The Privacy Badge - A Privacy-Awareness User Interface for Small Devices

Martin Gisch
Eyeled GmbH
Science Park 1, 66123
Saarbruecken, Germany
gisch@eyeled.de

Alexander De Luca
Media Informatics Group
Amalienstraße 17, 80333 Munich,
Germany
alexander.de.luca@ifi.lmu.de

Markus Blanchebarbe
Eyeled GmbH
Science Park 1, 66123
Saarbruecken, Germany
blanchebarbe@eyeled.de

ABSTRACT
In this paper, we present the Privacy Badge, 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. Moreover, the interface was created to work on small devices, which suffer of limited input and output capabilities and for which desktop interface approaches are not appropriate. We evaluated our prototype in a user study to find out, whether the concepts are suitable and users are able to interact with it. The evaluation shows that our approach satisfied our expectations. Nevertheless, during the study, some improvements to our idea could be identified, which we are planning to include and evaluate in future work.

Categories and Subject Descriptors
H.5.2 [**Information Interfaces and Presentation**]: User Interfaces – *Input devices and strategies.*

General Terms
Design, Experimentation, Security, Human Factors.

Keywords
Privacy, Privacy Awareness, Mobile Devices, User Interfaces.

1. INTRODUCTION
The presentation of information on small devices like mobile phones is a difficult task. This is mostly due to the limited input and output capabilities of these devices, like small screens and buttons. When thinking about privacy visualization, this problem is even worse since there is a lack of appropriate concepts for privacy visualization even for desktop computers. Nevertheless, privacy visualization for small devices is important, even more due to pervasive and ubiquitous computing. Such environments normally contain services that are likely to collect personal data of the users. In general, these services are either executed invisible, without the user knowing about it or, if any visualization is done, this mostly happens on small devices like PDAs and mobile phones.

In this work, we present the Privacy Badge, a privacy-awareness user interface designed for small devices. It enables users of the privacy aware computing system D-Core as specified in [3] to view their privacy status and the so called privacy loss at anytime. Additionally, it contains means for doing privacy settings for this system in an easy way regarding the limited input capabilities of small devices. This interface has been evaluated in a user study and proven useful and efficient.

Privacy at the user interface level has been also addressed in other research. In [5], Ngyuen et al. describe privacy mirrors, a framework describing a catalogue of characteristics that have to be considered when handling privacy in socio-technical systems. A very early approach called Privacy for the RAVE environment [1] uses physical hints to visualize what is going on in a system. Thus, it is one of the earliest approaches in the field of privacy aware interfaces.

For P3P [6], a privacy description language for websites, there are various implementations available. A highly elaborated P3P tool is Privacy Bird [2], which integrates into the Internet Explorer and signals the users whether a website's policy fits her privacy settings or not using bird icons in different colors. The Orby Toolbar [7] works very similarly, but provides a so-called trust meter which allows more fine-grained comparison of policies to settings than Privacy Bird. Unfortunately, the Privacy Bird visualization approach is way too undifferentiated while the Orby Toolbar provides a scale whose meaning remains incomprehensible for the users. Additionally, their privacy setting approaches rely on text intense interfaces.

None of these works actually includes methods for small screen devices. A first attempt on that can be found in the PaWS System [4] by Langheinrich which offers a small PDA interface for viewing service descriptions and a list of active services in a ubiquitous environment. However, the interfaces rely on providing large amounts of text, which is not appropriate for small screens and use technical terms not feasible for non-technical persons. In contrast to that, for the Privacy Badge we tried to find mechanisms usable for everyone, even for people without special technical knowledge.

At first, we will describe the privacy badge in detail. This includes how it visualizes privacy loss and risks as well as how it can be used to set privacy preferences. After that, the user study will be outlined in detail as well as its result. Finally, an outlook on future work is presented.

2. AWARENESS UI PROTOTYPE

2.1 Design Goals

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 [3]. More important, the interface has to work on small, mobile devices, dealing with their restrictions: small screen space and limited input capabilities. In particular, the limited input capabilities need to be taken into account when creating preference setting concepts since long lists, text fields, long texts etc. are bad concepts for small devices.

During the design phase, we found that two modes of user interaction and thus of interfaces are required: one to visualize and interpret the loss of privacy that already occurred and the other one to adjust the users' preferences regarding their private data. Nevertheless, one of the design goals was to make both modes similar in appearance leaving the user with only one interface metaphor to learn.

In this work, we introduce the concept of the so called privacy loss visualization. The idea is to find a form for showing a highly abstract process, the loss of privacy, to the users. While they are interacting with pervasive and ubiquitous services, private data about them is disclosed to these services. Thus, over time, the amount of lost privacy increases and users should be notified about that.

This so called privacy loss is a rather abstract term that cannot be converted to a concrete number. Thus, percentages and absolute scales are no appropriate visualization approaches for it. Since there is no absolute scale to measure the amount of privacy loss, exact information (if produced via some sort of heuristic or algorithms which assigns a certain weight to different types of privacy loss) is useless and should be avoided. This rules out any form of scale or meter because there is always a percentage implied which misleads the user into thinking "I have still 50% of my privacy" when there is no scientific base for such a statement.

With the privacy-aware interface, the user should be able to see at a glance four characteristics of the privacy loss:

- What has been disclosed? (i.e. the datatype)
- When has it been disclosed? (in order to judge retention times of the information)
- To whom and to what end? (i.e. the service which requested the information)
- Does the user care about the information? (i.e. was that information important according to his preferences)

2.2 Main Metaphor

In order to show something, which accumulates the privacy loss over time without providing a direct scale and which can be integrated easily in any existing user interface on small devices, we chose the metaphor of radiation badges.

Radiation Badges (also known as dosimeters) are devices handed out to workers who get in contact with radio-active materials. They collect radiation dosage over time and get darker with the total exposure increasing. Normally they are worn as badges on the workers' coveralls but models in form of cards or even rings also exist. Each exposure registers as some points of the badge getting dark where rays have hit the exposure-sensitive coating.

Figure 1: Privacy Badge states. From left to right: no loss, some loss, more loss.

Fortunately, this metaphor easily transfers to our privacy loss scenario. For our prototype we decided to create a digital badge, which we darken more and more to illustrate continuing loss of privacy. Still, this leads to some sort of scale, but there is no exact amount and thus, no misinterpretation of values. The metaphor also implies an ongoing change in the interface which will be noticed by the users and may be helpful to rate the privacy loss over a specific amount of time. Figure 1 shows three different states occurring in an exemplary change that is likely to happen over time.

2.3 Awareness UI

Since normally, the screen of the device is needed for displaying service related information, it is not feasible to display a huge amount of privacy information on the screen during the service execution. Even though, the visualization respectively the privacy-awareness should be present at every time, it has to be available in an ignorable and space sparing way. Therefore, we decided to have a small badge present each time at the lower left of the screen.

This miniature badge, as shown in Figure 1, is always visible in each application and gives at-a-glance information without any details. When new privacy loss occurs a notification mechanism is started. The badge can blink, beep or start vibrating. By tapping the miniature badge, a more detailed view is provided to the user in which he has the possibility to review the loss in detail and change his personal privacy preferences.

For the details view, there is either a badge shown with privacy losses from each used service or an overall badge which sums up all privacy loss as explained in the next section.

2.4 Detailed UI

2.4.1 Interpreting Data Loss

When tapping the miniature badge, it expands to a full-screen view of the privacy loss interface, which is depicted in Figure 2. Each instance of a data loss occurrence is shown as an icon representing the type of the data disclosed (i.e. a "$" for credit card information, a telephone for address data, etc.). Since this view includes all losses for all services, it is possible that the same data type occurs several times at different locations. The symbol in the middle of the badge depicts the user having the data arranged around. If the view gets too crowded, filters can be used to show only certain data types or a specific service. At the moment, three filter types are available: by time, by service and by datatype.

Nevertheless, standalone symbols, i.e. only displaying these icons, would be useless, because they do not imply any information but the datatype. Therefore, by tapping the symbols,

tooltips appear in which the time and date as well as the service and the type of data are shown in detail. Tapping has been chosen instead of any mouse over effect as the input type because we are dealing with small devices that do not support mouse interaction but for example pen interaction for PDAs.

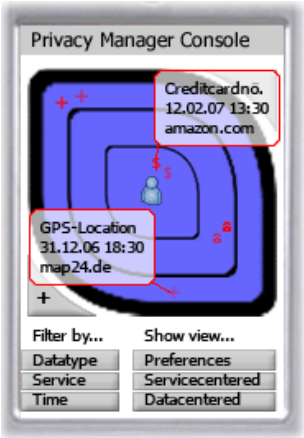

Figure 2: Detailed view of the Privacy Badge.

As shown in Figure 2, the badge is divided into concentric rings which symbolize the importance of the data with less important data put further away from the user in the middle. Talking about the miniature badge from Figure 1, this means that when dots cumulate around the center, the privacy loss concerns important data. If they cumulate near to the outer border, the privacy loss contains mostly unimportant data.

With these metaphors, we are able to answer the questions set in the design goals as follows:

- What has been disclosed is indicated via icons and colors.
- When the incident occurred is shown in the tooltips but can also be visualized through fading in size and color.
- To whom the information has been disclosed is shown in the tooltips or via the filters.
- Whether the user cares is shown through the distance to the center, the icons being arranged according to the user's preferences.

2.4.2 Changing Preferences

The second mode of interaction with the Privacy Badge is setting user preferences. That is, how the users want their data to be handled. For instance, this includes whether a specific service can access specific data or not. Thus, through the buttons in the lower right corner the user can switch to the preferences view as shown in Figure 3 (left) where he can move around the icons representing the datatypes with a simple drag and drop mechanism. The nearer to the center a datatype is moved, the more important is the respective datatype to the user. The metaphor here is a leash, because the user can keep his data "on a short leash" to have more control over it.

The angle in which a datatype is set relative to the user is not evaluated but serves the purpose to help the user to categorize his settings by grouping data together spatially. For a more elaborated grouping mechanism, one can switch to a novice mode where similar datatypes are grouped together automatically.

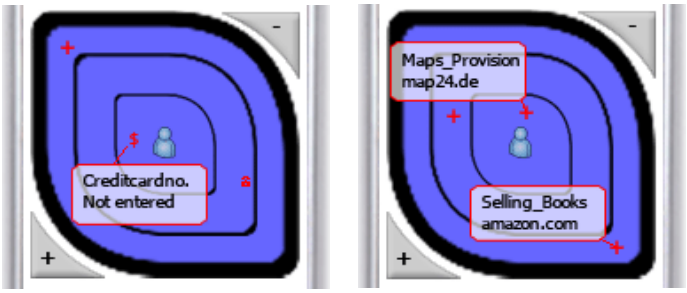

Figure 3: Preferences view. Datatype view (left) and service view (right).

In addition to this so called datatype view (Figure 3 left) of the preferences the users can switch to a services view (Figure 3 right) where services are shown as symbols around the user instead of datatypes. This view can be used to alter preferences for a specific service only. Here, the distance to the center is interpreted as how much the user trusts the service.

Figure 4: Service centered view.

To show, what data a service is allowed to get, the interface can be switched to a service-centered view as depicted in Figure 4 on which the service is symbolized instead of the user in the middle of the badge. The datatypes it requests are arranged around it according to the preferences for the datatypes as well as the preferences set for the service.

By overlaying the two user-centered views (datatype view and service view), the distance between the datatype 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.

Figure 5 shows how this overlaying is done. In both diagrams you see the datatypes in red and for better clarity the services overlaid in green. To extract privacy information for one specific service and one specific datatype it requests, the distances to the center of both markers are computed and compared.

The first case shows a service near the center meaning the user places great trust in this service. The datatype (location information) is held on a long leash meaning the user does not care about which service gets this information. Because the distance of the service and the user is smaller than the distance of the datatype and the user, this service gets the requested data.

distance(User,Service) <= distance(User,Datatyp) = disclose

In the second case you can see, that the service is in the outmost circle of the badge meaning distrust of the user whereas the requested datatype (here: credit card number) is in the innermost circle meaning a high privacy value assigned to it by the user.

Because the distance of the service and the user is greater than the distance of the datatype and the user, the service won't get this data.

distance(User,Service) > distance(User,Datatyp) != disclose

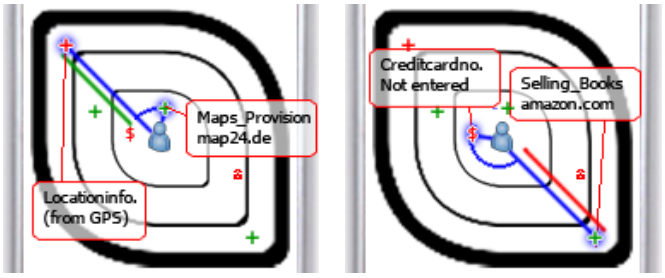

Figure 5: Data disclosure calculation for two services. Left: Service that gets location data. Right: Service that doesn't get credit card number.

When a new service or a new datatype is added to the system, the default values are applied to them. All data is in the center and all services are on the outer rim. Therefore, in the default setting no service gets anything and maximum privacy is applied. Preferences can be saved to assume different roles in different situations.

3. Evaluation

We not only created a privacy-awareness user interface for small devices, we also wanted to find out whether the concepts of the Privacy Badge are useful and understandable for real users. Therefore, we conducted a user study with 10 participants. The average age was 26 years. All of them owned a mobile phone and this they were used to interacting with small devices. For the study, we built a prototype with Adobe Flash simulating a PDA and containing the Privacy Badge functionality.

3.1 Procedure

For the study, we asked each participant to perform three different tasks related to the Privacy Badge. Before performing the tasks, the concepts were explained to all participants in the same way. The first task was a rather passive one. The participants were told to take a look at three different states of the miniature privacy badge: empty, little crowded, highly crowded. For the second task, they were told to switch to the detailed view, see what happened to their data and filter the view for at least two services. For the last task, they were told to make privacy settings in both the data view and the service view. At the end of the conduction, a questionnaire had to be filled out by each participant.

3.2 Results

The results of the user study approve the concept of the Privacy Badge. In the questionnaire, we asked the users to rate several concepts of the badge on a Likert scale from 1 (do not agree/like) to 5 (strongly agree/like). Regarding the users' answers, they liked the miniature badge (3.8) and found it easy to understand (4.0). The position of the badge was rated good (4.2) and the meaning of the different states could be identified without any problems (4.4). When asked if they liked it, that the badge was always visible, also within other service screens, users affirmed with 3.8. Nevertheless, four users would prefer an option to hide and show the badge.

When asked about the different functionalities of the detail view and whether they liked it, the users rated the concept of the distance of data to the user (closer data is more important) with 4.7, the service filter with 4.2 and the additional information when clicking a symbol with 4.6. The ease of using the filtering was rated with 4.6.

The last block of questions was related to the preferences interface. They were asked to rate how they liked the different functionalities and rated the concept of moving the symbols and services and therewith affecting their importance with 4.8.

4. DISCUSSION AND FUTURE WORK

In this work, we presented the Privacy Badge, a visualization mechanism for the highly complex field of privacy awareness. Moreover, we developed a concept appropriate for the limitations of small devices, by entirely abandoning concepts of describing facts with huge amounts of text. Therefore, we relied on some visual metaphors like the leash metaphor.

We evaluated the Privacy Badge in a user study with fairly good results. All participants found it very easy to use the prototype, all concepts were clear to them and they had no problems interacting with the interfaces. However, the participants encouraged some improvements. Most importantly, two additional features were requested: enabling the users to hide the miniature badge and adding some kind of data set. That is, including a mechanism to mark data that will never be disclosed, not even to the highest trusted services. Therefore, we are planning to include these features into a future version of the Privacy Badge and conduct further evaluation.

As mentioned before, this work has been performed to find an appropriate user interface for the system developed in [3]. Since it has proven to be adequate for this purpose, one of the most important parts of our future work is to include it into this system.

5. ACKNOWLEDGMENTS

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

6. REFERENCES

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

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

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

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

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

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

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