HCI Pattern Collection – Version 2

Editors:	Simone Fischer-Hübner (KAU) Christina Köffel (CURE) John-Sören Pettersson (KAU) Peter Wolkerstorfer (CURE) Cornelia Graf (CURE) Leif Erik Holtz (ULD) Ulrich König (ULD) Hans Hedbom (KAU) Benjamin Kellermann (TUD)
Reviewers:	Eros Pedrini, (UNIMI) Stefanie Pötzsch (TUD)

Identifier:	D4.1.3
Type:	Deliverable
Class:	Public
Date:	February 27, 2010

Abstract

One of the core activities in PrimeLife is the design and implementation of privacy-enhancing identity management systems and applications that are usable. Therefore it is one of the goals of PrimeLife Activity 4 to create an extensive HCI (Human Computer Interaction) pattern collection to provide guidelines on how to design usable user interfaces for privacy-enhancing systems and applications. The HCI Pattern Collection – Version 2 presented in this Deliverable provides HCI patterns developed within the first two project years, which should guide all PrimeLife activities that are developing user interfaces. The HCI patterns are structured into patterns related to privacy policies management and display, patterns for the visualisation of privacy information, patterns related to workflows and interaction paradigms as well as descriptions of interactive PET mock-ups.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483 for the project PrimeLife.

SEVENTH FRAMEWORK PROGRAMME

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe – Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

List of Contributors

This deliverable has been jointly authored by multiple PrimeLife partner organisations. The following list presents the contributors for the individual parts of this deliverable.

Chapter	Author(s)
Introduction	Simone Fischer-Hübner (KAU) Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Template	Christina Köffel (CURE) Peter Wolkerstorfer (CURE)
Secure Passwords	Christina Köffel (CURE) Peter Wolkerstorfer (CURE)
Privacy Policy Display	Simone Fischer-Hübner (KAU) John Sören Pettersson (KAU) Christina Köffel (CURE) Peter Wolkerstorfer (CURE)
Dynamic Privacy Policy Display	Simone Fischer-Hübner (KAU) John Sören Pettersson (KAU) Christina Köffel (CURE) Peter Wolkerstorfer (CURE)
Informed Consent	Simone Fischer-Hübner (KAU)
Privacy Icons	Christina Köffel (CURE) Peter Wolkerstorfer (CURE)
Icons for Privacy Policy	Leif Erik Holtz (ULD) Ulrich König (ULD)
Trust Evaluation of Services Sides	Simone Fischer-Hübner (KAU)
Privacy Aware Wording	Christina Köffel (CURE) Peter Wolkerstorfer (CURE)

Policy Matching Display	Simone Fischer-Hübner (KAU) Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Data Track	Simone Fischer-Hübner (KAU) Hans Hedbom (KAU) Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Credential Selection	Erik Wastlund (KAU)
Privacy Existence in Collaborative Workspaces	Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Privacy Options in Social Networks	Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Selective Access Control in Forum Software	Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Privacy Enhancing Access Control for Wiki	Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Privacy Enhanced Group Scheduling	Cornelia Graf (CURE) Benjamin Kellermann (TUD) Peter Wolkerstorfer (CURE)
Delegation	Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)
Conclusions and Outlook	Simone Fischer-Hübner (KAU) Cornelia Graf (CURE) Peter Wolkerstorfer (CURE)

Executive Summary

This document provides the PrimeLife pattern collection for the privacy enhancing technologies (PETs) developed in PrimeLife. One of the core activities of PrimeLife is the design and implementation of privacy-enhancing identity management (IDM) systems and applications that are usable.

Activity 4 has the task to provide HCI (Human Computer Interaction) guidance to other PrimeLife activities, which is provided with the help of this HCI pattern collection. The HCI pattern approach should enable capturing, sharing and structuring user interface knowledge for PrimeLife.

The HCI Pattern Collection contains the final status of the HCI-SEC pattern collection within PrimeLife. HCI-SEC means the part of the Human Computer Interaction which concerns especially with (information) security. The patterns are organised and structured according to common pattern description methods into problem, solution, use when, how, why and related patterns. The problem statement provides an overview of the given problem that is resolved through the pattern. The solution shortly introduces the suggested solution, if possible underlined with some images. Use when and how describe when and in which way this pattern is best applied. Patterns that are related to the current pattern are to be stated in the section related patterns.

Whereas traditional patterns have been extensively tested and successfully employed for many years, the HCI patterns provided in this deliverable have different levels of maturity. The reason for this is that HCI for PETs and for privacy-enhancing Identity Management in particular is a rather new area of research, so that the HCI knowledge gained for this area is still limited and solutions have not been yet “successfully employed for many years”. We decided to still stick to the term "pattern" as we want to preserve the quality of the method itself which is the structured knowledge capturing and communication.

The patterns presented in this document are structured into the following categories:

PET patterns for privacy policies – patterns related to privacy policies

PET Visualisation – patterns related to icons and display of privacy information

PET Interaction – patterns related to workflows and interaction paradigms

Descriptions of interactive PET Mock-ups – this section provides holistic approaches to PrimeLife areas

The pattern collection can be found in the PrimeLife wiki (https://trac.ercim.eu/primelife/wiki/HCI/HCI).

Within the last project year, further user tests will be performed and some of the user interfaces. The knowledge that we will gain from these developments and user tests may lead to an update and extension of our HCI pattern collection. The final version will eventually be published as an appendix to the final HCI research report at the end of the PrimeLife project.

Contents

List of Figures

Chapter 1

Introduction

The PrimeLife project aims at addressing the life-long privacy and trust issues pertaining to technical and end-user challenges. Especially the latter challenges demand sound user interfaces for privacy enhancing technologies (PETs) which mediate the complex technical issues and provide end users with adequate interaction facilities in a user friendly way .

This document describes user interface (UI) patterns and interactive mock-ups for the different activies of PrimeLife that are developing user interfaces. It is the formal report of Activity 4 about the knowledge gathered during the work on PrimeLife mock-ups and prototypes within the first two project years. The pattern approach was introduced to PrimeLife to enable capturing, sharing and structuring user interface knowledge as patterns are a powerful tool for such objectives.

1.1 Background

Patterns are solutions to specific problems in various areas (e.g. programming, user interface design, etc.) that have been successfully employed for many years, especially in the area of user interface design (cf. Welie Patterns in Interaction Design [http://www.welie.com/patterns/], UI Patterns User Interface Design Pattern Library [http://ui-patterns.com/], Yahoo! Design Pattern Library [http://developer.yahoo.com/patterns]).

As the area of Usability of PETs is so new that solutions which are "successfully employed for many years" are not present we had to modify the pattern approach to fit PrimeLife's needs.

Our UI solutions - the patterns - evolved through the PrimeLife project and were evaluated using various empirical and heuristic evaluation methods. During the projects the focus for activity 4 changed slightly and shifted from small scaled patterns to more holistic interface approaches. Hence the collection in this document does not only include user interface patterns but also descriptions of interactive mock-ups of special areas of PrimeLife (e.g. the DataTrack).

As long term experiences with the patterns are not present we extended the title of the patterns with a rating which reflects the degree of user-feedback based re-design. Even though part of the patterns are holistic interface approaches rather than classical patterns, we choose to continue to use the term "pattern" and its respective style of description in order to preserve the structured knowledge capturing and communication that is inherent to the patterns.

1.2 Structure and Content of the Deliverable

The remainder of this deliverable is structured as follows:

Chapter 1 provides background information about the deliverable itself and the pattern approach taken in PrimeLife

Chapter 2 contains the patterns structured in:

- PET patterns for privacy policies – patterns related to privacy policies
- PET Visualisation – patterns related to icons and display of privacy information
- PET Interaction – patterns related to workflows and interaction paradigms
- Descriptions of interactive PET Mock-ups – this chapter holds the holistic approaches to PrimeLife areas

Chapter 3 provides conclusions and presents next steps.

Chapter 4 provide the literature list.

1.3 Gender-Neutral Speech

For the purpose of readability we refrain from using gender-neutral pronouns such as "he/she". Accordingly, gendered pronouns are used in a non-discriminatory sense and are meant to represent both genders.

Chapter 2

Patterns

2.1 Explanation of the Pattern Structure

The following sections explain the structure of a pattern and briefly describe a pattern's content.

Title (*****)

The title of the pattern includes in brackets a 5-star rating (from 0 to 5 stars) for reflecting how much end-user testing has been done on the pattern. It reflects how much experience we have with the pattern.

The rating scheme is as follows:

- Zero stars mean that there weren't any end-user tests done with it.
- One star: low-level HCI knowledge included (in form of usability principles)
- Two stars mean that at least the user-feedback of two users was integrated.
- Three stars mean that more than two preliminary user evaluations have been done.
- Four stars means that a pattern is in a draft state and only misses a final iteration round.
- Five-stars mean that much end-user testing was done and the results prove the content of the pattern; such patterns can be seen as final.

Problem

This section summarises and outlines the existing problem in the field of usable privacy and security, e.g. the user needs to login with personal data to some webpage, the user needs to acquire personal information from another user, etc. The problem outlines the given situation the application is placed into.

Solution

The solution-section briefly describes the intended solution to the problem as described before. Ideally the solution is underlined by some graphic displaying the best approach to solve the given problem.

Use when

This section outlines the situation the pattern is best applied in. For example, a login interface might be of need when users are frequently returning to a page and need protection in order to

disclose personal information. Basically a general scenario is given that describes the situation the pattern is best and most efficiently applied to.

How

While the solution-section only provided a short outline of how to best solve the problem, this section will provide more insights into the best way to solve the problem. The single steps needed for the solution are described, e.g. the password should be checked against a dictionary, etc. All different aspects needed to realise the solution should be clearly structured and outlined. This section instructs the developer on how to do it himself.

Why

This section reasons on why the solution is needed and how the user is able to benefit from it.

Related Patterns

This section simply refers the reader to other patterns solving or circumventing the problem.

2.2 PET patterns for privacy policies

2.2.1 Privacy Policy Display (***)

(By CURE, KAU)

Problem

Users need to be well informed about possible consequences when releasing personal data upon certain actions such as login, registration, payments, etc. Art. 10 EU Directive 95/46/EC requires that data subjects are at least informed about what personal data are processed, by whom (i.e. the identity of the controller), and for what purposes.

However Jensen and Potts (2004) as well as Protor et al. (2006) showed that privacy statements posted on web sites contain long legal phrases that are usually not comprehensible to most end users.

Solution

Provide the user with all necessary information on what kind of data is to be disclosed to whom and for what purposes it is used. The user should not be given too much and unnecessary information. The user should not be bothered with cumbersome work, for example in case of recurring visits. Therefore he should have the possibility to create customized settings. It is utterly important that the user understands possible consequences in order to make well-informed decisions.

The complexity of privacy notices can be better managed by following the Art. 29 Working Party's recommendation of providing information in a "multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions" [3]. They suggest three layers of information provided to individuals:

- short notice (layer 1)
- condensed notice (layer 2)
- full notice (layer 3)

The prototype of a menu-based approach for selecting Credentials developed within PRIME, which follows the Art. 29 Working party recommendation is shown below and is further described in (Pettersson 2008).

Figure 1: Prototype of a menu-based approach for selecting Credentials

Use when

This approach should be employed whenever the user is required to enter personal data such as login, credit card or other private information. Through this multi-layered approach, the user obtains information on why what information is requested, by whom it is required and what it is used for. Furthermore, a link to the condensed or full privacy policy needs to be displayed.

How

The Art. 29 Working Party (2004) recommends providing information in a "multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions". They suggest three layers of information provided to individuals: The short notice (layer 1) must offer individuals the core information required under Article 10 of the Directive 95/46/EC, which includes at least what data is requested, the identity of the controller and the purpose of processing. In addition, a clear indication must be given as to how the individual can access additional information. The condensed notice (layer 2) includes in addition all other relevant information required by Art. 10 of the Directive such as recipients or categories of recipients, whether replies to questions are obligatory or voluntary and information about the individual's rights. The full notice (layer 3) includes in addition to layers 1 and 2 also "national legal requirements and specificities."

Why

Informed users are able to make informed decisions which lead to a more responsible handling of their personal data. The EU Directive 95/46/EC therefore also requires that certain information needs to be provided to the user when personal data is requested from him.

Related Patterns

- Dynamic Privacy Policy Display
- Privacy Aware Wording

2.2.2 Dynamic Privacy Policy Display (****)

(By CURE, KAU)

Problem

Users need to be well informed about possible consequences when releasing personal data upon certain actions such as login, registration, payments, etc. Art. 10 EU Directive 95/46/EC requires that data subjects are at least informed about what personal data are processed, by whom (i.e. the identity of the controller), and for what purposes.

This information should be provided to the user in a way that he also recognized it and is able to capture its full extend.

Solution

The Multi-layered presentation approach by the Art. 29 Working Party (as described in the pattern "Privacy Policy Display") can be extended by dynamical information “tooltips” that inform the user about the nature of the data disclosed and possible consequences. The tooltips need to be adapted to the context of the website it is used on. It should only include relevant security and privacy information and have a unique standard layout that makes it easy to recognize.

Figure 2: PrimeLife prototype for dynamic display of information

Figure 2 shows a PrimeLife prototype for dynamic display of information without the mouse on the login-interface (left) and with the mouse on the login-interface (right). The privacy disclaimer appears on the login-interface, when the user is entering the required information. This prototype was used for usability tests in Austria. To reduce the bias of the language it was designed in German.

Use when

Dynamic privacy policy displays can be applied to small interfaces (e.g. login) or when the credential selection contains information that needs the user's attention. Research within the PrimeLife project has shown that users easier recognize dynamic privacy policy display interfaces.

How

The information should be provided to the user where it is needed. Therefore the tooltip should appear on demand (i.e. need of information). This could be for example in a login dialog as soon as the user navigates the mouse into the concerning part of the interface. The tooltip should then be made visible to the user and contain all necessary information for making an informed decision.

Why

Because of peripheral viewing, the user is able to recognize visual change (i.e. motion) even when on the border of the field of view. The user will recognize each visual change and might automatically connect it to danger. Hence he will immediately notice the visual change and direct the attention to it. Using this approach it is increasingly unlikely that the user might oversee the privacy indications.

Motion design is a known research area in the field of usability. According to Frank Jacob (2008), it decreases the cognitive load and creates user inputs – but only when applied correctly. Tooltips instead of pop-ups create a sense of seriousness (e.g. windows tooltips), whereas pop-ups are nowadays connected with error messages or unwanted advertisements. The physical connection between the tooltip and the Login dialog displays a certain attachment (i.e. that the tooltip is connected to the login dialog).

Related Patterns

- Privacy Policy Display

2.2.3 Policy Matching Display (**)

(By CURE, KAU)

Problem

Most policies are written in a very juridical language using long and complicated legal phrases . For many users i is very difficult to see if terms of the policy are matching to their prospect of privacy and security or not. Hence, UI elements are needed for informing users in a user-friendly manner on whether their privacy preferences (i.e., their privacy settings which they have defined earlier, e.g. by choosing from a list of predefined settings) correspond ("match") with the services side's privacy policy. The question on how to best inform users about mismatches between a policy and their preferences is however not an easy one. First of all, there is the risk that non-obstructive warnings are not noticed at all.

Furthermore, from our experiences from usability tests performed in PRIME and PrimeLife we see at least two more problems that privacy alerts must address:

First of all, we experienced that users may try to get rid of intrusive privacy warnings by changing to less privacy-friendly settings. In usability tests of early privacy policy management mockups, we experienced that very prominent warnings (illustrated by a yellow triangular warning sign with an exclamation mark) informing test users about a mismatch between her privacy preferences and the services side's privacy policy, led to some test users reacting in panic by changing to more "generous" privacy preference settings just in order to eliminate the warning.

Secondly, our previous usability tests also showed that extensive warnings can be misleading and can even result in users losing their trust in the identity management system.

The traffic light metaphor, which has been used by the AT&T privacy bird (http://www.privacybird.org/) to show whether a P3P policy matches the user's preferences (illustrated by a green bird), mismatches the user's preferences (illustrated by a red bird), or whether there is no policy existent (yellow bird), is not perfectly suitable, as users should actually be more alarmed about a site that has no policy at all (and thus does not give any privacy promises) than a site that has a policy, which is however not corresponding to all the user's preferences.

Solution

Create a tool with which users after having entered their preferred privacy settings can be informed in a noticeable but non-intrusive manner about how far their privacy settings match with a services side's policy. Hence, it should display to the user the terms of the policy in relation to the privacy settings of the user in a simple way.

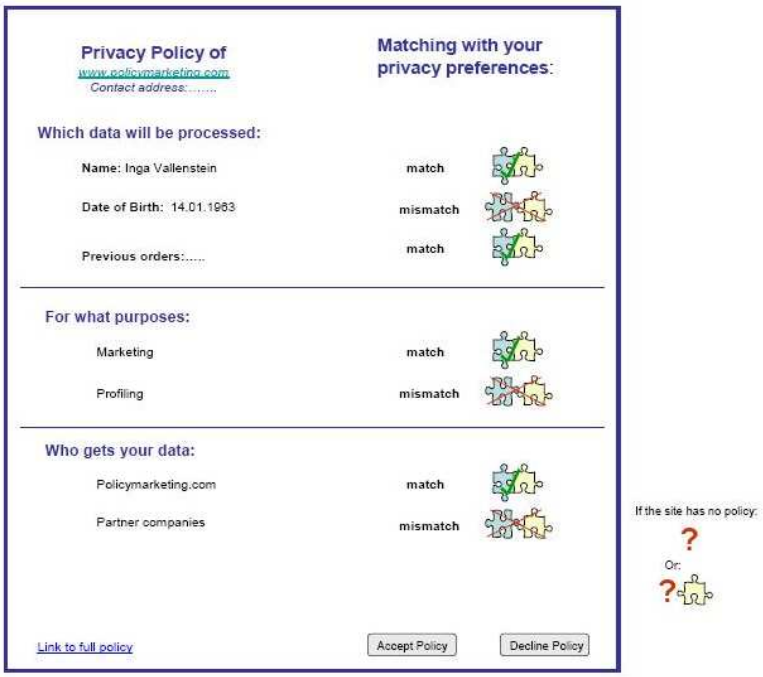

Figure 3: First draft of a policy matching display

Use when

The user's privacy settings should be compared to every policy as soon as a user contacts a services side. Besides, it should be displayed when users are requested to consent to disclose personal information.

How

An interface should be created, which helps the user to see which parts of the policy are matching to the preferred settings.

For informing users about matches/mismatches, we use the metaphor of matching/mismatching puzzle pieces in combination with a green check or red crossing through has been used. A missing policy is indicated by a red question mark. The red colour is however not used very prominently to prevent any irrational overreactions by users. The matching result is also described verbally.

The user can accept or decline each policy, irrespective if the policy conforms to the privacy settings or not.

Why

Privacy policies of web sites are often consisting of long and complicated legal statements that are difficult to understand and to evaluate by users with the consequence that many users just click “OK” without reading or understanding the content of the policy.

To display their current policy settings and visualize the matching between these settings and the policy should help users to make the essential parts of privacy policies more transparent and comprehensible.

Related Patterns

- Informed Consent
- Policy Icons
- Policy Display

2.3 PET Visualisation

2.3.1 Privacy Icons (*)

(By CURE)

Problem

Consistent, understandable and distinguishable icons concerning privacy are needed for all kind of applications where users find similar features to disclose personal data.

Solution

Icons, especially in the area of security and privacy need to speak for themselves, i.e. they need to be clear, represent the underlying purpose and should not offer space for misinterpretation. Users need to be informed about what is to be found behind an icon.

Figure 4: DataTrack Icon

The Data Track icon in PRIME's led many users (see PrimeLife deliverable D4.1.1) to the correct assumption that behind this icon they are able to see the traces that they have left online.

Figure 5: Data-Privacy Icons v0.1

Another icon-set called „Data-Privacy Icons v0.1" was developed by Matthias Mehldau, also described in (Hansen 2007).

Use When

In any case when icons are needed in the area of security and privacy it is important that they are speaking for themselves. A program's usability is not only determined by its functionality, feedback and response rate; but the cognitive load required by a user is also very important. The following image indicates some privacy icons and possible uses of them.

	You agree not to use this data for marketing purposes.
	You agree not to trade or sell this data.
	You agree to submit to a third-party audit program on data use; if government has requested access to my data, you agree to involve my governmental ombudsman.
	You agree to make available to me the data that you have on me without my having to pay for it/at a minimal charge.
	You allow me to address inaccuracies in the data and request its removal.
	You agree to take reasonable steps to keep my data secure.
	You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]

Figure 6: Icon-set from Rundle (2006) which is also described in (Hansen 2007).

How

Icons in use should be self-descriptive and allow to easily deducting their meaning. The Data Track for example, easily allows the user to assume that there are some data traces behind this information. Therefore it is utterly important that the icon uses a clear sign language.

Figure 7: Security icons from http://www.filebuzz.com/software_screenshot/

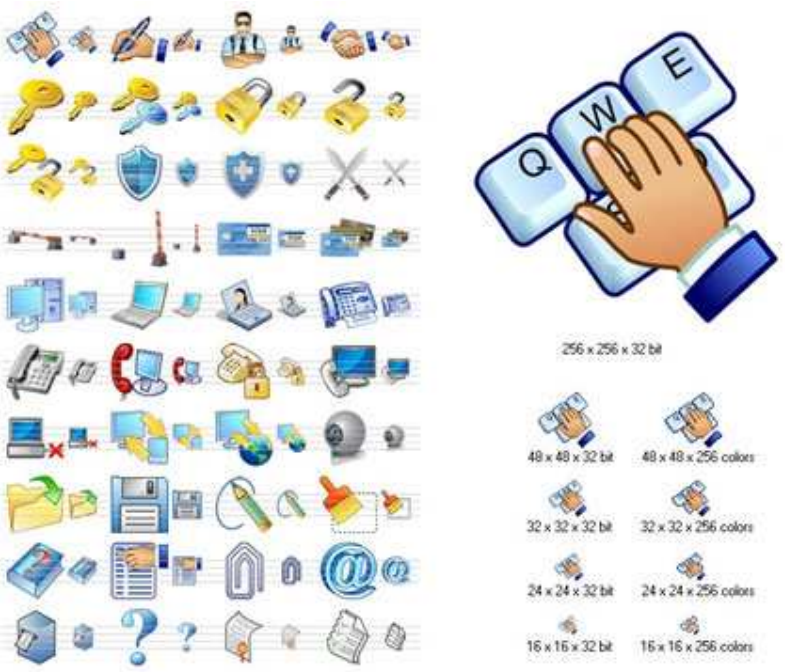

Figure 8: Example of an icon-set that can be purchased on the internet, taken from http://www.aha-soft.com/stock-icons/

Why

Informed users are able to make informed decisions which lead to a more responsible handling of private information. Since icons are an integral part of any kind of interfaces, it is important that they convey the right information. Furthermore users are only able to use an application/website to its full extend when they trust it. Therefore the icons used should look according to the purpose. Furthermore tooltips should be mandatory for all icons, not only from an accessibility point of view.

2.3.2 Icons for Privacy Policies

(By ULD)

Problem

One of the problems in developing solutions for privacy enhancing tools is the fact, that privacy policies and the description of the usage of data are often too long and too complicated. As a result many users do not read them.

Even if they read the privacy policies, it is often hard to understand, what kind of personal data are processed to whom and what exactly happens with the stored data.

Solution

This could be solved by using privacy Icons, which display how data are collected, processed and stored for which purposes and what happens to the data.

Icons do not displace a regular privacy policy, but they can be used in addition to point out the privacy aspects to all those users, who do not read the privacy policy.

These Icons must be clear and understandable in representing the underlying purpose and should not leave space for misinterpretation.

They also have to be displayed in a way that each user is informed about the purpose behind the Icons.

PrimeLife therefore has developed privacy Icons especially for social networks as well as privacy Icons for general usage.

Icons may display different things: special kind of data being collected, ways of processing personal data, subjects that are collecting personal data or Icons for different purposes for the collecting and processing of personal data.

Below there is an example of the developed Icons:

Figure 9: Personal data

Use when

This approach should be used every time when Icons in the area of security and privacy are needed for describing a policy or the usage of personal data. It is important that these Icons are self-explanatory. A program's usability is not only determined by its functionality, feedback and response rate; but also by the cognitive load required by a user is very important

The following examples may show, in which scenarios privacy Icons mightbe relevant and how they could look like:

Figure 10: Personal data

Figure 11: Sensitive data

Figure 12: Medical data

Figure 13: Payment data

Figure 14: Data purpose: legal

Figure 15: Data purpose: Shipping

Figure 16: Data purpose: user tracking

Figure 17: Data purpose: user profiling

Figure 18: Storage

Figure 19: Deletion

Figure 20: Pseudonymisation

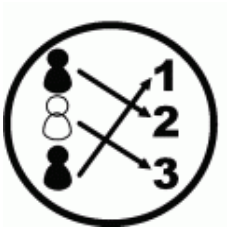

Figure 21: Anonymisation

The following examples may show, in which scenarios Icons for usage in social networking sites might be relevant and how they could look like:

Figure 22: Friends

Figure 23: Friends of friends

Figure 24: Selected individuals

Figure 25: Public

The following examples may show, in which scenarios Icons for displaying data transfer might be relevant and how they could look like:

Figure 26: Data dissemination

Figure 27: Data importing

Other Icon-Sets were created during the PRIME project, there is also another Icon-set called "Data-Privacy-Icons v0.1", developed by Matthias Mehldau which is described in 2.3.1, Figure 5: Data-Privacy Icons v0.1.

How

Any Icons in use should be self-descriptive and allow to easily deduct their meaning. The general Icons for medical data for example easily allow the user to assume, that there are personal data according his health, which he is revealing. Combined with the general Icons for data traffic, he can also see, what will happen with this very sensitive data.

Using icons when displaying policies should support the user to see on the first glance the important things of the policy. Therefore, it is important, that the Icons use a clear sign language.

They also have to be simple structured for being displayed on websites and applications. It is important, that Icons are still understandable for users even if they are displayed in a very small way.

If Icons are used in the same way on many of the applications or websites the user visits, it will be easy for the user to learn their purpose and to accept them as assistance. When users are aware of the icons from other purposes it will be also become more easy for them to create a mental model which supports them when reading a policy

In a first step, the user would only have to identify the Icons and decide manual, how he wants to handle the application the website or the policy. Another aim in using Icons could be in a next step the using of a program, that is able to scan each application or website a user wants to visit. This program would inform the user about the way of data handling and storing on the concerned sites.

Why

Users are only able to use an application or a website to its full intend, if they trust it.

Only well informed users will be able to make an informed decision, whether they want their personal data to be handled and stored.

These information should be displayed by privacy policies, which are usually read only by a few users. Instead of informing the user only by privacy policies - which might also additional be displayed by Icons - some of the important information could be displayed by Icons.

By using Icons the user may also decide to revoke a given consent on handling his data, because he now realizes, what really happens with the personal data.

Icons can also be used to increase the user's trust in a website or a community, because the usage of Icons leads to more transparency.

2.3.3 Privacy Awareness Panel in Collaborative Workspaces (****)

(By CURE)

Problem

The problem with users' awareness for privacy in collaborative workspaces, e.g., forums or wikis, is twofold. First, the users can contribute under self-chosen nick names instead of using their real names, which leads to a higher perceived anonymity of the users. However, providers of collaborative workspaces clearly get to know cues about a user's real identity (e.g., IP address, geolocation). Second, in collaborative workspaces, users disclose information – personal and non-personal – to an unknown audience. They have no idea how many and what kind of people can access their contributions.

Solution

In the so-called privacy-awareness panel, it is shown to the user which audience (all internet users, registered users, girls younger than 26…) can access his/her contribution and it is also pointed out that providers have additional information about the user. Hence, the privacy-awareness panel helps users to better understand their level of anonymity and private sphere within the collaborative workspace and based on this they can make better informed decisions whether they want to disclose personal information in their contributions.

The following Image shows the top section of a privacy-enhanced forum.

Figure 28: Privacy Awareness Panel of a Forum

Figure 29: Mockup of a Privacy Awareness Panel for a Wiki

Use when

The approach should be used with every collaborative workspace.

How

First, it should be made clear to users who is able to access their contributions. Second, users should know that providers get additional information about them for instance their IP addresses, browser versions, location information etc. and thus that they are not completely anonymous in the forum, wiki or other collaborative workspaces.

Why

To allow users to make better informed decision whether they want to disclose personal data in their contributions to collaborative workspaces.

Related Patterns

- Privacy Options in Social Networks
- Selective Access Control in Forum Software
- Privacy Enhanced Group Scheduling

2.4 PET Interaction

2.4.1 Secure Passwords (****)

(By CURE)

Problem

Since passwords are keys to many applications it is necessary for human to remember them. Without knowing their passwords they are not able to get access to the offer they want to use – is the same like standing in front of a house without the key.

So most users choose passwords which are easy for them to remember, but easy passwords play into the hands of hackers.

The usage of secure passwords is necessary to improve security and privacy of personal data. The problem is that current password selection mechanisms do not allow including usability mechanisms 0,[23].

Solution

According to [5] there are three different possibilities to help users create secure passwords:

- Passive mechanisms (e.g. help button)
- Static mechanisms (e.g. pop-ups)
- Dynamic mechanisms (e.g. dynamically adjusting message)

The method that is most noticed by the users and therefore also most helpful are dynamic mechanisms [5]

When the user has to re-enter a password it is also helpful to provide according feedback (e.g. passwords match, passwords do not match). The following three images indicate possible solutions for the issue of creating secure passwords. In any case the display of the level of security should be obvious and easy understandable by the users. Additional help such as tips on how to increase the security of a (existing) password can also be provided (e.g. "your current password does not contain numbers" or "click here to read more on how to increase the security of your password").

Figure 30: Passive/dynamic example by Conlan and Tarasewich (2006)

Figure 31: Dynamic example with feedback on the verified passwords from http://www.mepisguides.com/Mepis-6/user-tools/changing-password/change-password.html

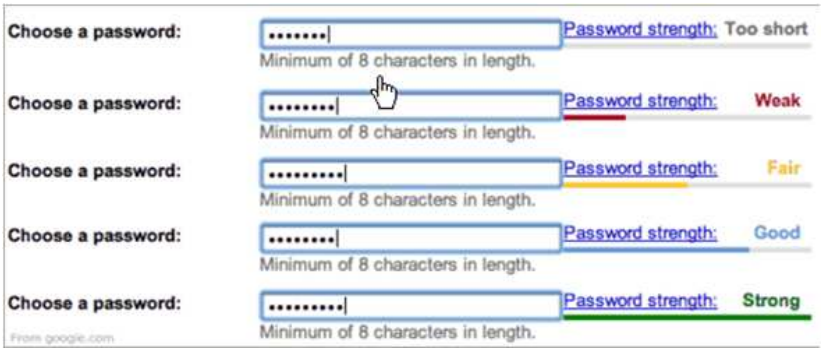

Figure 32: Example for Password Strength Meterfrom http://ui-patterns.com/pattern/PasswordStrengthMeter

Use when

For every interface the user needs to change a password. It is utterly important that the user gets appropriate feedback to all actions. Therefore dynamic feedback immediately informs the user whether or not the chosen password is safe. According to current research, users are able to remember more complex passwords when provided according feedback (PGP, Gehringer 2002). Users are generally interested in safe passwords but are lacking the knowledge on how to create secure passwords 0, [25]. Available password changing mechanisms do not provide enough information for the users to choose secure passwords. Current password changing interfaces do not offer any information neither on the security of the password nor on the correctness of the verified password.

Figure 33: Example for current password changing mechanisms

How

Four different feedback and help mechanisms should be incorporated into the password changing interface. The password-check should be accurate, use appropriate algorithms (not only dictionary-based), should not cause any delay in the interface's response and should require the user to re-enter the password in order to confirm its accuracy. With this methodology the user benefits by:

- Obtaining appropriate feedback on the security of the password (length, composition),
- Obtaining help functionality where appropriate.

Why

Secure passwords are very important in today's online life. Users generally tend to use familiar words such as names of pets and family members and no special signs when creating a password. These passwords can hence be easier hacked using social engineering than longer passwords containing special signs. Secure passwords are a necessary step towards personal security. Using the above approach, the user obtains more feedback on the safety of the entered password and is therefore able to create safe passwords that can be remembered.

Related Pattern

- Pattern "Auto Create Password" to be implemented in PrimeLife

2.4.2 Informed Consent (****)

(By KAU)

Problem

“The data subject's consent is defined as any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed” (EU Directive 95/46/EC). Informed in this context means that the user fully understands what he is agreeing to and what implications this may have.

Informed consent by the data subject is often a prerequisite for the lawful data processing (see for instance Art. 7.a EU Directive 95/46/EC or Art. 8 EU Directive 2002/58/EC). Informed user consent is also seen as a HCI requirement in [16].

A special challenge is the development of UI constructs for obtaining really informed and unambiguous user consent for the disclosure of personal data. Ordinary click-through dialog windows with long legal terms, which are often used, may cause users to click the "I Accept" button too easily if the preference settings have filled in all the requested data for them. Putting up "Are you really sure?" boxes does not resolve the problem as people may often click the "I Accept" or "OK" button even more automatically if they have to go through an extra dialogue box every time [21]. Also Dhamija et al. conclude that when confronted with dialog boxes such as for end-user license agreements, users tend to quickly skim the text and efficiently swat away the dialog boxes without having read or understood what they consented to [6].

Solution

The following HCI concepts provide solutions for obtaining informed consent:

- Just-In-Time-Click-Through Agreements (JITCTAs), i.e. click-trough agreements that instead of providing a large list of service terms confirm the user's understanding or consent on an "as-needed basis" [16]
- Selection via cascading context menus, where users have to choose more consciously the menu options of data to be released
- Drag-and-Drop Agreements (DADAs), which also requires user to make more conscious drag and drop actions for consenting to data disclosures

Use when

These UI solutions should be employed whenever data disclosures need to be legitimised by the user's informed consent.

How

JITCTAs are as small agreements easier for the user to read and process and facilitate a better understanding of the decision being made in-context [16]. JITCTAs are in fact corresponding to such short privacy notices as defined by the Art. 29 Working Party (see entry on "Privacy Policy Display"), which include information about what data is requested, the identity of the controller and the purpose of processing. The "Send Personal Data?" depicted in Figure 34 corresponds with its form and content to a JITCTA.

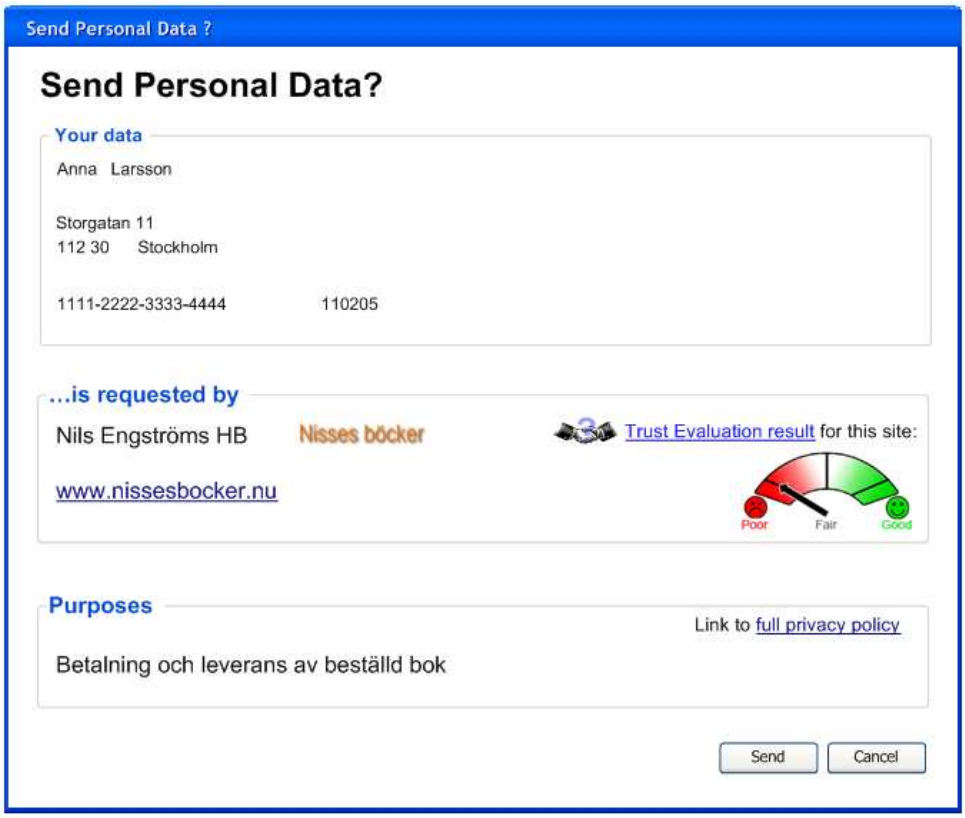

Figure 34: Send Personal data? - Window as a JITCTA for obtaining informed consent

As mentioned before, click-through dialogs have the disadvantage that users tend to click the OK button too easily without having read the text [21]. Presenting data items in cascading menus to select data or credentials, as shown in Figure 1, has the effect that the user must read the text for making the menu choices, which means that in this case she should make more conscious selections. Such cascading context menus need to also include the other information that is relevant for data disclosures, and therefore should also follow the Art. 29 WP recommendation for a multilayered structuring of privacy policies. However, this user interface design is not suitable if many data fields have to be filled; the design is intended as a special feature for very simple data requests where the user might have to select among a few credentials asserting a specific data claim.

"Drag-and-Drop Agreements" (DADAs) were also elaborated in the PRIME project in the context of a town map-metaphor based user Interface paradigm as a method for raising the consciousness about the nature of data disclosure [17]. Symbols were used to represent personal data – this allowed users to visibly drag-and-drop data to icons representing the receivers. Here, the user not only has to pick a set of predefined data (corresponding to clicking "I Accept", "I Agree" or "Send" in a pop-up window), but choose the right personal data symbol(s) and drop them on the right receiver symbol. These explicit actions to some extent offer a guarantee for more conscious user consent.

Figure 35: DADA for obtaining informed consent for disclosing credit card data

Why

Ensuring that users fully understand and unambiguously agree to the processing of their personal data is important for complying with legal privacy requirements. It is also a prerequisite for enabling control of users over their personal spheres.

Related Pattern

- Privacy Policy Display

2.4.3 Privacy Aware Wording

(By CURE)

Problem

Users should clearly understand the content of and terms used within privacy and security software. The terms are usually formulated on an expert-basis and therefore often difficult to understand for the average user.

Solution

Only easy to pronounce terms and phrases should be employed. They should be clearly formulated and understandable – even by users that are not familiar with privacy and security.

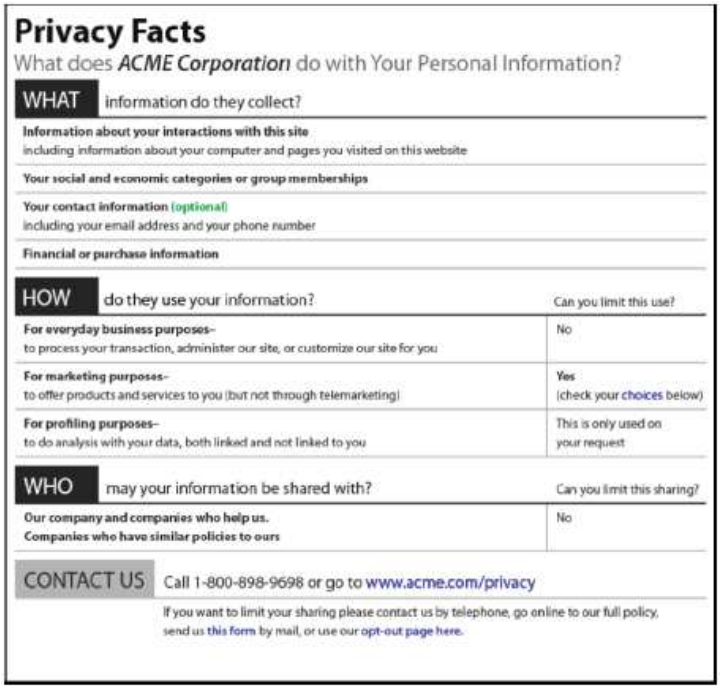

Figure 36: Example for Privacy Aware Wording, from [13]

Use When

This approach should be employed in applications with privacy and security related features, e.g., whenever the users are required to disclose personal information.

How

Before using the terms one should be sure that they are clear and understandable for the target-users. Therefore it is recommended to either refer to standardized terms that are currently only rarely available (c.f. [4], [9], [17]) or to conduct user tests on the understandability of these terms and phrases. These tests do not have to be extensive. Asking only few representative users from the target-group about their understanding of the terms should suffice.

Why

Studies have shown that difficult to pronounce names alert users [24]. These studies have so far only be conducted in the area of entertainment and food but according to different results obtained through user tests in PrimeLife (compare PrimeLife deliverable D4.1.1), these problems are also likely to apply to security and privacy interfaces.

According to the pattern "Privacy Policy Display" users need to be well informed in order to be able to make informed decisions. The information the user obtains has to be formulated understandably to form a basis for the user's decision.

Related Patterns

- Privacy Policy Display

2.4.4 Credential Selection (**)

(By KAU)

Problem

According to Art. 10 EU Directive 95/46/EC data subjects should at least be informed about what personal data are processed, by whom (i.e. the identity of the controller), and for what purposes when releasing personal data during actions such as login, registration, payments, etc. User tests have shown that user often overestimate the amount of personal data needed and hence processed during transactions and that this is due to flawed inferences from the mental model invoked by the UI.

Solution

Present the user with a selection mechanism that shows the user what possible choices are available and then show a summary page that contains the data to be sent. The UI should also clearly represent the chosen mental model. In both cases presented below the user is about to choose the credential issued by the Swedish road authority to prove her name.

Figure 37: Selection mechanism of card based mental model

Figure 38: Selection mechanism of issuer based mental model

Figure 39: Summary of selected information and meta-data that will be sent

Use when

This approach should be employed whenever the user is required to enter personal data such as login, credit card or other private information.

How

Independent of a mental model, the credential selection UI should contain two steps, namely, selection and summary. During the first step, all graphical elements of the selection mechanism should be based on the mental model. Thus, if working with the card based metaphor this should be apparent from the UI. During the second step, the invoked mental model is not as important as the key issue is to clearly convey which selected data and which meta-data is being sent.

Why

This approach should be used to make it easy for users to select the appropriate credentials. It also should inform them about which (personal) data and meta-data the recipient of the information will have after the transaction.

2.5 Descriptions of interactive PET Mock-ups

2.5.1 Trust Evaluation of Services Sides (****)

(By KAU)

Problem

Trust is an important prerequisite for individuals to use a system (e.g., e-commerce site or computer program) to its full potential [12]. However, usability tests of PRIME prototypes [17] have shown that there are problems to make people trust the claims about the privacy-enhancing features of privacy-enhancing system.

Trust plays a major role in PrimeLife because users do not only need to trust their own platforms to manage their data accordingly but also need to trust communication partners and their remote set of platforms that receives identity data to deal with these data appropriately.

Besides, PrimeLife also aims at enabling users to assess the trustworthiness of contents found on the Internet, particularly in cases where the information is provided by other users, such as in wikis. The emphasis of this entry will however be on trust evaluation of services sides.

Solution

A trust evaluation function can help to enhance the users' trust in PrimeLife and its back-end systems by communicating reliable information about trustworthiness and assurance (of providing the stated functionality) of communication partners. This trust evaluation function should display both information about the communication partner's trustworthiness in terms of privacy practices and of the reliability as a business partner as depicted in the Figure 40. Both will be important aspects for influencing the user's trust.

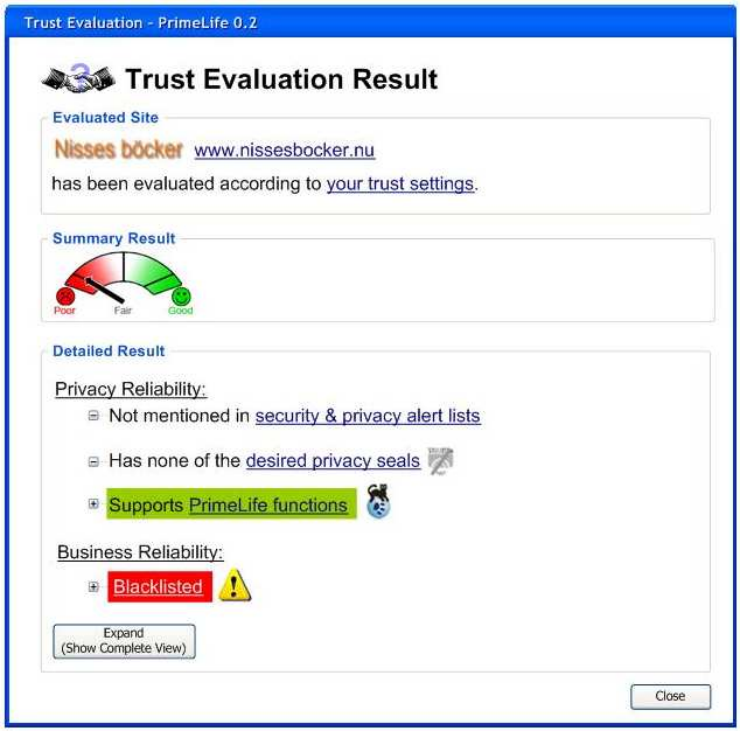

Figure 40: A mockup for Trust evaluation results

Use when

For allowing the user to do well-informed decisions, trust and assurance information needs to be presented to the user at least at the moment when he is requested to disclose personal data to a communication partner. The user interfaces for giving consent should therefore be augmented with a trust evaluation function to check the trustworthiness of communication partners (see "Send Personal data?" mockup under the pattern entry "Informed Consent"). Trust information can also be displayed when a side is contacted or when helpful in other contexts (e.g., for wiki entries, trust information about the creditability of authors could be displayed at the user interfaces that present these wiki entries).

How

A trust evaluation function should be based on suitable parameters for measuring the trustworthiness of communication partners and for establishing reliable trust. A model of social trust factors, which was developed by social science researchers in the PRIME project and which was summarised in [2], states that trust in a service provider can be established by monitoring and enforcing institutions, such as data protection commissioners, consumer organisations and certification bodies. Privacy seals certified by data protection commissioners or independent certifiers (e.g., the EuroPrise seal, the TRUSTe seal or the ULD Gütesiegel) therefore provide especially suitable information for establishing user trust. Such static seals can be complemented by dynamic seals conveying assurance information about the current security state of the system and its implemented privacy and security (PrimeLife) functions. Further information sources by independent trustworthy monitoring organisations that can measure the trustworthiness of services sides can be blacklists maintained by consumer organisations or privacy alert lists provided by data protection commissioners. The mockup shown above is based on those parameters. Also reputation metrics based on other users' rating can influence user trust. Reputation systems, such for instance the one in eBay, can however often be manipulated by reputation forging or poisoning. Besides, the calculated reputation values are often based on subjective ratings by non-experts, for who it might for instance be difficult to judge the privacy-friendliness of communication partners.

A trust evaluation function should in particular follow the following design principles:

- Use a multi-layered structure for displaying evaluation results, i.e. trust evaluation results should be displayed in increasing details on multiple layers in order to prevent an information overload for users not interested in the details or the evaluation.

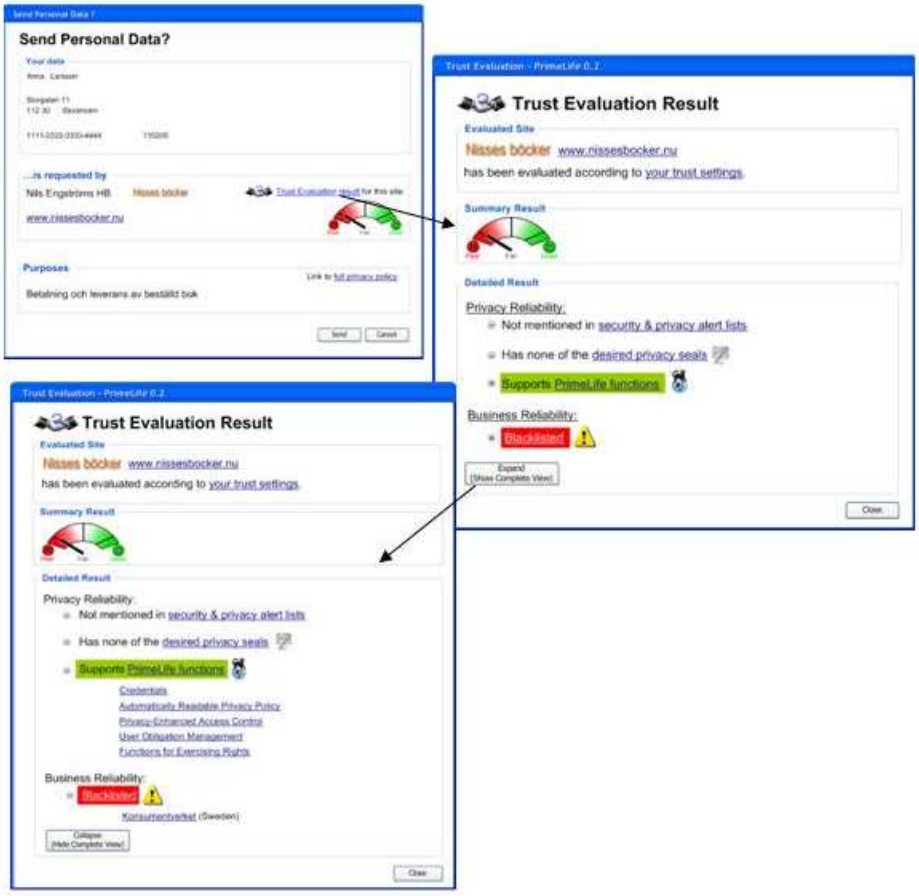

Figure 41: Display of trust evaluation results in multiple layers

- Make clear who is evaluated - this is especially important as previous usability tests have revealed that users have often difficulties to differentiate between user and services side [17]. Hence, the user interface should make clear by its structure and wording that the services side and not the user side is evaluated.
- Inform the user without unnecessary warnings - our previous usability tests showed that extensive warnings can be misleading and can even result in users losing their trust in the PrimeLife system. Therefore, for instances, cases where the evaluation of a site reveals that the site has no privacy seal and is not Prime enabled should not be displayed as a "negative" but rather a "neutral" results, as the majority of services sides today, including even the ones of privacy-friendly organisations, actually wont fulfil those requirements yet. Also, the yellow colour should be avoided for illustrating such "neutral" evaluation results (besides the use of the green colour for positive and the red colour for negative evaluation results), as yellow is already symbolising a state right before an alarm.
- Use a selection of meaningful overall evaluation results. For simplification, we suggest for instance to summarise the evaluation results into the three values "good", "fair" and "poor", which are displayed within a Trust Meter (see Figure 42). The following algorithm is used for calculating the overall results that are displayed:
    - A services side is rated as “fair”, if no positive (the services side has no privacy seals, no support of PrimeLife functions) and no negative (the services side does not appear on security & privacy alert lists or blacklists) evaluation results are reported (see Figure 42 a).

- A services side is rated as “poor” if it is either blacklisted or mentioned in security & privacy alert lists lists (independently on whether it has a privacy seal or is implementing PrimeLife functions).. If the services side is both blacklisted and appears on alert lists, the arrow of the trust meter points to the very left end of the meter (see Figure 42 b and c).
- A services side is rated as “good”, if nothing bad can be reported (i.e., the services side is neither blacklisted nor appearing on security & privacy alert lists) and something positive can be reported (meaning that the services side has been awarded a privacy seal or supports PrimeLife functions). If the services side is neither blacklisted nor does it appear on alert lists, and if it has a privacy seals and supports PrimeLife functions, the arrow of the trust meter points to the very right end of the meter (see Figure 42 d and e).

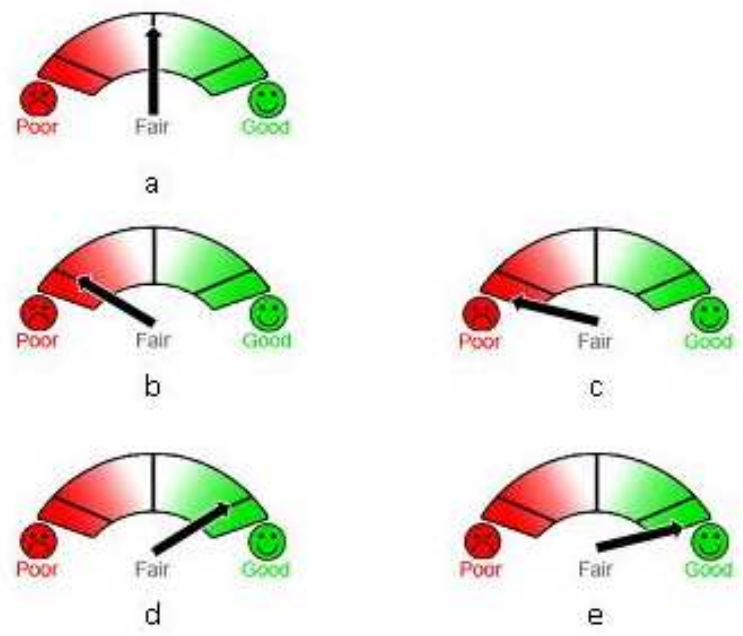

Figure 42: Trust Meters illustrating three different trust evaluation results

Why

Trust evaluation will allow users to establish reliable trust in communication partners and can warn users about non-trustworthy sides. First usability tests of trust evaluation mockups in Primelife (partly depicted above) have shown that such a function is much appreciated by end users. A PrimeLife-enabled system that provides a well-designed trust evaluation will also be more trusted to take the user's privacy interests seriously into account.

2.5.2 Data Track (***)

(By CURE, KAU)

Problem

Users leave every time when using the Internet personal data traces online. Users may lose an overview of what kind of data they disclosed to whom under which conditions, or in other words: who knows what about them and what happens with their data processed by others.

Solution

Provide a Data Track as an end user transparency tool, which is a history function providing the user with a detailed overview of all the user's personal data releases to communication partners. The Data Track also includes online functions allowing users to exercise their rights to access, correct and delete their data at services sides. The tool should store the released data over the whole lifetime of the user.

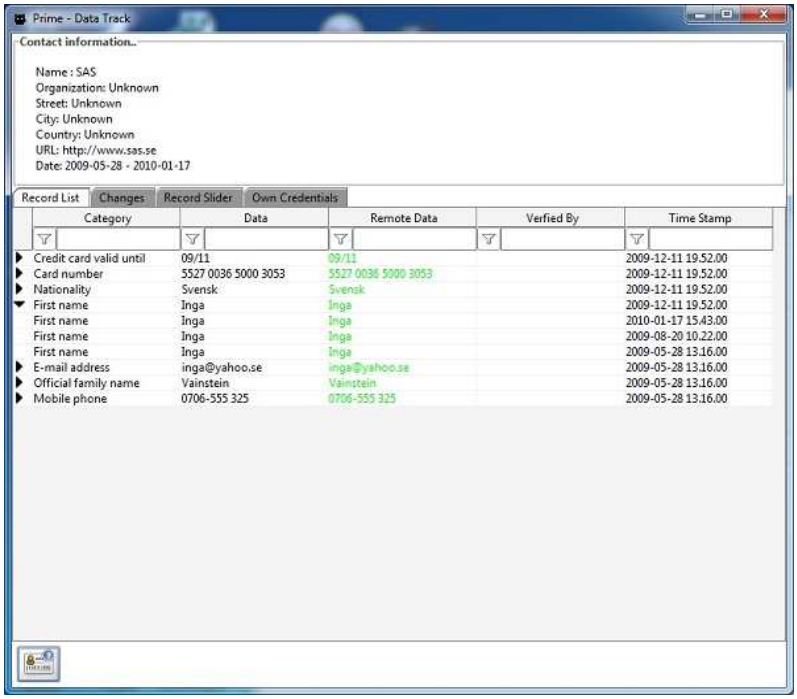

Figure 43: Summary of all data sent to a specific receiver and the data that is actually stored by the receiver (in green letters).

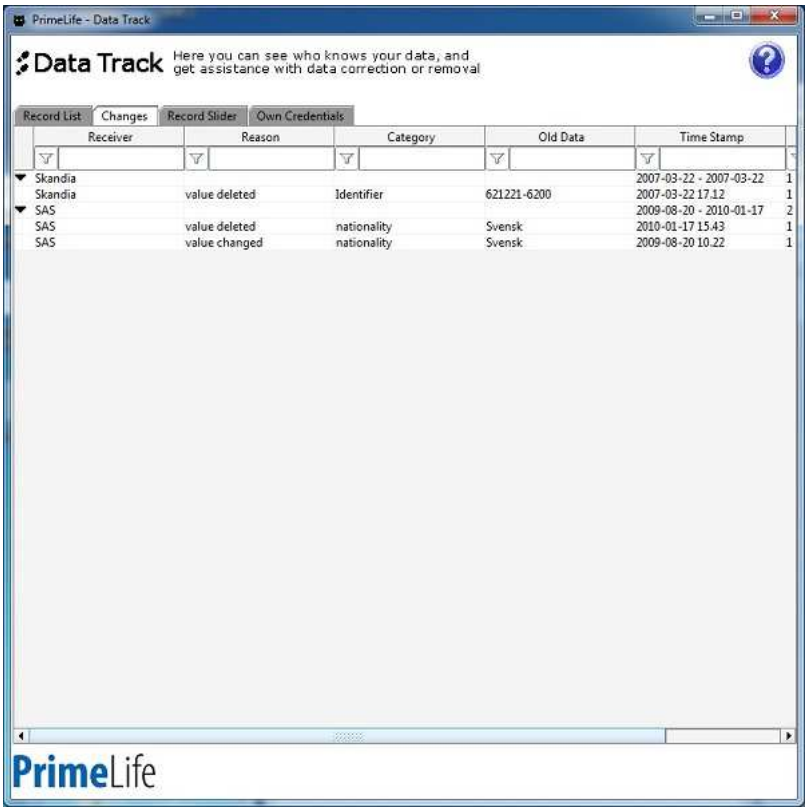

Figure 44: Summary of changes to remote data

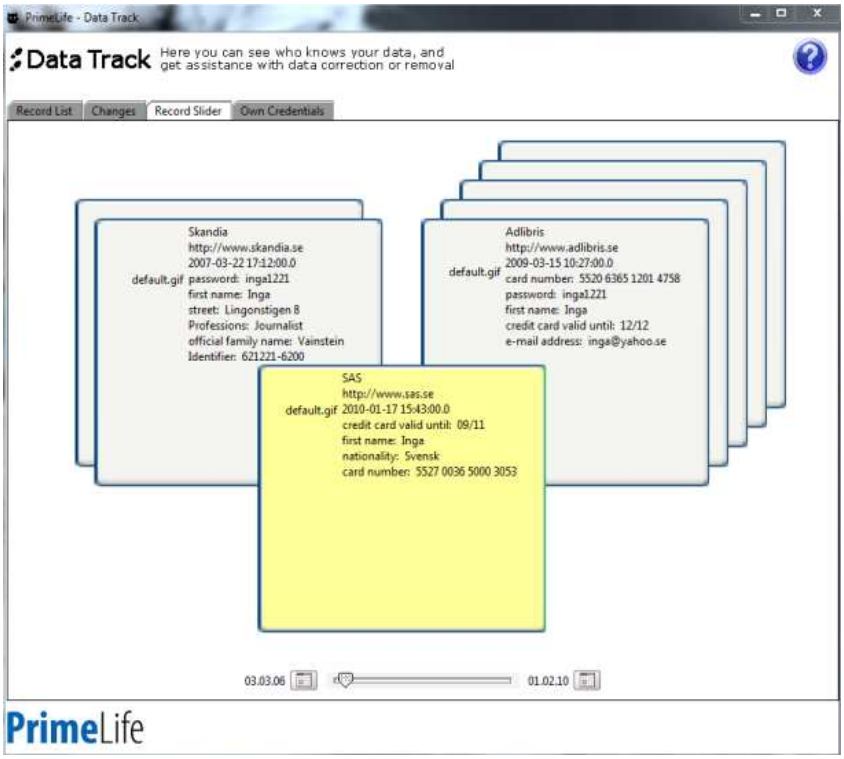

Figure 45: Record Slider of the Data Track

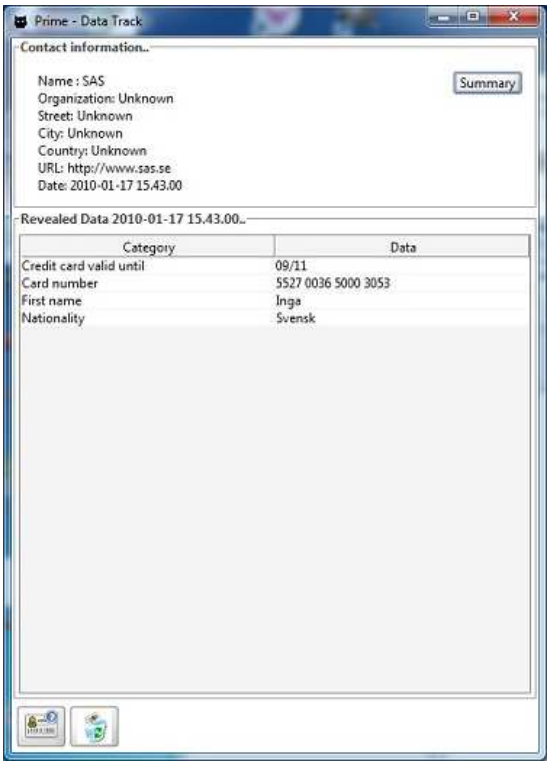

Figure 46: Summary of data send in one session

Figure 47: Summary of data sent in one session and the corresponding remotely stored data (in green)

Use when

The Data Track should be provided as a browser plugin or as a stand-alone tool. Every personal data release will trigger the storage of a Data Track record in the user's Data Track.

How

The Data Track function should store at the user's side all transaction records comprising personal data sent, pseudonyms used for transactions, credentials that were disclosed, date of transmission, purposes of data collection, recipient (i.e., the data controller) and all further details of the privacy policy that the user and recipient have agreed upon (Please note that in the Figure 42 to Figure 42 above, the detailed negotiated privacy policy is not stored yet in the Data Track records). Easy tools for finding relevant records about past data disclosures must be part of such a Data Track. The Data Track provides the user different views of the entries, the table-view and the interactive view. The Data Track offers also the possibility to search for websites in the user's transaction history, to show data releases that happened within a period of time and to correct or delete already released data directly online at remote services sides (as long as these services sides permit online access/correction/deletion). The Data Track stores a lifelong history of data that the user has released to other sites. So the user is able to reconstruct to whom she released which kind of data under which conditions.

Why

This transparency tool helps the user to recall where she posted which data, when and under which conditions. Transparency of personal data processing is regarded as a basic privacy principle, because a society, in which citizens could not know any longer who does, when, and in which situations know what about them, would be contradictory to the right of informational self-determination (as also the German Constitutional Court proclaimed in its Census Decision in 1983). Usability tests and studies on end user trust have also shown that users will put more trust in applications, if transactions are transparent and reversible, so that the users feel to keep somehow control over their personal data that they released [17] [14].

2.5.3 Privacy Options in Social Networks

(By CURE)

Problem

In social networks users have the possibility to provide data about themselves, but not all data should be visible to all users. To differentiate which user is allowed to see which data is very important for privacy, so the users should be able to control their visibility of information.

Solution

The solution for this problem is a selective access control for social networks.

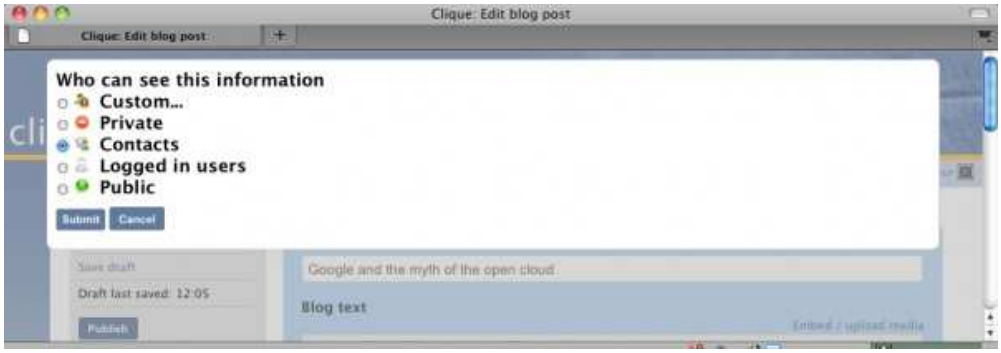

Figure 48: Selective Access Control

Figure 49: The own profile from the view of another user

Use when

This tool should be used in social networks to guarantee privacy.

How

Give users the possibility to create different social groups like family, friends, co-workers…

Another point is the possibility to create "pseudonyms" – this means that a user has one login with one address book and one administration screen but more than one identity inside the system.

If a user creates or modifies a message he should be asked each time for the privacy settings, e.g. just the social group "family" is allowed to read is post.

A selective access control gives users the possibility to choose in their privacy settings who can see which information.

Users should be also able to look at their own profile from the view of another user; this view helps users to maintain control over their audiences.

Why

The goal is, to give the user the possibility for individual privacy settings and guarantee higher privacy in social networks.

Related Patterns

- Privacy Awareness Panel in Collaborative Workspaces
- Privacy Enhanced Group Scheduling
- Selective Access Control in Forum Software

2.5.4 Selective Access Control in Forum Software (*)

(By CURE)

Problem

In current forums there is an imbalance between those who generate the content (users), which may include also personal data and those who control access to the contributions (administrators). Users have no influence on who is able to read their threads and posts in forums.

Solution

Provide users with the option to define the audience of their contributions by specifying the access rules to their own threads and posts in a forum. For instance, a user defines whether all people who provide any nick name should be able to read his/her thread or if access should only be granted to females who can proof to be younger than 26.

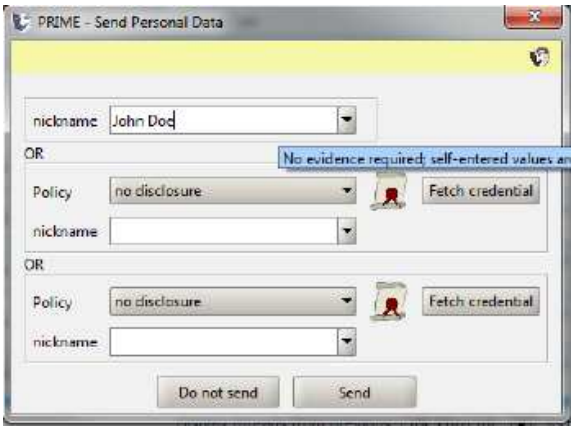

Figure 50: User has to choose a nickname before creating a thread

Figure 51: Show owner credential

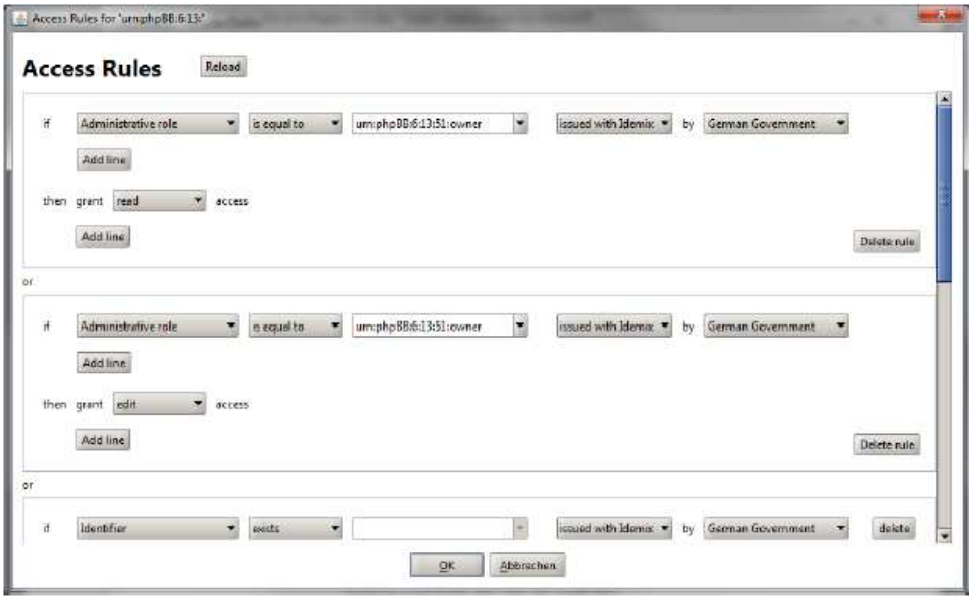

Figure 52: Access Rules editing window

Figure 53: Policy is editable for each thread and post

Use when

This approach should be implemented by all forum providers to increase the privacy of their users.

How

Users are able to create access control rules in which they can specify the access control policies for their threads or posts. Since in forums users are not necessarily known to each other by name, the access control specification is done based on certain provable properties (e.g., age, location). For example “if location is equal to ‘Dresden’ issued with Idemix by German Government” then “Grant read access” means that everybody who can proof with a credential issued by the German Government (ID card) that he/she lives in Dresden can read posts in this thread.

The creator of the thread should be able to change the access settings also afterwards.

Why

Users have the option to change the privacy settings of their own threads and posts that may contain personal data. So they can choose who should be able to see their threads or posts.

Related Patterns

- Privacy Awareness Panel in Collaborative Workspaces
- Privacy Options in Social Networks
- Privacy Enhanced Group Scheduling

2.5.5 Privacy Enhanced Group Scheduling

(By CURE, TUD)

Problem

Event schedulers, well-known from groupware and social software, typically share the problem that they disclose detailed "availability patterns" of their users.

These availability patterns often contain sensitive information in at least two respects.

- First, direct inference from the availability at a particular date may reveal information about one's private life (‘will my husband votes for the date of our wedding anniversary?’).
- Second, indirect inference arises from the fact that availability patterns contain much entropy and thus allow to (re-)identify individuals who would otherwise remain pseudonymous (‘The availability pattern of user bunny23 looks suspiciously like the one of my employee John Doe!’).

Solution

Create an application, which allows some event without revealing the availability pattern.

Three different parties may try to disclose private information of the users:

- the service provider,
- the other participants of a poll, and
- all other internet users.

In addition, sometimes one may have a special role of an event organizer, who initiates some event schedule.

In a maximum privacy-preserving application, no one of the three groups may learn anything about the availability patterns. To avoid, that an attacker simulates several participants, it is necessary, that users authenticate themselves (i.e., login).

A "decision rule", which decides about the chosen time slot for the event should be defined before a poll starts. As the most common decision rule seems to be the maximum of available users, a first solution may reveal only the sum of available participants at a certain time slot.

Figure 54: Dudle Poll with regular and anonymous voting

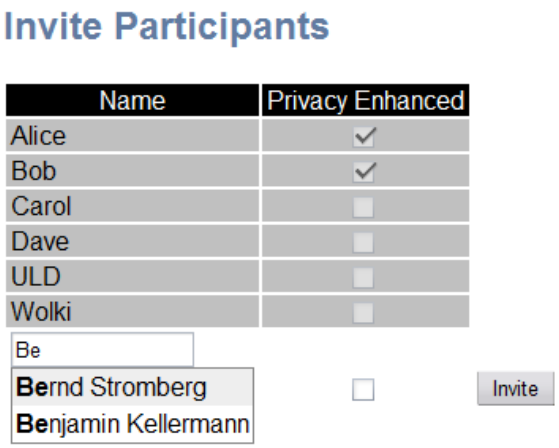

Figure 55: Dudle Window with auto completion for inviting participants

Use when

Such an application should be used every time, when it is not necessary to know the availabilities of each participant.

How

- The participants have to authenticate themselves via cryptographic methods. To adept a common pattern, a login before voting may be used. If they have no account it is necessary to create one, to create cryptographic keys.
- The initiator invites all participants via e-mail to the voting.
- All participants encrypt their availability pattern within their trusted device (browser).The cryptography should be hidden from the user, to ensure usability.
- After every participant send his encrypted availability pattern, some computation gives the necessary output for the decision rule.

Why

Demanding an authentication of the participants ensures a fixed anonymity set (i.e., no attacker should simulate other participants).

Secrecy of the availability patterns (i.e., votes) ensures freedom of choice (i.e., social pressure is avoided).

Related Patterns

- Privacy Awareness Panel in Collaborative Workspaces
- Privacy Options in Social Networks
- Selective Access Control in Forum Software

Chapter 3

Conclusions and Outlook

The HCI pattern collection presented in this Deliverable aims at providing HCI guidance to other PrimeLife activities, which are developing user interfaces for PrimeLife prototypes and tools. Our HCI pattern approach enables capturing, sharing and structuring user interface knowledge for PrimeLife.

The user interface artifacts (patterns and descriptions of interactive mockups) presented in this document are still under evaluation and re-design. We expect a further re-work of the interfaces after the next rounds of usability evaluations which are planned in 2010. The knowledge that we will gather from these evaluations will be continuously integrated into the document, which is available online for all PrimeLife project members within the PrimeLife internal Wiki. . We also expect new requirements coming up during the development of the policy management interfaces which will lead to new HCI patterns. Modifications and extensions to this document will be provided as an appendix to D4.1.5 Final HCI Research Report, which will be published at the end of the PrimeLife project.

Chapter 4

References

[1] Adams, A., Sasse, M. A. Users are not the enemy. In Comm. ACM, Vol. 42, No. 12, 1999.

[2] Andersson, C., Camenisch, J., Crane, S. Fischer-Hübner, S., Leenes, R., Pearson,.S., Pettersson, J.S., and Sommer, D.. Trust in PRIME. Proceedings of the 5th IEEE Int. Symposium on Signal Processing and IT, pages 18-21, 2005.

[3] Article 29 Data Protection Working Party. Opinion on More Harmonised Information provisions. 11987/04/EN WP 100, November 25 2004.

[4] Boyle, M. and Greenberg, S. 2005. The language of privacy: Learning from video media space analysis and design. ACM Trans. Comput.-Hum. Interact. 12, 2, pages 328-370, 2005.

[5] Conlan, R. M. and Tarasewich, P. 2006. Improving interface designs to help users choose better passwords. In CHI '06 Extended Abstracts on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). CHI '06. ACM, New York, NY, 652-657.

[6] Dhamija, R. and Dusseault, L. The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security and Privacy, vol. 6, no. 2, pages 24-29, 2008.

[7] Gehringer, E. Choosing Passwords: Security and Human Factors. ISTAS'02, pages 39-373, 2002.

[8] Hansen, M. Marrying Transparency Tools with User-Controlled Identity Management, In Proceedings of IFIP/FIDIS Summer School, 2007.

[9] Iachello, G. and Hong, J. End-user privacy in human-computer interaction. Found. Trends Hum.-Comput. Interact. 1, 1, pages 1-137. 2007.

[10] Jacob, F. 2008. Ästhetik und UX: Das Potential von Serious Motion Graphics, Xtopia 2008

[11] Jensen, C. and Potts, J., Privacy policies as decision-making tools: An Evaluation of online privacy notices, in CHI 2004, 6, pages 471-478, 2004.

[12] Johnston, J., J. H.P. Eloff & L. Labuschagne. Security and human computer interfaces. Computers & Security, Vol. 22 (8): pages 675-684, 2003.

[13] Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security (Mountain View, California, July 15 - 17, 2009). SOUPS '09. ACM, New York, NY, 1-12. DOI= http://doi.acm.org/10.1145/1572532.1572538

[14] Lacohée, H., Crane, S., Pippen, A.: Trustguide: Final Report, Oktober 2006.

[15] Mehldau, M. Iconset for Data-Privacy Declarations v0.1. http://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf. Accessed 2 December 2007.

[16] Patrick, A.S. & S. Kenny. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interaction. Privacy Enhancing Technologies Workshop (PET2003), Dresden/Germany, 2003.

[17] Pettersson, J.S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauß, S., Kriegelstein, Th. & Krasemann, H. Making PRIME usable. SOUPS 2005 Symposium on Usable Privacy and Security, Carnegie Mellon University, July 6-8 July, 2005, Pittsburgh. Available in ACM Digital Library.

[18] Pettersson, J.S. HCI Guidance. PRIME Deliverable D06.1.f. 1 February 2008.

[19] PGP Corporation's PGP Desktop. Available at: http://tinyurl.com/8fh38.

[20] Protor, R., Ali, A., Vu, K.-P. L., Information requested by Web Sites and User's comprehension of Privacy Policies, Poster Proceedings of the Symposium of Usable Privacy and Security (SOUPS 2006), July 14-16, 2006, Pittsburgh, PA.

[21] Raskin, J. The Humane Interface – New Directions for Designing Interactive Systems. ACM Press, New York, 2000.

[22] Rundle, M. International Data Protection and Digital Identity Management Tools. Presentation at Internet Governance Forum 2006, October 2006, Athens. http://identityproject.lse.ac.uk/mary.pdf. Accessed 2 December 2007.

[23] Sasse, M.A., Brostoff, S., and Weirich, D. Transforming the 'weakest link': a human-computer interaction approach to usable and effective security. BT Technical Journal, Vol 19 (3), pages 122-131, 2001.

[24] Song et al. If It's Difficult to Pronounce, It Must Be Risky. Psychological Science, 20 (2): page 135. 2009.

[25] Yan, J., et al. The Memorability and Security of Passwords – Some Empirical Results. IEEE Security & Privacy Magazine, Vol. 2, Issue 5, pages 24-31, 2004.