A Pattern Collection for Privacy Enhancing Technology

Cornelia Graf[1], Peter Wolkerstorfer[1], Arjan Geven[1], Manfred Tscheligi[1,2]

(1) CURE
Center for Usability Research & Engineering
Modecenterstraße 17 / 2
1110 Vienna
+43.1.743 54 51
{last name}@cure.at

(2) ICT&S Center
University of Salzburg
Sigmund-Haffner Gasse 18
5020 Salzburg
+43.662.8044.4811
manfred.tscheligi@sbg.ac.at

Abstract— **Patterns are a useful approach to describe, organize and present solutions and best practices for design problems. Although much work can be found concerning either patterns or privacy, work focusing on patterns for Privacy Enhancing Technologies (PET) is very rare. This paper describes the development of User Interfaces Patterns for PET and the benefit of using them. We used different proven approaches and guidelines and merged them for creating efficient and useable patterns for PETs. Anyhow, some of our patterns were not tested much with end-users, so further tests will be necessary to prove worth of the patterns. Nevertheless we maintain that our patterns will support the development of PET UIs. In this paper, we provide a short overview of the whole pattern collection and present two patterns in detail.**

Keywords*- patterns; privacy; user interfaces desing; privacy enhancing technologies; pattern development; pattern approach.***

I. Introduction

Patterns provide solutions that have been successfully used for many years for specific problems. This paper describes the development of patterns for different User Interfaces (UI) for PETs and presents two of them more detailed. In current literature, patterns for PETs are very rare; approaches concerning patterns for privacy enhancing technologies are presented by [6], [10], [15], [16], [17] and [18].

The usage of PETs for privacy protection is a very important aspect for users' online life. Therefore, the lack of patterns concerning UIs for PETs is a big deficiency, for developers and designers as well as end-users. To help designers and programmers when dealing with the creation of UIs for privacy enhancing technologies we developed twelve patterns for PETs.

In the following Section, we will give an overview about the current research in the field of privacy patterns. Section III presents the development of our patterns approach and gives an overview of the PET patterns. In Section IV, we describe two of them in detail. In the last Section, we will discuss our approaches and give an overview about our future research.

II. Related Work

In literature, much work can be found concerning either privacy or patterns but our literature research showed a lack of work concerning patterns for PETs.

Goldberg [3], [4] and Goldberg et al. [5] presented an overview about currently existing privacy enhancing technologies and gave an outlook of future PETs. Schumacher [17] presented two patterns, one deals with protection against cookies and the other one with pseudonymous mailing.

Schümmer [18] pointed out another privacy pattern approach, which covers the filtering of personal information in collaborative systems. These patterns address how to protect personal data from transmission to others and how to filter information received from others.

Other research concentrated on privacy protection and anonymity. Hafiz [6] presented a collection of privacy design patterns, which addresses anonymity solutions for various domains. Romanosky [15] developed three patterns, which describe how users can protect their privacy in web-based activities.

Another topic concerns patterns, which are related to privacy policies. Sadicoff [16] introduced a pattern especially for affording user awareness for privacy policies of network sites. The approach of Lobato [10] dealt with the development of user-friendly privacy policies.

In this paper, we present some patterns we created to support designers and developers when working on the development of UIs for PETs.

III. PET Patterns

Since the observing of privacy should be one main goal in users' online behavior, it is necessary to provide PETs for supporting them. Our current work deals with the development of different user interfaces for privacy enhancing technologies. As patterns provide useful and proven approaches for design problems we decided to use them for the development of our PET UIs. However, while we looked for patterns and proven approaches we concluded that only few patterns for privacy enhancing technologies are available and that they were not adaptive for our requirements. Hence, we decided to work not only on UIs for PETs but furthermore on development of patterns for assisting future PET developers.

The main requirement was to develop PET-UIs, which present the complex techniques of PETs in an understandable way to end-users. Another important requirement was to support users to protect their privacy in an active way. To achieve this we worked on solutions to make users aware of privacy related topics in web, like private data are requested, and so on. The online life of users can include many different use-cases of the Web; to cover all this use-cases with PETs it was necessary to develop several patterns for different tasks, i.e., support when creating a password, displaying if the privacy policy of a website matches with the preferred privacy settings and so on. Furthermore, we developed basic approaches for supporting users' privacy-behavior in the Web in privacy related way, i.e., information about visible private data in collaborative workspaces.

Our pattern approach should support the usage of best practice solutions for defined PET problems. Furthermore, they shall assist designers and developers as a guideline when creating UIs. This shall guarantee usable and consistent UIs in PET software. It should also enable capturing sharing and structuring of PET development knowledge inside the project team.

A. Pattern Development

Since we did not find feasible patterns for the needs of our UIs, we developed patterns by ourselves. A crucial factor when developing patterns is that each pattern must be consistent with the other patterns. The reason for this need for consistency is that a pattern describes not only a solution for a special problem but furthermore a solution for a special problem in a domain [8]. This means all patterns must veer toward the same purpose; - in our case, all patterns have to support the creation of user interfaces for PETs. Additionally, patterns are not allowed to contradict other patterns in the same domain. To create patterns, which complement one another in a meaningful way, we created our patterns during an iterative design process, which starts with the definition of the problem each pattern shall solve.

As a next step, we looked for approaches in literature and if guidelines on how to handle this problem already exist. We also integrated the knowledge, the experience and results which we gather in a predecessor project into the PET Patterns (e.g., [12]). This knowledge contains e.g., the observation that users try to get rid of intrusive privacy warnings by changing to more "generous" privacy preference settings.

Another point of interest were different guidelines of the European Union (EU) which describe privacy related concerns or approaches for supporting user perception of information ([2] e.g., Art. 25, Art. 7a, Art. 29 "Working Party") – these guidelines are commonly known as "European Data Protection Directive (DPD)".

Finally yet importantly, we looked for already proven approaches for our defined problems and adapted or merged them to create useable solutions. The most important approaches for the development of our patterns were:

- The multi-layered presentation approach, which is presented in Art. 29 Working Party [2]. This article 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.
- Dynamic tooltips, which are based on the idea of motion design [7]. In motion design motion graphic are used for supporting the interactive system.
- An adaption of the "nutrition label for privacy" presented by Kelley [9]. Kelley adapted the nutrition label from the food domain and used it for displaying privacy policies to user.
- In addition, we also applied to the approach of Patrick [11], which lists four categories of human factors requirements for privacy interface design.

During the development, we combine guidelines and already proven approaches from the HCI. This grants already proven methods for the presented PET patterns.

For example, we used the multi-layered presentation approach and merged it with dynamic tooltips to inform users that private information is required. The "Dynamic Privacy Policy Display" which bases on this approach will be presented in Subsection IV.A.

Furthermore, we customized the "nutrition label for privacy" for a policy matching display. This display shall show users if and how much their preferred privacy settings matches with the policy of a website.

Experts first evaluated the outcomes of this merging through heuristic evaluation methods. Within this evaluation, they reviewed the outcomes based on classical usability principles. If this expert based analysis supports the design of the patterns we started with the next step – the end-user testing, otherwise we reworked the patterns. The goal of the end-user testing is, to look if the presented UI solutions of our patterns are understandable for end-users.

The end-user testing was done in several steps. If any problems were uncovered, we adjusted the pattern. This end-user testing is not completed yet, it will be continued in the further design of the patterns.

The goal of the patterns is to present complex technical PET mechanisms in an understandable way for users. The patterns will help designers and developers to create usable and supportive interfaces for PETs. For better usability of the patterns for designers and programmers we grouped the patterns, this shall provide a more efficient search for patterns for a special problem.

We classified our patterns through affinity diagramming [1] to grant designers and developers an efficient way to look through the patterns for solutions for PET concerning problems. The idea of grouping patterns can be also found at e.g., Welie [20] and Tidwell [19].

We didn't have categories in the beginning of the affinity diagramming; instead we analyzed the content and theme of each pattern and put related/similar patterns next to each other. In the end, we get three groups, which we named after the topic the patterns addresses.

Group 1: "PET Interaction" contains patterns, which are related to workflows and interaction paradigms.

Group 2: "PET patterns for privacy policies" includes patterns concerning the displaying of privacy policies.

Group 3: "PET Visualization" is related to the depiction of privacy information and to icons, which shall support a better visualization.

B. Patterns Structure

We based our patterns on the structure used by Welie [20] and extended it by a star rating, which illustrates the number of end-user testing we did with the pattern. Each Pattern consists of the following elements:

Title: The Name of the Pattern
Rating: A 0 to 5 star rating. It shows how much end-user tests were done.

- *Zero stars* mean that there weren't any end-user tests done with it.
- *One star* mean that low level HCI knowledge is 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.

  In Section IV, we will present two patterns with 4-stars rating.
- *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: Summarizes and outlines the existing problem.
Solution: Brief description of the solution.
Use when: This group outlines the situation the pattern is best applied in.
How: More detailed insight into the solution
Why: Presents why the solution is needed and how to the user benefits from it.
Related Patterns: Refers to other patterns similar to the presented one.

From our point of view, this structure displays patterns in a plain way even for persons who never worked with patterns before and the appending of the star rating provides a first glance impression of how much end-user testing was done.

C. Overview of PET-Patterns

We developed twelve patterns for PET. Although all patterns are related to privacy, they can be clustered into different subgroups as described above.

In the following, we will give an overview of the three groups and the patterns related to them.

1) PET Intercation

The patterns in this group are related to workflows and interaction paradigms in PETs. This group has to offer elements, which can and shall be used in PETs to inform user about different topics concerning the approval of his data in the web. Patterns for following topics are attributed to PET Interactions:

a) Secure Passwords (****)

Secure passwords are a main concern for personal privacy protection.

This approach should help users to create and choose secure passwords by giving appropriate and dynamic feedback.

b) Informed Consent (****)

Users should fully understand what will happen if they release personal data in the web.

This UI solution should be used every time when the user needs to disclose personal data.

c) Privacy Aware Wording ( )

Users shall clearly understand the content and the terms of privacy policies. This approach should be used every time when a privacy policy will be displayed to a user.

d) Credential Selection (**)

This pattern should be used to make it easy for a user to select the appropriate credential and to inform him which data will the recipient have after the transmission.

2) PET Patterns for Privacy Policies

The patterns in this group are related to workflows and interaction paradigms in PETs. This group has to offer elements, which can and shall be used in PETs to inform user about different topics concerning the approval of his data in the web.

Following patterns can be found in this group:

a) Privacy Policy Display (***)

The goal of this display is to provide the user information about why what information by whom is requested.

It should be used whenever personal data are required from the user.

b) Dynamic Privacy Policy Display (****)

This pattern is presented in Section IV.

Display a tooltip to the user when his attention is required for privacy matters, e.g., person data are requested by a website.

c) Policy Matching Display (**)

Provide the user a possibility to compare each privacy policy with his preferred privacy settings. This approach should be used when a user contacts a service side or when the entry of personal data is required.

3) PET Visualization

PET Visualization offers suggestions on how to display privacy-related topics like "who sees which data" to the user.

The patterns in this group shall help designers to present this "who sees which data"-topic in an understandable way to users.

This group contains following patterns:

a) Privacy Icons (*)

Icons are able to speak for themselves, so icons are a great solution to aid written text. These icons should be used

ISBN: 978-1-61208-111-3

for PET software to support the user when he reads privacy information.

b) Icons for Privacy Policies ( )

Icons are able to speak for themselves, so icons are a great solution to support a user when he reads a privacy policy. These icons should be used together with privacy policies.

c) Privacy Awareness Panel in Collaborative Workspace (****)

This pattern is presented in Section IV.

The developed privacy panel shall users make aware of data (like IP or location) which are visible to others in a collaborative workspace. It should be used by collaborative workspace providers to help user protecting their privacy.

In the previous Section, we presented our patterns collection. The offered patterns cover various aspects of users' life. Through expert evaluation and previously done end-user tests, the patterns prove their worth for PET development. Furthermore, the multi-stage user tests showed that our solutions are understood by end-users. Therefore, we were able to fulfill our main requirement, an understandable presentation of the complex techniques of PETs to end-users. The second requirement was making users aware of privacy related topics. This requirement is integrated in different patterns, like "Secure Password" or "Policy Matching Display".

IV. Presentation of Selected Patterns

In the following Section, we will explain two selected patterns. First the "Dynamic Privacy Policy Display", which shall attract users' attention when needed, e.g., when private data are required; the second deals with an information panel for private data displaying in collaborative workspaces, it is called "Privacy Awareness Panel in Collaborative Workspaces".

We decided to present these two patterns because both are currently rated with four stars. This means that the patterns are still in draft state but only the final iteration round with end-users is missing. We think that these two patterns are good examples for the PET-Patterns we developed.

The presented patterns shall support user when login, reading and working on the web.

In accordance with Article 25 EU Directive 95/46/EC [2] individuals need to be informed about which of their data are processed, who is processing them and why. Therefore, it is necessary to inform users in an understandable way about what happened to their data and suggest possible consequences to them.

A. Dynamic Privacy Policy Display (****)

Problem

Users need to be well informed about possible consequences when releasing personal data upon certain actions such as login, registration, payments, etc. Art. 25 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 [2].

Solution

The multi-layered presentation approach by the Article 29 Working Party [2] can be implemented by dynamical information "tooltips" informing the user about the nature of the data disclosed and possible consequences. The dynamic information need to be adapted to the context of the website it is used in. It should only include relevant security and privacy information and have a unique standard layout making it easy to recognize.

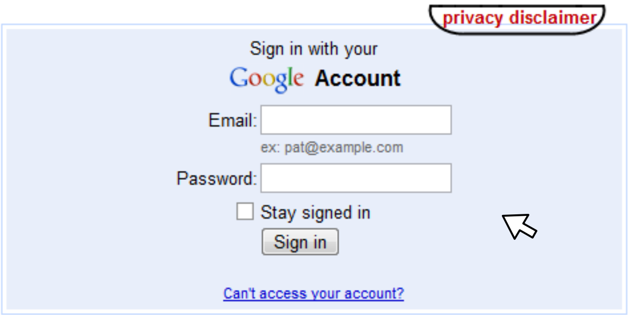

Figure 1: Prototype for Dynamic Display of Information

Figure 1 shows a prototype for dynamic display of information. When the mouse is moved nearby the interface, the privacy disclaimer in the top appears on the login-interface. 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.

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 (cf. Figure 1). 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; thereby motion graphics are used as functional elements in interactive systems. According to Jacob [7], 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).

Research we did on the displaying of privacy preferences has shown that users recognize dynamic privacy policy display interfaces much better than static privacy policy displays. So 100% of our participants indicated to having recognized the dynamic box (visible in Figure 1), on the other hand, only 43% noticed a static display.

Related Patterns

- Privacy Policy Display

B. Privacy Awareness Panel in Collaborative Workspaces (****)

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 nicknames instead of using their real names, which leads to a higher perceived anonymity of the users. However, providers of collaborative workspaces have more information about a user's real identity (e.g., IP address). Secondly, 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. Both harm the person's privacy, even if the person is unaware of this.

Solution

In a so-called privacy-awareness panel, the audience is made transparent to the user, i.e., who can access his/her contribution (all internet users, registered users …). 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.

Use when

The approach should be used with every collaborative workspace.

How

First, it should be made clear to users which persons will be 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.

Further information about the Privacy Awareness Panel can be found in Poetzsch et al. [13].

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

In the preceding Section, we presented two selected PET patterns from our collection.

The first presented pattern should be used every time when it is necessary to catch user's attention, e.g., when a user might oversee the privacy indications.

The second one, the privacy awareness panel, should be applied in every collaborative workspace to inform users which of their private data are visible to whom e.g., the provider.

Through implementation of these approaches, users will be better informed about what will happen to their private data and therefore be able to make informed decisions when dealing with their private data in web.

We advise that these approaches should be used every time to support users in making privacy aware decisions, although the patterns misses the final iteration round they prove their value during tests with end-users.

V. Conclusion and Future Work

In this paper, we have presented the development of UI patterns for privacy enhancing technologies. Furthermore, we have given an overview of the developed PET patterns and presented two of them in detail.

All the patterns in our collection have the same goal, helping designers and developers of PETs creating useable and understandable interfaces for end-users.

The merging of best practice solutions from HCI and different guidelines permitted us creating patterns for PETs with already proven solutions. Furthermore, the iterative development approves permanently improvements of the patterns. In a first step, experts evaluated each pattern and detected usability problems were remodeled.

Through end-user tests, we are able to identify user's problems of the different patterns and can therefore fix the uncovered usability problems in further version of the pattern. Furthermore, the patterns were rated with a star rating, which shows how much end-user testing has been done with each pattern. End-user testing has already been carried out with most of the pattern; only two have not yet been evaluated with end users. Four patterns are currently rated with four stars, so there is just the final iteration missing. However, for all patterns of our collection further user evaluations will be necessary.

Yet, results of end-user tests we made till now showed that we are able to fulfill our main requirement, the development of an understandable presentation of PETs for end-users. Anyhow, we maintain that the usage of our pattern collection for development of UIs for PETs will support users when dealing with private data in the web.

Future research will contain further usability testing of our presented patterns and based on the results of the tests a reworking and expansion of the UIs and patterns will be needed. The knowledge we gather from these evaluations will be continuously integrated into our existing patterns but it will also be necessary to create new patterns for new requirements.

The complete pattern collection can be found at [14].

ACKNOWLEDGMENT

Thanks to our PrimeLife partners for support, help and input while creating the patterns.

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.

REFERENCES

[1] H. Beyer. and K. Holtzblatt, “Contextual design: Defining customer-centered systems”. San Francisco, CA: Morgan Kaufmann, 1998.

[2] European Parliament, “Directive 95/46/EC of the European Parliament” , 1995. available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML; Last accessed : 2010-08-09

[3] I. Goldberg. “Privacy-enhancing Technologies for the Internet, II: Five Years Later”. In Workshop on Privacy Enhancing Technologies 2002, Lecture Notes in Computer Science 2482, pp. 1–12.

[4] I. Goldberg, “Privacy Enhancing Technologies for the Internet III: Ten Years Later”. In Acquisti A., Gritzalis S., Lambrinoudakis C., di Vimercati S. D. C. (eds.) Digital Privacy: Theory, Technologies, and Practices, Chapter 1. Auerbach, 2007.

[5] I. Goldberg, D. Wagner, and E. A. Brewer, “Privacy Enhancing Technologies for the Internet”. In COMPCON '97, pp. 103–109, February 1997.

[6] M. Hafiz, “A collection of privacy design patterns”. In Proc.of the 2006 Conference on Pattern Languages of Programs. PLoP '06. pp. 1-13.

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

[8] D. Khazanchi, J.Murphy, and S. Petter , “Guidelines for evaluating patterns in the IS domain”. MWAIS 2008 Proc., Paper 24. http://aisel.aisnet.org/mwais2008/24; Last accessed : 2010-08-09

[9] P. G. Kelley, J. Bresee, L. F. Cranorand and R.W. Reeder, “A "nutrition label" for privacy”. In Proc.of the 5th Symposium on Usable Privacy and Security (SOUPS '09). pp. 1-12.

[10] L. L. Lobato and E. B. Fernandez, “Patterns to Support the Development of Privacy Policies”. First International Workshop on Organizational Security Aspects 2009 , pp.744-749

[11] A.S. Patrick and S. Kenny, “From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interaction”. Privacy Enhancing Technologies Workshop (PET 2003), Dresden/Germany, 2003, pp 107-124.

[12] J.S. Pettersson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, S. Clauß, Th. Kriegelstein, and H. Krasemann, “Making PRIME usable”. In Proc. of the 2005 Symposium on Usable Privacy and Security (SOUPS '05), vol. 93. pp. 53-64.

[13] S. Pötzsch, P.Wolkerstorfer and C. Graf. Privacy-Awareness Information for Web Forums: Results from an Empirical Study. NordiCHI 2010, 16.–20. October 2010, Reykjavik.

[14] PrimeLife Project, http://www.primelife.eu; Last accessed : 2010-08-09

[15] S. Romanosky, A. Acquisti, J. Hong, L. F. Cranor, and B. Friedman, “Privacy patterns for online interactions”. In Proc.of the 2006 Conference on Pattern Languages of Programs (PLoP '06). pp. 1-9.

[16] M. Sadicoff , M.M. Larrando-Petrie, and E.B. Fernandez, “Privacy aware network-client pattern”. In Proc. of the 12th Conference on Patterns Language of Programming (PLoP’05), 2005. Available at: http://hillside.net/plop/2005/proceedings/PLoP2005_msadicoff0_0.pdf. Last accessed: 2010-08-09

[17] M. Schumacher, “Security patterns and security standards - with selected security patterns for anonymity and privacy”. In Proc. of the European Conference on Patterns Language of Programming (EuroPLoP'02), 2002. http://citeseer.ist.psu.edu/schumacher03security.html. Last accessed : 2010-08-09

[18] T. Schümmer, "The Public Privacy -- Patterns for Filtering Personal Information in Collaborative Systems," In Proc. of the Conference on Human Factors in Computing Systems (CHI ‘04) 2004. Available at: http://www.pi6.fernuni-hagen.de/publ/CHI2004.pdf; Last accessed: 2010-08-09

[19] J. Tidwell, “Designing interfaces.” - Sebastopol, Calif. [u.a.] : O'Reilly 2005.

[20] M.v. Welie, “Patterns in Interaction Design”. Available at: http://www.welie.com/patterns/index.php; Last accessed : 2010-08-09