The Privacy Badge Revisited - Enhancement of a Privacy-Awareness User Interface for Small Devices

Sven Gehring[1] and Martin Gisch[2]

[1] gehring@eyeled.de, Eyeled GmbH, Science Park 1, D-66123 Saarbrücken, Germany, http://www.eyeled.de
[2] gisch@eyeled.de, Eyeled GmbH, Science Park 1, D-66123 Saarbrücken, Germany, http://www.eyeled.de

Abstract. In this paper, we present enhancements of the Privacy Badge, which is a privacy-awareness user interface for small devices with limited capabilities. The Privacy Badge was created to visualize privacy loss in ubiquitous and pervasive computing environments and to enable users to do privacy settings in an easy and understandable way. We introduce the service anticipation as a new feature and present enhancements of existing features. We evaluated the enhanced Privacy Badge with a user evaluation whose results approve the overall system as well as the modifications.

1 INTRODUCTION

When dealing with privacy visualization, there is a lack of appropriate concepts like there is for user interfaces for desktop computers. It becomes even worse when considering small screen mobile devices. One reason is that presenting information on mobile devices is a difficult task, due to their limited capabilities like small screens and small buttons. Nevertheless, privacy visualization for small devices is important, even more due to pervasive and ubiquitous computing.

In [GLB1], the Privacy Badge has been introduced, which is a privacy-awareness user interface for small devices. It visualizes the privacy loss that accumulates over time and allows the users of a pervasive computing environment to do privacy settings. We assume, that the more personal data persons loose, the smaller becomes their privacy. This is expressed in the term privacy loss and this is what the Privacy Badge tries to visualize in an easy and intuitive way. The version of the Privacy Badge presented in [GLB1] was only a prototype and therefore we could only evaluate the basic concept in a non natural prototype environment. Now we introduce a revised version of the Privacy Badge, which is an enhancement of the prototype version and offers new features like the service anticipation. Additionally, we evaluated the revised version with a user evaluation in order to approve the interface.

2 RELATED WORK

Privacy is an important topic and subject to a huge amount of research work. Nevertheless, only few literature exists that is specifically dedicated to user interface design for privacy.

In [NM1], Ngyuen et al. describe privacy mirrors, a framework that offers a catalogue of characteristics that have to be considered when handling privacy in socio-technical systems. Another approach is called Privacy for the RAVE environment by Belotti et al. [BS1]. It is one of the oldest approaches in the field of privacy awareness interfaces and it uses physical hints to visualize what is going on in a system. For P3P[W3C], a privacy description language for websites, there are various implementations available.

None of these works actually include methods for small screen devices. A first attempt on that can be found in the PaWS System[ML1] by Langheinrich, which offers a small PDA interface for viewing service descriptions and a list of active services in a ubiquitous environment. This attempt relies on providing large amounts of text, which is not appropriate for small screens and uses technical terms not feasible for non-technical persons.

3 DISCREET

The Privacy Badge concept has been specifically developed as the visualization application for the framework developed within the Discreet project. Therefore, it provides means for visualizing privacy related events within the framework and to set privacy preferences for it. The Discreet project is an FP6 european project for discreet service provision in smart environments[DIS] that involves 10 partners from 5 countries.

The goal of Discreet is to design, specify and implement a distributed framework, called *Discreet-Core* (D-Core). The D-Core is a fully distributed middleware, which acts as a distributed entity of mediation and provides primitives to properly manage privacy related data. The D-Core is aimed to manage the exchange of personal data among users, communication networks, environmental monitoring/sensing devices, and service providers. Its design goal is to minimize and control the amount of personalized information made available to the involved organizations, in order for the users to benefit of services without worrying about dissemination and improper use of their personal data.

Discreet includes law specialists to ensure that the technical solutions proposed in [KC1] properly address and reflect the legal requirements. The analysis of the legal situation defines a design space for privacy solutions which is delimited on one hand by rules prescribing the limitations under which data can be collected, stored, processed or communicated to third parties and is delimited on the other hand by rules enforcing the accessibility of some information for public security organizations.

Finally, a further goal of Discreet is the development of solutions to protect data when they are gathered and delivered to the unit of trust. The project specifically focuses on technologies and solutions deployed in intelligent environments, with special attention towards Wireless LAN (WLAN), Radio Frequency Identification (RFID) and sensor networks.

4 THE PRIVACY BADGE

The Privacy Badge is a privacy-awareness user interface, created to visualize privacy loss in ubiquitous and pervasive computing environments and enable users to do privacy settings in an easy and understandable way. The main goal of the prototype was to design an easy-to-use and intuitive user interface to visualize and manage privacy aspects in the interaction with services for the privacy-aware system architecture described in [KC1], which works on small, mobile devices, dealing with their restrictions. Since privacy loss is a rather abstract term that cannot be converted to a concrete number, percentages and absolute scales are no appropriate visualization approaches for it.

Hence, the metaphor of radiation badges[3] was chosen for visualizing the privacy loss that accumulates over time.

With the Privacy Badge, the user is able to see at a glance four characteristics of the privacy loss, namely *what has been disclosed*, *when has it been disclosed*, *to whom and to what end* and *does the user care about the information.*

4.1 User Interfaces

The Privacy Badge is separated in two user interfaces, an awareness user interface (miniature badge) for visualizing the privacy loss that already occurred and a detailed user interface (detailed view) for doing privacy settings.

The miniature badge is a small icon in a circle shape that is present on the screen at any time. It gives at-a-glance information without any details. The nearer to the center a point is located, the more important is the according data to the users. Fig. 1 shows three possible states of the miniature badge. The more crowded the badge, the higher the privacy loss.

When tapping the miniature badge, it expands to the full-screen detailed user interface that depicts the privacy loss which occurred. Each instance of a data loss occurrence is shown as a small symbol, representing the certain data type. If the view gets too crowded, filters can be applied that show only certain data types or a specific service.

4.2 Changing Preferences

Setting and changing preferences is another mode of interaction with the Privacy Badge. This includes setting whether a specific service can access specific data

[3] Radiation Badges are devices handed out to workers who get in contact with radioactive materials. They collect radiation dosage over time and get darker with the total exposure increasing.

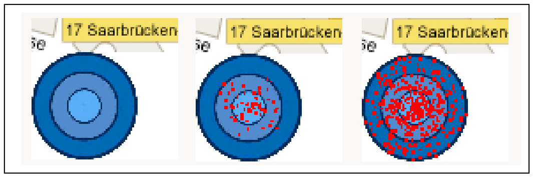


Fig. 1. Privacy Badge states. From left to right: no loss, some loss, high loss

or not. The user can switch to a preference view where he can simply adjust the preferences by moving the preferences icons with a drag and drop mechanism. The nearer to the center a data type is moved, the more important is the respective data type to the user. The metaphor here is a leash, because the users can keep their data ”on a short leash” to have more control over it. The angle of a data type is not evaluated but serves the purpose to help the user categorize his settings by grouping data together spatially. For a more elaborated grouping mechanism, one can switch to a novice mode where the data types are grouped together according to the ontology. In addition, the user can also switch to service view where services are shown as symbols around the user instead of data types.

To show, what data a service is allowed to get, the interface can be switched to a service-centered view as depicted in Fig. 2 on which the service is symbolized instead of the user in the middle of the badge. The data types it requests are arranged around it according to the preferences for the data types as well as the preferences set for the service. By overlaying the two user-centered views, the distance between the data type and the service can be interpreted as level of obfuscation or blurring of data. In short, this means that the service can only gain full access to data that is on the same level or further away from the user than the service.

5 THE PRIVACY BADGE ENHANCED

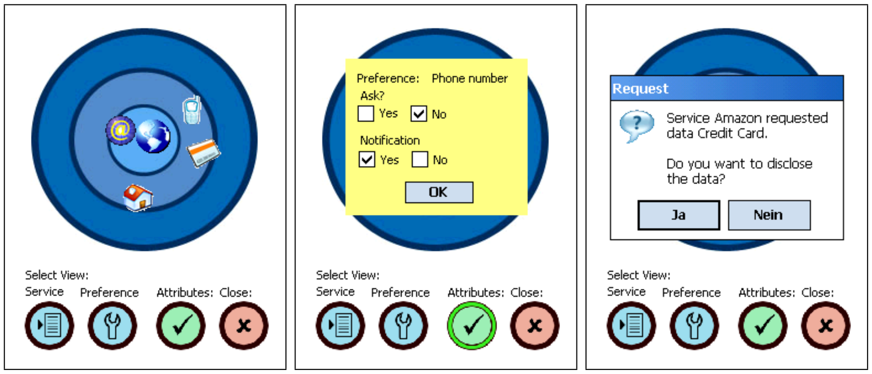
5.1 Setting Preferences

When setting preferences, the users could so far only specify if they want to disclose a certain data type or not. While working with the Privacy Badge, we decided to extend the preference setting functionality by adding two attributes to the preferences that can be set by the users. Like shown in Fig. 2, the users can now decide, if they want to be asked for disclosure every time data of a particular type is requested. They can also specify if they want to be notified when personal data of a certain type is disclosed. This gives the users a better control over the disclosure of personal data.

5.2 Service Anticipation

If a service requests personal data of the users, it might be possible that this particular service requests several different personal information. To enable the users to see all data types requested by one service at a glance, we added the feature of service anticipation. The Privacy Badge is now capable of displaying *all* information a service requests in a service anticipation view, which is shown in Fig. 2. Before any data is disclosed the users have the possibility to see what would be disclosed and what preferences apply to the case at hand. In addition to the privacy preferences, the service description is shown so the users has every data they need to calculate his "return on disclosure", meaning what he gets and what - in terms of privacy loss - they have to "pay" for it.

Using the same interface used for setting the preferences, the users are now enabled to decide whether the surplus value of a new service's use outweighs the privacy loss associated with it before using the service.



Preference: Phone number
Ask? ☐ Yes ☑ No
Notification ☑ Yes ☐ No

Request
Service Amazon requested data Credit Card.
Do you want to disclose the data?

Fig. 2. From left to right: setting preferences for a single service in the service anticipation, setting attributes of a preference, user is asked for consent.

6 USER EVALUATION

Since we enhanced a privacy-awareness user interface, it is essential to verify the used concepts in order to provide a user interface which is easily understandable and useful for real users. Hence, we conducted a user survey with 10 participants. The average age of the participants was 28.8 years. Every participant owns a cell phone and uses mobile devices like PDAs or cell phones regularly. By this, we can assume that the participants are conversant in interacting with small devices.

6.1 Preparation

As the very first step of preparing the survey, the Privacy Badge must be introduced to the participants.Therefore, every participant received the same introduction on the Privacy Badge.

We started with introducing the separation of the Privacy Badge into the awareness user interface and the detailed user interface and how the two user interfaces are related. The introduction was continued by the introduction of the three different states of the awareness user interface, which are *empty*, *little crowded* and *highly crowded*. The last part of the introduction covered the detailed user interface and its views as well as the functionalities that are offered by the views. The introductory part was finished by explaining how to perform several tasks like setting a preference value in the detailed user interface or activating a filter.

6.2 Conduction

After passing the introductory part, every participant was asked to perform the same tasks with the Privacy Badge. The tasks to perform were looking at the three different states (empty, little crowded, highly crowded) of the miniature view, switching to the detailed user interface, switching to the service view and finding out more about the disclosed data, setting a preference value and finally setting preference values in the service anticipation view.

After performing the tasks, we handed out a questionnaire with 25 questions that could be answered on a scale from 1 to 10 where 1 is the worst, 5 standard and 10 the best.

6.3 Result

By evaluating the survey, we can say that the results approve the concepts used in the Privacy Badge, as well as the enhancements made to the earlier version of the Privacy Badge. The average result on the questions we asked can be found in Fig. 3. The participants liked the general design (7.6) and evaluated the usability of the Privacy Badge as user friendly (8.7). They also liked the partition of the Privacy Badge into a miniature badge and a full-screen view (9.1).

Asked about the miniature badge, the participants liked the design (6.7) and evaluated the three different states as easy to understand (8.3). The position of the miniature badge on the screen of the PDA was rated to be reasonable (8.2) as well as the permanent visibility of the awareness user interface (6.6).

In the last block of questions concerning the detailed user interface, the participants expressed they like the design (7.7) and interaction (7.3) of the user interface as well as the separation of the different views inside the detailed user interface (8.0). The concept of using the distance to the center of the different views as a measure of importance was evaluated as reasonable (7.4). Asked about the service view, the participants liked the possibility of receiving additional information on the disclosed data by clicking the point on the screen (7.9) and rated the view as easy to understand (7.5). The preference view was also rated as easy to understand (7.3) and easy to use (7.4). The availability of the service anticipation feature was rated reasonable (7.4). According to the participants, the service anticipation is easy to understand (7.3) and easy to use (7.0). Furthermore, the participants liked the feature of filtering for certain data types (7.6). One general remark that was raised by some participants was the absence of a Privacy Badge internal help function. This might be a feature to add in future versions of the Privacy Badge. One might argue that the result of the evaluation is not representative, since the participants were only cell phone and PDA experienced users and therefore represent only a small part of the population.

This can be countered by the fact that the Privacy Badge is designed for experienced users which frequently use mobile services. Hence, the result of the survey is representative since the participants represent the target audience of the Privacy Badge.

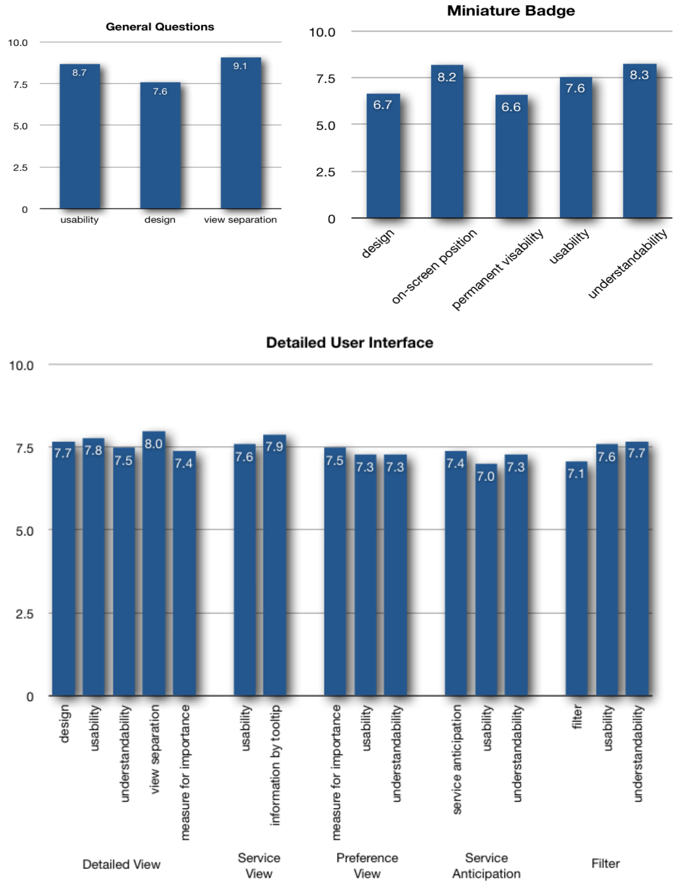


Fig. 3. User Evaluation, questions and average answer.

Summing up the evaluation, we can say that the enhanced Privacy Badge together with the used concepts was approved by the users.

7 DISCUSSION AND FUTURE WORK

In this work, we introduced an enhanced version of the Privacy Badge, a privacy-awareness user interface which is appropriate for small devices with limited capabilities. We evaluated the Privacy Badge with a user evaluation with 10 participants. The participants rated the Privacy Badge as easy to understand and easy to use. They had neither problems with understanding the used concepts nor with performing given tasks. Hence, the Privacy Badge together with the used concepts was approved by the evaluation.

A starting-point for future work would be the enhancement and standardization of the Discreet framework and the Privacy Badge. It is desirable that the Privacy Badge can be integrated and used on mobile devices or also on common desktop computers when surfing the internet or using applications that need to handle private data.

8 ACKNOWLEDGEMENTS

This work is partially supported by the European Union, in the framework of the FP6 - IST Project DISCREET.

References

[BS1] V. Bellotti, A. Sellen: **Designing for Privacy in Ubiquitous Computing Environments**. In: The third European Conference on Computer-Supported Cooperative Work. Milan, Italy. September 1993.

[PB1] CMU Usable Privacy and Security Laboratory. **Privacy Bird.** 15.03.2006. http://www.privacybird.com/

[DIS] **Discreet Project - Discreet Service Provision in Smart Environments**. Official Homepage, http://www.ist-discreet.org, 2007.

[SG1] S. Gehring: **The Privacy Badge - Development and Implementation of a Privacy-Awareness User Interface for Small Devices**, Master's Thesis, Computer Science Library, Saarland University, Saarbrücken, Germany, January 2008.

[GLB1] M. Gisch, A. De Luca, M. Blanchebarbe: **The Privacy Badge - A Privacy-Awareness User Interface for Small Devices**. In Proceedings of the Mobility Conference 2007. Singapore, 10-12 September,2007.

[KC1] C. Kiraly et al.: **System Architecture Specification**, IST DICREET Deliverable D2201, October 2006, available at http://www.ist-discreet.org/Deliverables/D2201.pdf

[ML1] M. Langheinrich: **Personal Privacy in Ubiquitous Computing Tools and System Support**. Dissertation, University of Bielefeld, Bielefeld, Germany, 2005.

[NM1] D. Ngyuen, E. Mynatt: **Privacy Mirrors: Making Ubicomp Visible**. In CHI 2001. Seattle, WA.

[W3C] W3C: **The Platform for Privacy Preferences 1.0**. (P3P1.0) Specification. 16.04. 2002. http://www.w3.org/TR/P3P/

[YOU] YOUpowered Inc: **Orby Toolbar**. 2001. http://www.pixelcode.com/youpowered/products_orbyintro.html