Advances in Engineering Software 40 (2009) 1231–1241

Contents lists available at ScienceDirect

Advances in Engineering Software

journal homepage: www.elsevier.com/locate/advengsoft

A methodology for designing information security feedback based on User Interface Patterns

Jaime Muñoz-Arteaga [a,*], Ricardo Mendoza González [a], Miguel Vargas Martin [b], Jean Vanderdonckt [c], Francisco Álvarez-Rodríguez [a]

[a] Universidad Autónoma de Aguascalientes, Centro de Ciencias Básicas, Av. Universidad 940, 20100 Ciudad, Universitaria Aguascalientes, Mexico
[b] University of Ontario Institute of Technology, 2000 Simcoe St. N. Oshawa, Canada L1H7K4
[c] Université Catholique de Louvain, Belgian Lab. of Computer-Human Interaction (BCHI) Place des Doyens, 1 – B-1348 Louvain-la-Neuve, Belgium

ARTICLE INFO

Article history:
Received 22 September 2008
Received in revised form 19 November 2008
Accepted 19 January 2009
Available online 14 April 2009

Keywords:
Design patterns
Heuristic evaluation
Security information feedback
Trust
Usability
User-centered design
User Interface Patterns

ABSTRACT

A methodology is provided here to assist in the design of secure interactive applications. In particular, this methodology helps design an adequate security information feedback based on User Interface Patterns, the resulting feedback is then evaluated against a set of design/evaluation criteria called Human–Computer Interaction for Security (HCI-S). In case of a security issue the security information feedback is generally presented using the visual and auditory channels required to achieve an effective notifications, and it is explicitly specified in the design of user interfaces for secure web system.

1. Introduction

The term "user feedback" is often referred to as any form of communication from a system towards the user. Similarly, information security feedback is any information related to the system's security conveyed to the end user. This information must to be shown in an adequate manner to the final user. A good alternative to generating a well-designed information security feedback consists of applying design patterns, because it is well known that a pattern represents a proven solution for a recurrent problem within a certain environment. From a computer science perspective, Human–Computer Interaction (HCI) deals with the interaction between one or more users and one or more computers using the User Interface (UI) of a program [17]. The concepts of traditional HCI can be used to design the interface or improve an existing one, considering aspects such as usability. Usability determines the ease of use of a specific technology, the level of effectiveness of the technology according to the user's needs, and the satisfaction of the user with the results obtained by using a specific technology to perform specific tasks.

Security HCI (HCI-S) has been introduced [19] to reflect the need to explicitly support security in the UI development life cycle. The concept of HCI-S modifies and adapts the concepts of the traditional HCI to focus in aspects of security and to find out how to improve security through the elements of the interface. We use the HCI-S definition proposed by Johnston et al. [19] which textually reads "The part of a UI which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security". According to [19], HCI-S deals with how the security features of the UI can be as friendly and intuitive as possible, because the easier a system is to use, the less likely is that the user will make a mistake or try to bypass the security feature, resulting in a more reliable system.

Our contribution consists of a set of design patterns to design usable information security feedback combining the concept of User Interface Patterns and HCI-S criteria. We create a basic model to exemplify the presentation of information security feedback to the end user when a threat is detected. Our model is divided into three stages (Fig. 1): first, an additional notification form is triggered to notify the end user about some security threat, possibly enhanced with auditive notifications or any other kind of feedback.

* Corresponding author.
E-mail addresses: jmunozar@correo.uaa.mx (J. Muñoz-Arteaga), mendozagric@yahoo.com.mx (R.M. González), miguel.vargasmartin@uoit.ca (M.V. Martin), jean.vanderdonckt@uclouvain.be (J. Vanderdonckt), fjalvar@correo.uaa.mx (F. Álvarez-Rodríguez).

0965-9978/$ - see front matter
doi:10.1016/j.advengsoft.2009.01.024

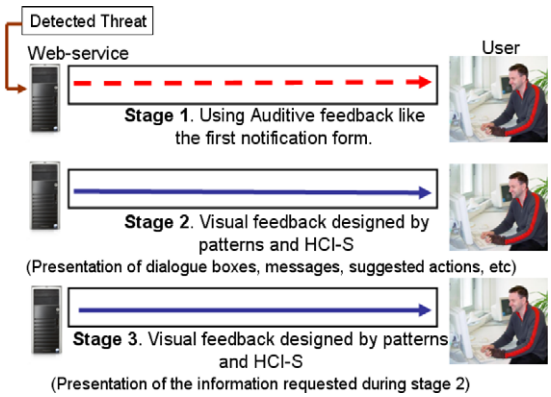

Fig. 1. The three steps of the method for feedback when a threat is detected.

Then, the visual feedback is effectively designed based on the design patterns that are explicitly based on HCI-S criteria. Finally, the feedback is constructed.

Combining visual and auditive channels in an alert benefits from the following advantages [16]:

- A sound may be more interruptive than other types of alerts, this combined with some specific colors and images may represent a very good way to notify users about some threat or error detected, and permits an efficient sensorial correlation.
- Auditive feedback, in theory, should permit to assign a specific sound to a specific threat.
- A particular sound may be identified by the users in a set of auditive alarms.

So far, the importance of integrating security and usability in the UI development life cycle has been widely recognized [3,15,19] both from the user studies point of view [8,18,28] and the usability challenges posed by this integration [27]. Despite this recognition, there is little or no attempt to integrate those two factors into a single design method. Some guidelines, recommendations, and best practices exist [3,10,13,28], but their effective integration remains the designer's responsibility.

In order to address this shortcoming, this paper introduces a method for designing visual and auditive user feedback based on design patterns. The remaining of this paper is organized as follows. Section 2 explains the HCI-S design/evaluation criteria. Section 3 describes the general problem within the framework of our research work. Section 4 defines the steps of the method for designing information security feedback that is then applied in a laboratory study in Section 5. Section 6 compares this work with respect to other relevant and related works. Finally, Section 7 summarizes our concluding remarks and provides some potential avenues for future work.

2. HCI-S design criteria

To achieve a successful application of the HCI-S's concepts, it is necessary to consider the design criteria proposed by Johnston et al. [19]. These criteria facilitate developing usable interfaces that are used in a security environment, based on Nielsen's heuristics traditionally used for heuristic evaluation [26]:

- **Visibility of system status**: The UI must inform the user about the internal state of the system (e.g., using messages to indicate that a security feature is active, etc.). The warning or error messages must be detailed but specific including a suggested corrective action for some security problem, and links to obtain additional information or external assistance.
- **Aesthetic and minimalist design**: Only relevant security information should be displayed. The user must not be saturated with information and options, and the UI must avoid the use of technical terms as much as possible. The security UI must be simple and easy to use, maintaining a minimalist design.
- **Satisfaction**: The security activities must be easy to realize and understand. Without the use of technical terms in the information showed to the user, in some cases, it is convenient to use humor situations or figures to present important security concepts to the user in an entertaining manner.
- **Convey features**: The UI needs to convey the available security features to the user clearly and appropriately; a good way to do it is by using figures or pictures.
- **Learnability**: The UI needs to be as non-threatening and easy to learn as possible; it may be accomplished using real-world metaphors, or pictures of keys and padlocks. The meaning of these metaphors may be incorporated to the security interface indicating users how to easily use the specific security features.
- **Trust**: It is essential for the user to trust the system. This is particularly important in a security environment. The successful application of the previous criteria should typically result in a trusted environment. The concept of trust can be adapted for the HCI-S criteria of trust [19] to "the belief, or willingness to believe, of a user in the security of a computer system". The degree of trust that users have in a system will determine how they use it. For example, a user that does not trust a web site will not supply their credit card details.

Similarly, D'Hertefelt [14] identified six primary factors (i.e., fulfillment, technology, seals of approval, presentation, navigation and brand) that convey trust [1] in an e-commerce environment. Four of these factors are related directly to HCI-S as illustrated in Table 1. Applying these concepts in a security environment using the HCI-S criteria, it is possible to achieve the user trust in the specific system's security.

Table 1
HCI-S and the primary factors that convey trust in an e-commerce environment.

HCI-S Criteria	Primary e-commerce Factors	Relation
Convey features, visibility System	Fulfillment, seat of approval	The users must be appropriately informed about which security features are available, and when are being used.
Aesthetic and minimalist design	Presentation, navigation	A web-site with a minimalist design is easier to use and navigate.
Leamability	Navigation	A web-site that is easy to navigate is also easy to learn by the users
Satisfaction	Fulfillment, presentation	Appropriate notification of available security features using a minimalist web site design. This leads to a more satisfying experience for the users.