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 Crown Copyright © 2009 Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.advengsoft.2009.01.024

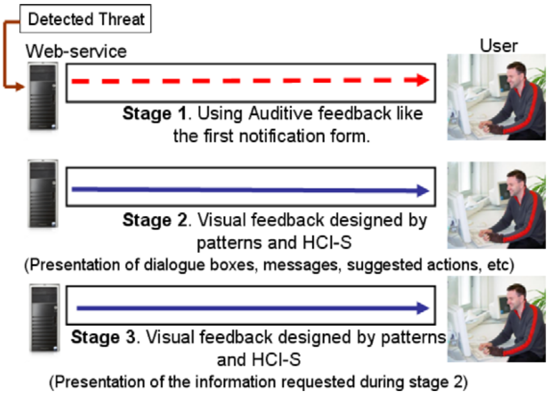

Detected Threat
Web-service
User
Stage 1. Using Auditive feedback like the first notification form.
Stage 2. Visual feedback designed by patterns and HCI-S
(Presentation of dialogue boxes, messages, suggested actions, etc)
Stage 3. Visual feedback designed by patterns and HCI-S
(Presentation of the information requested during stage 2)

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 Criferia	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.

3. Problem outline

We believe that the security information of a specific web-service must be shown in an easy to understand manner. According to Dhamija [13], and Johnson and Zurko [18], a usable security information feedback could reduce possible errors caused by final users when important notifications are ignored, nevertheless the most of the designers or/and programmers do not consider the available design criteria because their application is frequently complex and the criteria are not specified enough [13,18,28]. Another problem may be the insufficient consideration of the end users by the current design specifications. Many design specifications are not comprehensible enough for the Designers and Programmers because the application of patterns is not considered. We think the combination of design patterns and HCI-S criteria could mitigate these problems and makes easier the design of adequate security information feedback.

Braz et al. [3] demonstrated the importance of finding equilibrium between security and usability. Nevertheless most of the security researches not consider usability topics during its development, for this reason it is necessary to provide a support for security, by means of design criteria and guides based on usability and ergonomic principles. In accordance with Atoyan et al. [1], such design rules must be considered during the design of trust systems to increase its proper use and interpretation.

It is necessary an adequate feedback to reduce the possibility that the final users misunderstand security notifications or other information related with the internal state of the system [2,9,18]. Our classification is oriented towards the design of a usable security information feedback, easy to understand and interpret by users with different experience and backgrounds (experts, advanced, and beginners). In the same way our proposal may to incorporate the points of view of the final users to establish improvements. The proposal may complement previous efforts by including the new HCI-S criteria.

4. Methodology for designing information security feedback

Fig. 2 graphically depicts a general view of the application of our methodology. The graphical model is divided in three basic stages to represent an alternative collaboration between three type users (end users, programmers, and designers) to improve a security information feedback of a secure web-service. Other advantage of the application of our proposal consist that the implementation of the improvements could be easier and quick, for Designers and Programmers, because the feedback was originally generated by means of design patterns and considering the HCI-S criteria.

Additionally, we propose the incorporation of UsiXML (http://www.usixml.org) and XML web technologies, which allow, in a standardized and easy manner, the conversion of the knowledge given by the pattern's specification. The proposed methodology based on User Interface (UI) patterns could be more formally expressed in PLML (Pattern Language Markup Language – http://www.hcipatterns.org/PLMLl), in this way it is possible to transfer the design solutions, and criteria offered by patterns to the corresponding UI fragments to the UI which are built in UsiXML. In accordance to the literature [4,5,21], a model for engineering-reverse engineering process, combined with these web-technologies could makes easier the application of design concepts and enhancement of the UI.

We consider that our proposal could facilitate, to Designers and Programmers, the planning and construction of a usable security information feedback, which could makes easier for end users the comprehension and use of the security features available in a specific secure web-service. In other way, the application of our proposal could permit a better use of the knowledge through the different users, this because the patterns may to include experience as a way to find viable solutions to problems. The application of our proposal could to provide the following benefits, among others, to the end users:

- The well designed security information feedback could to facilitate the learning and comprehension of important security concepts conveyed through the interface to end users, even those inexperienced in security.
- The security information feedback designed in a minimalist and aesthetic manner could make easier the learning and memorization of its appearance. The possibility of success of threats like phishing and pharming could be reduced if an end user knows the appearance of the genuine security features of a specific web-service.
- The security feedback generated could to increase the end users' trust during transactions of personal information, or during the buying and payment of products. This because the end users will be notified appropriately if some security problem is detected.

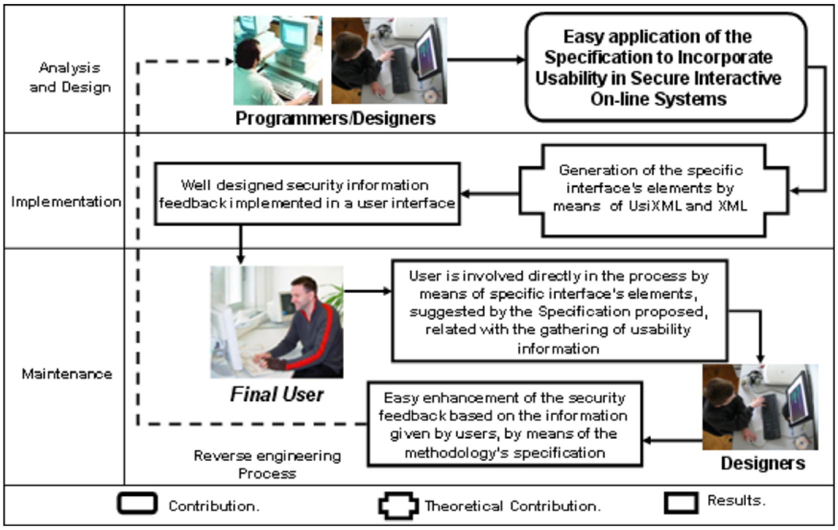

Analysis and Design
Programmers/Designers
Easy application of the Specification to Incorporate Usability in Secure Interactive On-line Systems
Implementation
Well designed security information feedback implemented in a user interface
Generation of the specific interface's elements by means of UsiXML and XML
Maintenance
Final User
User is involved directly in the process by means of specific interface's elements, suggested by the Specification proposed, related with the gathering of usability information
Easy enhancement of the security feedback based on the information given by users, by means of the methodology's specification
Designers
Reverse engineering Process
Contribution.
Theoretical Contribution.
Results.

Fig. 2. Methodology for designing security information feedback explicitly incorporated in the development life cycle.

4.1. User Interface Patterns library

It is well known that secure web services must to keep informed to end user about the internal state of the system and the technologies used by the system to protect confidential information during a transaction. In the same way, the security feedback must to include elements that makes easier the direct operation and use of the available security features. We propose a library of User Interface Patterns bearing in mind the HCI-S criteria, intended to design a usable security information feedback (Fig. 3).

The classification proposed is divided in the following levels which are oriented to represent the basic aspects to handle a UI:

- **Informative Feedback**: This level includes the UI patterns useful to present information about: available security features, the correct way to use these features, detection of threats, and internal status of the system. In the same way, in this level is considered the request of complementary information about detected threats or related with other security aspects.
- **Interaction Feedback**: This level brings together the interaction forms useful to establish the feedback's navigation and operation. This level includes UI patterns needed to create feedback to enabling or disabling security features, and interaction forms to present suggestions of actions to follow when some security threat is detected.
- **Interactive Feedback**: This level includes the UI patterns to specify the security feedback needed to convey information to the end user when the elements of the interface are handled by means of the mouse or the keyboard. We incorporate auditive feedback in the first level to enhance the visual notifications considering the sonification prototype proposed in [16]. This prototype establishes a relationship between five potential threats and a specific animal sound effect in order to identify easier a specific threat. In addition, we complement the Sonification of threats prototype [16], assigning a specific colour to each threat under consideration, and bearing in mind the following colour scheme (see Table 2).

Table 2
Colours scheme for visual notifications.

Colour	Meaning	Activity
Blue	Information	Provide information
Green	Access	Provide information
Yellow	Warning	Provide information and suggestion
Gold	Error warming	Provide information and suggestion
Orange	Emergency	Provide suggestion
Red	Danger	Quick response
Vermilion	Critical	Immediate response

Table 3
Enhanced Sonification prototype with visual feedback.

Colour	Sound effect	Activity
Yellow	Frog	guess
Gold	Cat	rep
Orange	Horse	rsh
Red	Cock	rlogin
Vermilion	Bird	port-scan

The classification of colours presented in Table 2 corresponds to a particular action to follow by users: Immediate response, provide a suggestion, and provide information. Additionally, we establish a priority for the notifications considering visual feedback based on colours to complement the Sonification prototype of García-Ruiz et al. [16], we assign a specific colour to each of the five potential threats considered in [16]. The relation of colour, sound effect, and detected threat is presented in Table 3.

The assignment of colours to the threats was performed considering the risk of the threats, as described in [12].

1. **Guessing Threat**: Here the intruder tries to guess the password that protects the computer network in order to gain access to it (e.g., guess).
2. **Spoofing threat**: The goal of this threat is to usurp an authorized IP address to gain unauthorized access to the victim's system. The IP spoofing threat is often used against communication services taking advantage of their security vulnerabilities (e.g., rsh, rlogin, and rcp threats). This allows the intruder to hide the origin of the threat (typically used in denial-of-service threats).
3. **Scanning Threat**: The intruder probes different ports of the victim's system to find some vulnerable points from where they can launch other threats, (e.g., ICMP threats).

The Scanning and Spoofing attacks may be considered more risky, because they typically represent the preface for other attacks.

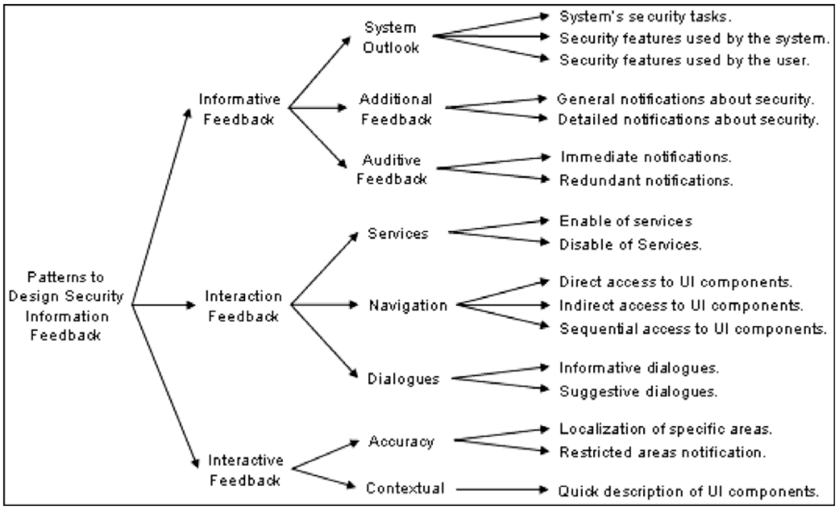

Patterns to Design Security Information Feedback
Informative Feedback
Interaction Feedback
Interactive Feedback
System Outlook
Additional Feedback
Auditive Feedback
Services
Navigation
Dialogues
Accuracy
Contextual
System's security tasks.
Security features used by the system.
Security features used by the user.
General notifications about security.
Detailed notifications about security.
Immediate notifications.
Redundant notifications.
Enable of services
Disable of Services.
Direct access to UI components.
Indirect access to UI components.
Sequential access to UI components.
Informative dialogues.
Suggestive dialogues.
Localization of specific areas.
Restricted areas notification.
Quick description of UI components.

Fig. 3. Classification of audiovisual User Interface Patterns.

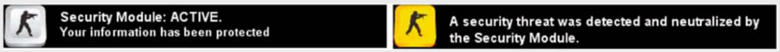
Table 4
Description of the User Interface Patterns included in the library proposed.

Informative Feedback - System Outlook

Pattern's Name: System's security tasks.

- **Problem**: How to inform users about the security tasks performed by the system during an information transaction?
- **Context**: The interface must to inform users about the security activities realized by the system to protect confidential information during a specific transaction. These notifications must be showed avoiding complicate sentences, and the use of technical terms.
- **Motivation**: It is possible to increase trust in a system, if the user knows the activities performed to keep secure all the confidential information.
- **Solution**: The users could be notified about the system's security tasks by means of simple text messages without technical terms. These messages could be reinforced with images, pictures or others visual notifications.

Example: Some system security tasks notifications combining text, images, and real World metaphors.



Security Module: ACTIVE.
Your information has been protected

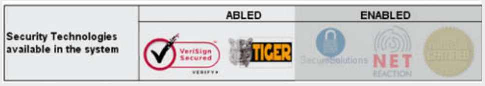
A security threat was detected and neutralized by the Security Module.

Notification of two different security tasks performed by the system.

Pattern's Name: Security features used by the system.

- **Problem**: How to inform users about the security features used by the system during an information transaction?
- **Context**: The interface must notify users about the security technologies activated by the system to protect confidential information during a specific transaction. These notifications must be shown avoiding complicate sentences, and the use of technical terms.
- **Motivation**: It is possible to increase trust in some system, if the user is informed about the technologies used by the system to keep secure all the confidential information.
- **Solution**: The users could be notified by means of a specific panel that shows active and non-active security technologies.

Example: Notification about the active security scheme's elements using a specific panel and logotypes.

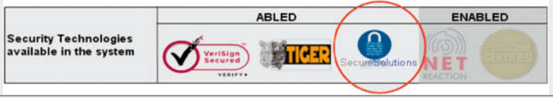


Security Technologies available in the system

Pattern's Name: Security features used by the user.

- **Problem**: How to inform users about the security features used by She/He during an information transaction?
- **Context**: The interface must to notify users about the security technologies activated additionally by She/He to protect confidential information during a specific transaction. These notifications must be presented avoiding complicate sentences, and the use of technical terms.
- **Motivation**: It is possible to increase trust in some system, if the user is informed about the technologies used by She/He to keep secure all the confidential information.
- **Solution**: The users could be notified by means of a specific panel that shows those security technologies selected and activated by the user.

Example: Notification about the security scheme's elements activated by the user. Bearing in mind the previous example, the new element was activated when user select it from the logotype's list using the mouse.



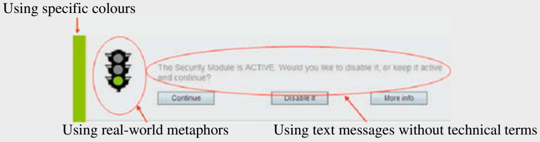
Security Technologies available in the system

Informative Feedback - Complementary Feedback

Pattern's Name: General notifications about security.

- **Problem**: How to inform users about the general state of the system during an information transaction?
- **Context**: The interface must to provide the necessary information about its internal state. These notifications must be showed to the users avoiding complicate sentences, and the use of technical terms.
- **Motivation**: If the users are informed about the internal state of the system during a transaction the trust environment could be enhanced.
- **Solution**: The users could be notified through messages, images, real world metaphors, combination of colours, among other visual feedback, always considering a minimalist and aesthetic design.

Example: Some notifications about the general state of the system.



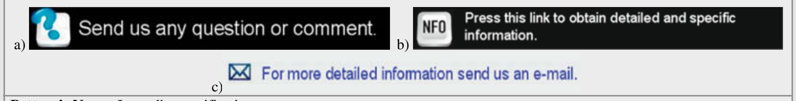
The Security Module is ACTIVE. Would you like to disable it, or keep it active and continue?

Using specific colours
Continue
Disable it
More info
Using real-world metaphors
Using text messages without technical terms

Pattern's Name: Detailed notifications about security.

- **Problem**: How to permit the user to get specific information about the security of the system?
- **Context**: The interface must to provide options to obtain detailed information about the system for general or specific topics.
- **Motivation**: This alternative avoids showing irrelevant information through the interface, reducing space, and contributing to maintain an aesthetic design.
- **Solution**: Including in the notifications presented to the end users e-mail links to obtain specific information about the security features of the system, and detected threats.

Example: Three suggestions to present users the option to obtain detailed information by e-mail.



a) Send us any question or comment.

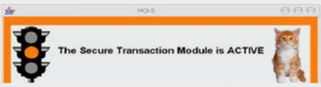
b) Press this link to obtain detailed and specific information.

c) For more detailed information send us an e-mail.

Pattern's Name: Immediate notifications.

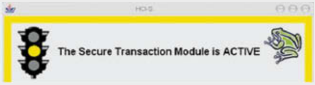
- **Problem**: How to inform to the end user about a detected threat?
- **Context**: The interface must to notify users about the internal state of the system in a quick and efficient way.
- **Motivation**: If the users are informed immediately about some detected threat the possibilities to mitigate it are increased.
- **Solution**: An additional feedback form could enhance the visual notifications and inform users in a quick manner.

Example: In this case, we present two examples of the combination of auditive and visual feedback. We establish a specific relation between an animal sound effect, a colour, and a specific threat (see Subsection 4.1).



The Secure Transaction Module is ACTIVE

Cat sound-effect – gold colour– "rcp" threat.



The Secure Transaction Module is ACTIVE

Frog sound-effect – yellow colour– "guess" threat.

Pattern's Name: Redundant notifications.

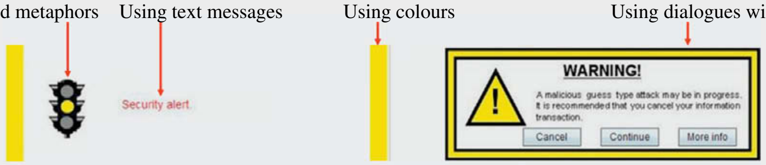
(continued on next page)

Table 4 (*continued*)

- **Problem**: How to maintain informed users about some detected threat?
- **Context**: Some users need redundant information about the internal state of the system.
- **Motivation**: Showing redundant notifications (in restraint) the users will be correctly informed about some detected threat.
- **Solution**: The users could be notified through messages, images, real world metaphors, combination of colours, among other visual feedback which stand visible through user considers the suggestions provided.

Example: In this case we present the notification of “guess” threat detection, using colours, text messages, images, and dialogues and considering the relation presented in Table 3.

Using real-world metaphors Using text messages Using colours Using dialogues with options



Security alert

WARNING!

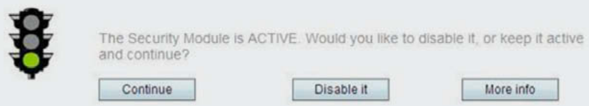
A malicious guess type attack may be in progress. It is recommended that you cancel your information transaction.

Interaction Feedback – Services

Pattern’s Name: Disable of services.

- **Problem**: How to give to the end users more control over the system?
- **Context**: Sometimes the security technologies make slower a particular transaction.
- **Motivation**: If the system provide options to able and disable specific security features, user could have a feeling of more control over the system.
- **Solution**: Including options to disable the security features or to continue using it.

Example: Options to able and disable specific security features.



The Security Module is ACTIVE. Would you like to disable it, or keep it active and continue?

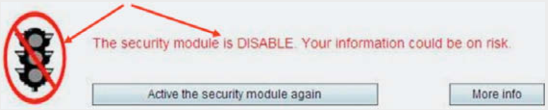
Interaction Feedback – Navigation

Pattern’s Name: Direct access to UI components.

- **Problem**: How to facilitate to the end users the access to the elements of the interface?
- **Context**: The system must to provide to users a quick an easy access to the elements of the complete interface.
- **Motivation**: An easy and quick access to the elements of the interface in any system is very important. Accessibility represents an essential topic in usability.
- **Solution**: By means of a minimalist and aesthetic design it is possible to keep accessible all the security elements, including those disabled.

Example: Presentation of security feedback to notify about the available security technologies.

Additional indicators

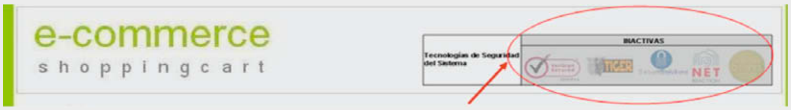


The security module is DISABLE. Your information could be on risk.

Pattern’s Name: Indirect access to UI components.

- **Problem**: How to facilitate to the end users the access to features of the system necessarily presented in additional screens?
- **Context**: The system must to provide to users a quick an easy access to the external features available or used by the system.
- **Motivation**: An easy and quick access to external features could to increase the trust of the user in the system.
- **Solution**: By means of a panel that list those security features used by the system. The panel must allow the access to these technologies.

Example: Options to accessing external features available in the system.



Options to accessing external features

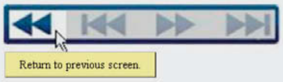
Pattern’s Name: Sequential access to UI components.

- **Problem**: How to facilitate to the end users the access to features of the system presented in previous screens?
- **Context**: The system must to provide to users the navigation between screens in an agile and easy manner, considering a logical and continuous sequence.
- **Motivation**: An easy and quick access to the all the elements and features of the system represents a very favorable experience for the user.
- **Solution**: Including a simple navigator in the user interface.

Example: A classical navigator enhanced with messages that appear when user select an option with the mouse.

(continued on next page)

Table 4 (*continued*)

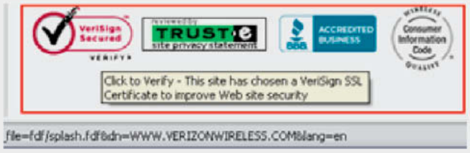

Return to previous screen.

Interaction Feedback – Dialogues

Pattern's Name: Informative dialogues.

- **Problem**: How to makes easier the showing of notifications about some detected threat?
- **Context**: The system must to inform users about the internal state of the system in a quick and easy to understand manner.
- **Motivation**: Avoiding technical terms and irrelevant information in all the notifications the number of errors (caused by users when a security notification is ignored or misunderstood) could be reduced.
- **Solution**: By means of simple and specific messages the users could be notified about the internal state of the system.

Example: Notification about the internal state of the system using text messages enhanced with images and real world metaphors.



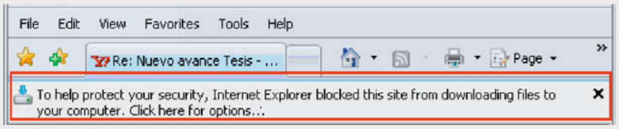
Click to Verify - This site has chosen a VeriSign SSL Certificate to improve Web site security

file=fdf/splash.fdf&dn=WWW.VERIZONWIRELESS.COM&lang=en

Pattern's Name: Suggestive dialogues.

- **Problem**: How to facilitate the interpretation of a security alert and the reduction of damages caused by some detected threat?
- **Context**: The system must to provide users suggested actions to follow to mitigate the damages caused for some detected security threat.
- **Motivation**: A suggested action represents a contribution to reduce misunderstands and makes easier the decision making.
- **Solution**: By means of specific messages (without technical terms or irrelevant information) the users could be notified about the internal state of the system. The messages must include suggested actions to follow in case of eventuallity.

Example: Security notification by means of a dialogue box that includes a simple text message, suggested actions to follow.



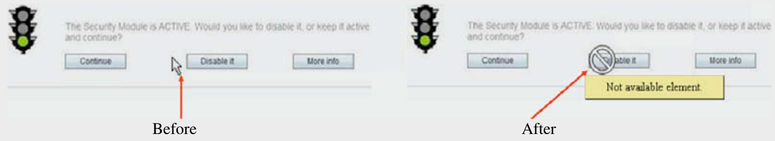
To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...

Interactive Feedback – Precision

Pattern's Name: Localization of specific areas.

- **Problem**: How to indicate to the end user the limits of specific elements of the interface?
- **Context**: The system must to indicate clearly those elements in the interface that belongs to system's security, and to provide an appropriated access to these elements.
- **Motivation**: An adequate distinction of the security elements could to speed up the localization of specific elements of the interface.
- **Solution**: Changes in the shape of the mouse's cursor is a good alternative to notify about the frontiers between the different elements of the interface. It could be enhanced including text messages.

Example: Notification of localization by means of a change in the mouse's shape enhanced with a message visible when the user points the mouse over a specific element of the interface.


The Security Module is ACTIVE. Would you like to disable it, or keep it active and continue?

Not available element.

Pattern's Name: Restricted areas notification.

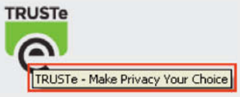
- **Problem**: How to notify users about the restricted areas in the system?
- **Context**: The system must to inform users the limits established for specific elements in the interface. This notification must to be made in a very kind manner.
- **Motivation**: An adequate feedback makes easier the introduction of restrictive messages.
- **Solution**: Changes in the shape of the mouse's cursor is a good alternative to notify about the restricted elements of the interface. Additionally, messages with a touch of humor could be used (in moderation). See previous example.

Contextual

Pattern's Name: Quick description of UI components.

- **Problem**: How to provide to the end users basic information about specific security information feedback elements?
- **Context**: The system must to inform about which elements of the interface belongs to the security scheme.
- **Motivation**: These notifications could to reduce errors related with security and contribute to establish a trusted environment.
- **Solution**: Using messages visible when the user points the mouse over a specific security element.

Example: Notification by means of messages visible when the user points the mouse over a specific security element.



TRUSTe - Make Privacy Your Choice

For that reason, we assign red tones to these threats (see Table 2). It is important to mention that the five potential threats considered in [16] are specified in a network log. This log file is available publicly and was generated by DARPA [11].

It is important to mention that association sound-threat proposed in [16] is oriented to be useful for network administrators, specifically to notify about malicious attacks either in real time or during the analysis of network logs, in forensics. We consider this relation like a starting point to establish other relations between sounds and threats (see Section 7).

4.2. Outlook of the proposed User Interface Patterns

In order to present a general view of the proposed pattern's library, we define the User Interface Patterns presented in Fig. 3, considering the Gamma's format, including a possible recurrent problem, the context, a motivation, and a suggested solution offered by the patterns (Table 4). We have several previous experiences acquired in order to discover the proposed patterns, two examples of prior versions are presented in [24,25]. All versions were constructed bearing in mind important researches, i.e. [23].

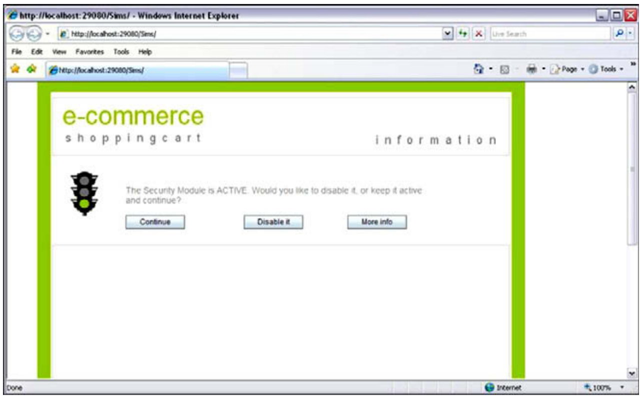
5. Laboratory study

Following the methodologies for usability tests presented in the literature [6,7,16]; we conducted a case study in order to evaluate the usability level of specific security information feedback designed applying the proposed User Interface Patterns (see Fig. 3). In general terms this study consists of having users filling a typical e-commerce formulary of personal information. The participants must follow security information feedback presented through the interface. The security feedback was designed applying the interface patterns proposed (see Fig. 3). We consider the following factors during the laboratory study:

- **Participants**: We recruit fifteen participants, consisting eight women and seven men varied in different ages from 22 to 54. The participants are common final users, graduates in areas including medicine, business administration, and computer science. Only four participants (three women and one man) are computer science graduates and have experience in the use of security and notification systems, the rest of the participants are novices in this topic.
- **Apparatus**: We designed an e-commerce form and a set of security information feedback generated by means of the specification of the proposed patterns, including auditive and visual notifications. This prototype was created using the Java Studio Creator 2 Update 1 Free version (http://developers.sun.com/jscreator/downloads/).
- **Training materials**: We presented participants with a two pages document on how to use the prototype, the paper included: The objective of the experiment, a brief introduction to the experiment, and a set of activities to realize during the experiment. Note: None of the information related with the use and interpretation of the security notifications and security concepts was shown to the participants in said paper.
- **Tasks**: Participants accessed the prototype and follow the suggested actions and options presented during the use of the prototype. Subsequently, participants answered a questionnaire related with the usability of the security information feedback presented by means of the prototype.

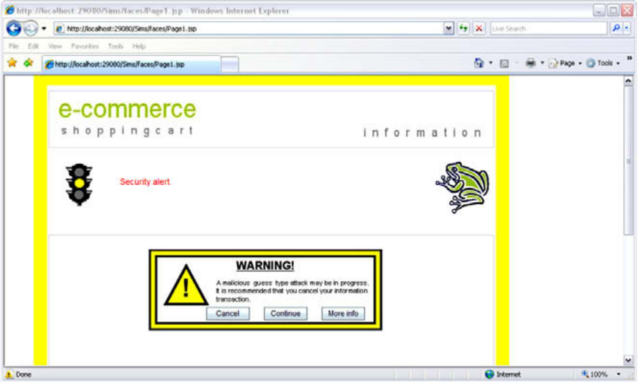
We consider the five potential threats (guess attack, rsh attack, and rcp attack) described in Section 4. The security feedback was designed bearing in mind the specification of the proposed User Interface Patterns presented in Table 4. To provide a general view of the prototype used for this experiment we present the following graphical examples (see Figs. 4 and 5) and its textual explanation.

- **Pattern's Name**: Security features used by the system, System's security tasks, and Enable/Disable all the security features.
- **Problem**: How to convey the security features of the web-service clearly?


http://localhost:29080/Sims/ - Windows Internet Explorer
http://localhost:29080/Sims/
Live Search
File Edit View Favorites Tools Help
http://localhost:29080/Sims/
Page Tools
e-commerce
shoppingcart
information
Continue
Disable it
More info
Done
Internet
100%

The Security Module is ACTIVE. Would you like to disable it, or keep it active and continue?

Fig. 4. A green colour is used in the frame and in the traffic lights to indicate the users that the system is protected (Application of the design pattern "*Security features used by the system*"). The text "The Secure Transaction is ACTIVE" is always visible, being other form to notify about the internal state of the system (Application of the design pattern "*System's security tasks*"). In the same way, a message is presented in a dialogue box that also includes the option to disable the security module or to continue using it giving the user more control over the system (Application of the design pattern "*Enable/Disable all the security features*").


http://localhost:29080/Sims/faces/Page1.jsp - Windows Internet Explorer
http://localhost:29080/Sims/faces/Page1.jsp
Live Search
File Edit View Favorites Tools Help
http://localhost:29080/Sims/faces/Page1.jsp
Page Tools
e-commerce
shoppingcart
information
Security alert
WARNING!
Cancel
Continue
More info
Done
Internet
100%

A malicious guess type attack may be in progress. It is recommended that you cancel your information transaction.

Fig. 5. This figure shows the appearance of the UI when a "guess" potential threat is detected, in this case, a frog sound is generated (a frog sound is mapped to this threat, see Table 3), yellow colour is used in the frame and in the traffic lights (Application of the design pattern "*Immediate notification of threats*"). Immediately, the interface presents a message in a dialogue box that includes the options "Cancel" and "More Information" (Application of the design pattern "*Dialogue with suggested actions to follow*"). At the same time, the dialogue shows a frog picture at the top right corner of the screen. In this dialogue was considered a specific threat-colour-sound-picture relation (see Table 3).

- **Solution**: Using an image of traffic lights and the message "The Security Module is ACTIVE" the users will be alerted about the protection of the system. Fig. 4 presents a graphical example.
- **Pattern's Name**: Dialogues with suggested actions to follow, and immediate notification of threats.
- **Problem**: How to present a clear visibility of the system status?
- **Solution**: By means of changing the color of the interface's frame and the traffic lights, a sound alarm, and a specific message (without technical terms or irrelevant information) the users will be notified about the internal state of the system. The messages include a suggested action to prevent or mitigate the damage caused by the threat, and also, as well as a link to obtain additional information.

After using the prototype, we presented to the participants the following questionnaire which is based on the HCI-S design/evaluation criteria:

(1) The notifications of security, presented throughout the filling of the formulary, were designed in order to be enough detailed but simple. From your own point of view, to what extent was this criterion respected?
(2) Did the notifications presented throughout the filling of the formulary provide an understandable and clear view-point about the state of the system?
(3) Did both the layout of the information about security and the options included in the design of the notifications make easier their use and understand?
(4) Did the notifications presented throughout the filling of the formulary suitably provide information about the security features available in the prototype?
(5) Did the notifications presented throughout the filling of the formulary provide an easy use of the security features available?
(6) Did the notifications presented throughout the filling of the formulary make you trust in the system?
(7) Do you consider that the design concepts, applied to generate the security information feedback, could help e-commerce sites users to understand easily important security concepts, in order to reduce security mistakes, and result in a trusted environment?

5.1. Data analysis

The participants answered the questionnaire with the tendency showed in Fig. 6. Each question had six possible answers: Strongly agree, agree, do not know, disagree, strongly disagree, unable to assess. In order to show the tendency of the participants we assign a specific color to each answer. In example for Question 4: Eleven participants selects the option "Strongly Agree", two selects the option "Agree", one selects the option "Do not Know", and one selects the option "Disagree".

The following points can be inferred from analyzing the result data:

- The auditive alerts combined with visual feedback results in a very useful notification method for users informing to them about the internal state of the system in a quick and adequate way.
- The use of animal sound effects results in a friendly and very useful form of security notification for the users. Nevertheless, using other animal sounds effects like a tiger's roar the user could easier become aware of a dangerous threat detected.
- The auditive alerts combined with visual feedback makes easier to the users the comprehension of important security notifications about the internal state of the system.
- The application of the proposed set of patterns permits to achieve a usable security information feedback combining auditive and visual notifications.
- The design solutions and specification offered by the proposed set of patterns may result in a trusted environment.
- The security information feedback designed by applying the patterns proposed, is detailed enough but concrete.

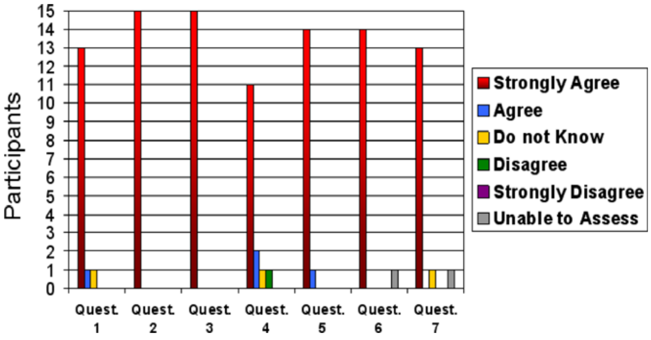


Fig. 6. Tendency of the participant's opinion.

In general terms, we believe that the design solutions and specification offered by the proposed set of patterns may increase the usability of security notifications presented to the end user. The design concepts of the patterns proposed, allows an appropriate conveying of security information to end users by means of the UI's elements. The use of the proposed set of patterns result in a well designed security information feedback combining auditive and visual notifications. The auditive-visual sensorial correlation represents a powerful alternative to reduce possible errors caused by end users when a security notification is ignored or misunderstood.

In addition, with the security feedback designed for this study case also was considered and covered the following HCI-S design criteria:

1. **Learnability**: The UI is easy to learn and friendly because the use of colors in the frame that notify about some threat detected and the use of real-world metaphors such as traffic lights. The UI also uses animal sound effects to distinguish among detected threats, and an image of the animal related with the threat type and the sound effect is presented at the top right corner of the screen.
2. **Aesthetic and minimalist design**: The UI informs about the security features available and when they are being used, showing only relevant information in the messages and notifications of the security features, maintaining a simple design. The relation between sounds and threats make easier the distinction among detected threats, and the color of the interface's frame and the traffic lights complement an easy to use interface.
3. **Trust**: The interface may to achieve that the user trust in a system, through adequate notifications, and clear suggested actions to prevent or mitigate the damage caused by the threat. The users know, by means of the interface's elements, that their information has being protected by the security features of the system.

6. Related work

In this section we present some of the most significant related work. We use the following criteria to identify advantages and disadvantages of our research: Proposal of a usable security information feedback, presentation of security aspects to the users, consideration of HCI-S design's criteria, and consideration of more than a sensory channel. We have considered the research works of: Rode et al. [28], Yurcik et al. [29], Cranor [9] and Cranor and Garfinkel [10], Ka-Ping [20], and McCrickard et al. [22] (see Table 5).

Table 5 illustrates the criteria performed by each research work. The focus of [28] has been on providing final users with information they can use to understand the implications of their interactions with a system, as well as assessing the security of a system.

The authors have been exploring two design principles for secure interaction: visualizing system activity and integrating configuration and action. The research shows a very good design strategy, but they are not consider the HCI-S design criteria, or the incorporation of sonification, which may complement this research. Similarly the work of Yurcik et al. [29] try to facilitate the realization of specific activities related to security by means

Table 5
Comparison of research works.

Researches	Criteria			
	Proposal of a usable security information feedback	Presentation of security aspects to the users	Consideration HCI-S design's criteria	Consideration of more than a sensory channel
Rode et al. [23]	X	X	–	–
Yurcik et al. [29]	X	X	–	–
Cranor [9]; Cranor et al. [10]	X	X	–	–
Ka-Ping [20]	X	X	–	–
McCrickard et al. [22]	X	X	–	–
Current work	X	X	X	X

of simple instructions and suggestions offered to the users through the interface elements. The research works presented in [9,10] propose a very interesting strategy to facilitate the creation of simple interfaces, easy to understand and use by users, emphasizing some challenges that face the designers during the development process of security and privacy software configuration options. The objective of the research presented by Cranor and Garfinkel [10] is very similar to the goal of our work; nevertheless, in [10] are not considered auditive notifications or an additional feedback form. In the same way, the incorporation of the HCI-S criteria is not included. The research of Ka-Ping [20] consists of the proposal of a model of 10 points to represent the interaction of the users with secure systems. The model is based on actors and their abilities, and provides the actors some authority to assist users determining whether a particular action is secure or not. In a similar way, McCrickard et al. [22] propose a very interesting strategy to design and evaluate usable feedback, but do not considered the application of the HCI-S design criteria and the incorporation of sonification. In general terms, we believe that, the application of the new HCI-S criteria, and the incorporation of sonification, may increase the usability of the works mentioned above. With the research work presented in this paper we try to perform the four comparison criteria (Table 5), and thus provide a complement for other research works.

7. Concluding remarks and future work

Bearing in mind previous works, such as those described in [13,18,20,28,29], we present a methodology intended to facilitate the way some security aspects are conveyed to the end user. We generate a non-exhaustive classification of information security feedback based on User Interface Patterns. With the proposed classification, it is possible to achieve an appropriate feedback through the elements of the interface by means of visual and auditive notifications about information related to the security and the internal state of a particular on-line system. Similarly, the User Interface Patterns are oriented to designing and generating information security feedback easy to understand and interpret by users with different levels of experience and backgrounds (experts, advanced, and beginners) avoiding, as much as possible, the use of technical terms. We consider that specific audiovisual notifications using intuitive elements designed by means of our guidelines application may represent a very good way to notify users about the security and the internal state of a specific web-service.

There are several aspects to explore as future work, such as the establishment of additional relationships between sounds and threats considering its dangerousness, i.e. using a panther's roar to notify users about a very dangerous threat. In the same way, it is necessary to perform a number of usability studies that consider enhanced evaluation methods, actually we recently create a prototype metrics based instrument oriented to complement and formally evaluate our proposal. In the near future, we also would like to investigate how other interaction modalities (e.g., speech, or haptic feedback) could complement or supplement the existing ways to provide feedback to the end users.

Acknowledgments

The second author thanks CONCyTEA (Consejo de Ciencia y Tecnología del Estado de Aguascalientes) for support in his PhD. He also thanks the Universidad Autónoma de Aguascalientes (UAA) for supporting his research collaboration with the University of Ontario Institute of Technology.

References

[1] Atoyan H, Duquet J, Robert J. Trust in new decision aid systems. In: Proceedings of the 18th international conference of the association francophone d'interaction Homme-machine IHM'06, Montreal, April 18–21. New York: ACM Press; 2006. p. 115–22.

[2] Berry B, Hobby L, McCrickard S, North C, Pérez-Quiñones M. Making a case for HCI. Exploring benefits of visualization for case studies. In: Proceedings of world conference on EDMEDIA'06, Orlando, June 26–30; 2006.

[3] Braz C, Seffah A, M'Raihi D. Designing a trade-off between usability and security: a metrics based-model. In: Proceedings of 11th IFIP TC 13 conference on human–computer interaction INTERACT'07, Rio de Janeiro, September 10–14. Lecture Notes in Computer Science, vol. 4663. Berlin: Springer; 2007. p. 114–26.

[4] Bouillon L, Vanderdonckt J, Eisenstein J. Model-based approaches to reengineering web pages. In: Proceedings of first international workshop on task models and diagrams for user interface design TAMODIA'02. Academy of Economic Studies of Bucharest, Bucharest: INFOREC Printing House; 2002. p. 86–95.

[5] Bouillon L, Limbourg Q, Vanderdonckt J, Michotte B. Reverse engineering of web pages based on derivations and transformations. In: Proceedings of third Latin American web congress LA-Web'05, Buenos Aires, Argentina, October 31–November 2. IEEE Computer Society Press; 2005. p. 3–13.

[6] Chiasson S, Biddle R, van Oorschot P. A second look at the usability of click-based graphical passwords. Best Paper Award. In: Proceedings of symposium on usable privacy and security, SOUPS'07, Pittsburgh, July 18–20; 2007.

[7] Chiasson S, van Oorschot P, Biddle R. Graphical password authentication using cued click points. In: Proceedings of 12th European symposium on research in computer security, September 24–27, Dresden, Germany. Lecture Notes in Computer Science. Berlin: Springer; 2007. p. 359–74.

[8] Chong Lee J, McCrickard S. Towards extreme(ly) usable software: exploring tensions between usability and agile software development. In: Proceedings of AGILE'07, Washington DC, August 13–17. IEEE Computer Society Press; 2007. p. 59–71.

[9] Cranor L. Designing a privacy preference specification interface: a case study. In: Proceedings of ACM CHI'2003 workshop on human–computer interaction and security systems, Fort Lauderdale, April 5–10. New York: ACM Press; 2003.

[10] Cranor L, Garfinkel S. Security and usability: designing secure systems that people can use. Sebastopol: O'Reilly; 2005.

[11] DARPA. Intrusion detection evaluation: data sets. Massachusetts Institute of Technology (MIT), Lincoln Laboratory, Boston; 1999. Accessible at: <http://www.ll.mit.edu/IST/ideval/data/1998/1998_data_index.html>.

[12] Dass M. LIDS: a learning intrusion detection system. BE thesis, Nagpur University; 2000.

[13] Dhamija R. Security usability studies: risk, roles and ethics. In: Proceedings of ACM CHI'07, workshop on security user studies, San Jose, April 28–May 3. New York: ACM Press; 2007.

[14] D'Hertefelt S. Trust and the perception of security; 2000. Accessible at: <http://www.interactionarchitect.com/research/report20000103shd.htm>.

[15] Dustin E, Rasca J, McDiarmid D. Quality web systems: performance, security, and usability. NY: Addison-Wesley; 2001.

[16] García-Ruiz M, Vargas Martin M, Kapralos B. Towards multimodal interfaces for intrusion detection. Audio engineering society: pro audio expo and convention, Vienna; 2007.

[17] Hewett T, Baecker R, Card S, Carey T, Gasen J, Mantei M, Perlman G, Strong G, Verplank W. ACM SIGCHI curricula for human–computer interaction. ACM; 2004. Accessible at: <http://www.acm.org/sigchi/cdg/cdg2.html>.

[18] Johnson M, Zurko M. Security user studies and standards: creating best practices. In: Proceedings of ACM CHI'07 workshop on security user studies, San Jose, April 28–May 3. New York: ACM Press; 2007.

[19] Johnston J, Eloff J, Labuschagne L. Security and human computer interfaces. IEEE Computers & Security 2003;22(8).

[20] Ka-Ping Y. Secure interaction design and the principle of least authority. In: Proceedings of ACM CHI'03 workshop on human–computer interaction and security systems, Fort Lauderdale, April 5–10. New York: ACM Press; 2003.

[21] Martínez-Ruiz F, Muñoz Arteaga J, Vanderdonckt J, González-Calleros J, Mendoza R. A first draft of a model-driven method for designing graphical user interfaces of rich internet applications. In: Proceedings of fourth Latin American web congress, LA-Web'06. Universidad de las Américas (UDLA), Cholula, Puebla, México, October 25–27; 2006.

[22] McCrickard S, Czerwinski M, Bartramc L. Introduction: design and evaluation of notification user interfaces. International Journal of Human Computer Studies 2003;58:509–14.

[23] Montero S, Díaz P, Aedo I. Web and design patterns. Chapter 12: integration of patterns in design process of hypermedia applications. Prentice-Hall; 2005 [in Spanish].

[24] Muñoz J, Mendoza R, Vargas Martin M, Vanderdonckt J, Álvarez F, González-Calleros J. A method to design information security feedback Using patterns and HCI-security criteria. In: Proceedings of seventh international conference on computer-aided design of user interfaces CADUI'08, Albacete, Spain, June 11–13. Lecture Notes in Computer Science. Berlin: Springer; 2008.

[25] Muñoz-Arteaga J, Ricardo Mendoza-Gonzalez, Vanderdonckt J. A Classification of security feedback design patterns for interactive web services. In: Heikkinen S, Jorstad I, Tapus N, editors. Proceedings of third international conference on internet monitoring and protection ICIMP'08, Bucharest, Rumania. Los Alamitos: IEEE Computer Society Press; 2008. p. 166–71.

[26] Nielsen J. Ten usability heuristics, Nielsen & Norman Group, Mountain View; 2005. Accessible at: <http://www.useit.com/papers/heuristic/heuristic_list.html>.

[27] Reeder R, Karat C, Karat J, Brodie C. Usability challenges in security and privacy policy-authoring interfaces. In: Proceedings of 11th IFIP TC 13rd conference on HCI, INTERACT'07. Berlin: Springer. LNCS, vol. 4663; 2007. p. 141–55.

[28] Rode J, Johansson C, DiGioia P, Silva Filho R, Nies K, Nguyen D, Ren J, Dourish P, Redmiles D. Seeing further: extending visualization as a basis for usable security. In: Proceedings of second ACM symposium on usable privacy and security SOUPS'06, Pittsburgh. New York: ACM Press; 2006. p. 145–55.

[29] Yurcik W, Barlow J, Lakkaraju K, Haberman M. Two visual computer network security monitoring tools incorporating operator interface requirements. In: Proceedings of ACM CHI'03 workshop on human–computer interaction and security systems, Fort Lauderdale, April 5–10. New York: ACM Press; 2003.