privacy Manager

The Privacy Manager is a program that allows users to define their privacy settings and hence is the basis for an automated privacy support. The software consists of three components. The main component is responsible for hiding applications and files depending on the proximity of other users and the current privacy profile. These profiles are managed in the second component, the "Profile Editor". Each application and document can be classified individually or assigned to a group with predefined privacy settings. Additionally, it is possible to use these settings in combination with arbitrary keywords. The Profile Editor also allows to define and edit the trust levels for single users or user groups. This enables users to easily define rules like: hide all websites that contain the words "music" or "football", if the individuals "a,", "b" or the group "project team c" is near the display. These rules can be assigned to different privacy profiles, each linked to a different ID stick of the Personal Aura artefact which is described in the next section. The information about running programs and open documents is provided by the third component called "File System Watcher". It permanently monitors the local file system and transmits all relevant changes to the main component.

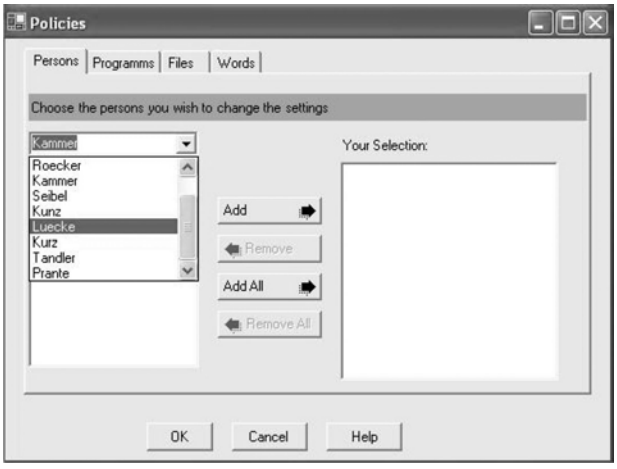

Fig. 4. Screenshot of the "Profile Editor"

The Personal Aura

In real life, every person adopts different social roles, depending on the present situation and current social environment. A person usually has several social roles which constantly change during the day. For example, the same individual can take up the roles of a family father, project manager, supermarket customer and member of a sports club during his daily routine. Within the professional role, there might exist different social profiles depending on project or team requirements. In all these roles, different types of information are disclosed to different groups of people and an unintentional disclosure of personal information might result in serious privacy infringements.

The Personal Aura is a small personal artefact designed to provide users with an easy and intuitive interface for recurring changes between the different privacy profiles defined in the Privacy Manager. The artefact consists of two matching parts: an ID stick containing the unique reference to a corresponding privacy profile, and a reader module which is able to transmit the data to the Privacy Manager (see figure 5). Each person has multiple ID sticks, which each stick symbolizing a different role with a related privacy profile. People can change their privacy profiles by connecting a specific ID stick to the reader module.

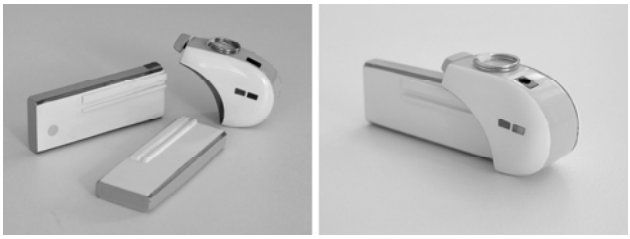
Fig. 5. Personal Aura: The reader module and two ID sticks (left), active Personal Aura (right).

The realization is based on active RFID transponders and allow detection ranges of up to 30 m within buildings. The existing circuit boards were modified and integrated in the two pieces of the Personal Aura artefact. The reader module comprises the battery, antenna and input/output controls, the ID stick contains the transponder electronics, identification information, and memory.

Sensing Infrastructure

The necessary information about nearby individuals is collected via a two-step sensing infrastructure. Infrared and active RFID sensors constantly monitor the area around each public display. For the identification of

persons via RFID we rely on the same standard technology that was used for the Personal Aura artefact. To detect the presence of persons who are not wearing a Personal Aura artefact we developed a special infrared detection system. The main component of the system is the IR-Box (see figure 6) that converts the signals from the IR-receivers and transmits them via a USB link to a host computer. Each IR-Box can handle up to ten IR-receivers simultaneously. People approaching a public display are detected by the infrared sensors and are simultaneously identified according to the current settings of their Personal Aura artefact.

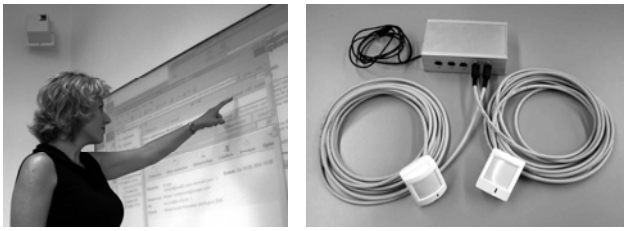

Fig. 6. Accessing personal information on a large public display with an RFID antenna in upper left corner (left) and infrared detection system with two sensors (right).

If people have deactivated their Personal Aura, the data collected from the infrared sensors still allow to detect the presence of people in the vicinity of the display. In such situations, when the identities of approaching individuals can not be determined, it would be possible to hide all personal information currently being displayed.

Conclusion And Future Work

In this paper, we described a novel approach for personalized privacy support at large public displays consisting of a program for privacy-enhancing information management based on individual privacy profiles and an easy and intuitive interface for recurring changes between different profiles. After receiving promising results in a first series of tests with a small group of users we are currently in the process of improving the current implementation according to the received user feedback. Our plan is to evaluate the revised implementation in a second, more detailed sequence of tests with a larger group of user.

Acknowledgment

This work was supported by the European Commission (contract IST–2000-25134) as part of the proactive initiative “The Disappearing Computer” of “Future and Emerging Technology” (FET). We thank our partners EDF, DALT, Wilkhahn, and wiege for contributing in the project “Ambient Agoras: Dynamic Information Clouds in a Hybrid Worlds” (www. ambient-agoras.org). Thanks are also due to the members of the AMBIENTE research division (www.ipsi.fraunhofer.de/ambiente) and our students – especially Sebastian Lex and Steffen Halama – for their various contributions and the implementation of hardware and software.

References

[1] Lamming, M., Eldridge, M., Flynn, M., Jones, C., Pendlebury, D. (2000) Satchel: Providing access to any document, any time, anywhere. *ACM Transactions on Computer-Human Interaction*, Vol. 7, no. 3, pp. 322 – 352.

[2] Eldridge, M., Barnard, P., Bekerian, D. (1994) Autobiographical memory and Daily Schemes at Work. *Memory* 2, 1, pp. 51 – 74.

[3] Whittaker, S., Frohlich, D., Daly-Jones, O. (1994) Informal workplace communication - What is it like and how might we support it? In: *Proc. of ACM Conference on Human Factors in Computing Science* (CHI ’95). ACM, NY, pp. 131 – 137.

[4] Churchill, E.F., Nelson, L., Denoue, L., Helfman, J., Murphy, P. (2004) Interactive Systems in Public Places: Sharing Multimedia Content with Interactive Public Displays: A Case Study. In: *Proc. of the 2004 Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, pp. 7 – 16.

[5] Russell, D.M., Gossweiler, R. (2001) On the Design of Personal & Communal Large Information Scale Appliances. In: *Proc. of the 3rd Intl. Conference on Ubiquitous Computing*, pp. 354 – 361.

[6] Huang, E.M., Russell, D.M., Sue, A.E. (2004). IM Here: Public instant messaging on large, shared displays for workgroup interactions. In: *Proc. of the ACM Conference on Human Factors in Computing Systems* (CHI 2004), pp. 279 – 286.

[7] Huang, E.M., Mynatt, E.D. (2003). Semi-public displays for small, co-located groups. In: *Proc. of the ACM Conference on Human Factors in Computing Systems* (CHI 2003), pp. 49 – 56.

[8] Rekimoto, J. (1998) A Multiple Device Approach for Supporting Whiteboard-based Interactions. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI 1998), pp. 18 – 23.

[9] Greenberg, S., Boyle, M., LaBerge, J. (1999) PDAs and Shared Public Displays: Making Personal Information Public, and Public Information Personal. *Personal Technologies*, 3, 1, pp. 54 – 64.

[10] Shoemaker, G.B.D, Inkpen, K.M. (2001) Single Display Privacyware: Augmenting public displays with private information. In: *Proc. of the ACM Conference on Human Factors in Computing Systems* (CHI 2001), pp. 522 – 529.

[11] Tan, D.S., Czerwinski, M. (2003) Information Voyeurism: Social Impact of Physically Large Displays on Information Privacy. In: *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems* (CHI 2003), pp. 748 – 749.

[12] Lahlou, S., Langheinrich, M., Röcker, C. (2005) Privacy and Trust Issues with Invisible Computers. In: *Communications of the ACM*, Vol. 48 March, pp. 59 – 60.

[13] Prante, T., Stenzel, R., Röcker, C., Streitz, N.A., Magerkurth, C. (2004) Ambient Agoras – InfoRiver, SIAM, Hello.Wall. In: *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems* (CHI 2003), pp. 763 – 764.

[14] Streitz, N.A., Prante, T., Röcker, C., van Alphen, D., Magerkurth, C., Plewe, D.A. (2003) Ambient Displays and Mobile Devices for the Creation of Social Architectural Spaces: Sup-porting informal communication and social awareness in organizations. In: K. O’Hara, M. Perry, E. Churchill, D. Russell (Ed.): *Public and Situated Displays: Social and Interactional Aspects of Shared Display Technologies*, Kluwer Publishers, pp. 387 – 409.

[15] Streitz, N.A., Röcker, C., Prante, T., van Alphen, D., Stenzel, R., Magerkurth, C. (2005) Designing Smart Artifacts for Smart Environments. In: *IEEE Computer*, March, pp. 41 – 49.