A Method to Design Information Security Feedback Using Patterns and HCI-Security Criteria

Jaime Muñoz-Arteaga[1], Ricardo Mendoza González[1], Miguel Vargas Martin[2], Jean Vanderdonckt[3], Francisco Álvarez-Rodriguez[1], Juan González Calleros[3]

[1] Universidad Autónoma de Aguascalientes, Centro de Ciencias Básicas, Av. Universidad 940, 20100 Ciudad Universitaria Aguascalientes (Mexico)
mendozagric@yahoo.com.mx, {jmunozar, fjalvar}@correo.uaa.mx
[2] University of Ontario Institute of Technology, 2000 Simcoe St. N. Oshawa, L1H7K4 (Canada)
miguel.vargasmartin@uoit.ca
[3] Université catholique de Louvain, Belgian Lab. of Computer-Human Interaction (BCHI)
Place des Doyens, 1 – B-1348 Louvain-la-Neuve (Belgium)
jean.vanderdonckt@uclouvain.be, juan.gonzalez@student.uclouvain.be

Abstract. In order to design a user interface of a secure interactive application, a method is provided to designers with guidance in designing an adequate security information feedback using a library of user interface design patterns integrating security and usability. The resulting feedback is then evaluated against a set of design/evaluation criteria called Human-Computer Interaction for Security (HCI-S). In this way, notifications combining visual and auditive channels required to achieve an effective feedback in case of a security issue are explicitly incorporated in the development life cycle.

Keywords: Design patterns, Heuristic evaluation, Security Information Feedback, Trust, Usability, User-centered design, User interface patterns.

1 Introduction

The term “user feedback” is often referred to as to any form of communication directed 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 [13]. The concepts of traditional HCI can be used to design the interface or improve some interface currently available, 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 recently being introduced [15] 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 how to improve security through the elements of the interface. We use the HCI-S definition proposed by Johnston et al. [15] which textually reads “The part of a user interface 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 [15], 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 end user about some security threat, possibly augmented with auditive notifications or any other kind of feedback; 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.

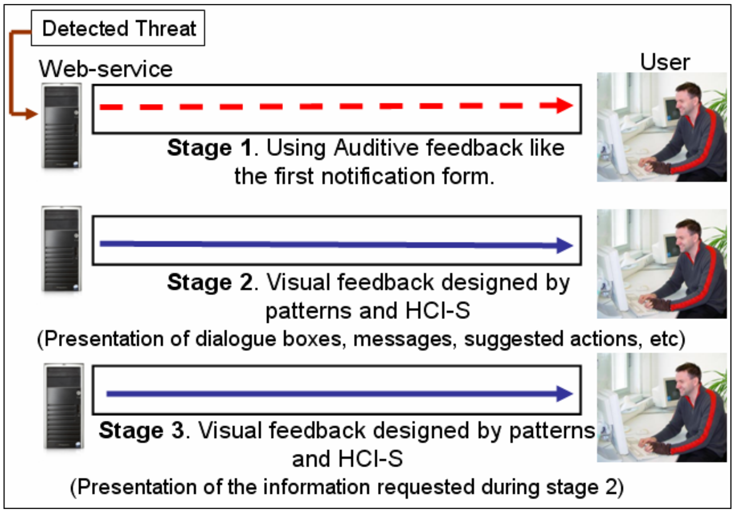

Detected Threat
Web-service
User
Stage 1. Using Auditive feedback like the first notification form.
Stage 2. Visual feedback designed by patterns and HCI-S
(Presentation of dialogue boxes, messages, suggested actions, etc)
Stage 3. Visual feedback designed by patterns and HCI-S
(Presentation of the information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

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

Combining visual and auditive channels in an alert benefits from the following advantages [12]:

- 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 [3,11,15] both from the user studies point of view [14,21] and the usability challenges posed by this integration [19]. 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 [3,6,9,20], 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 case 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. [15]. These criteria facilitate developing usable interfaces that are used in a security environment, based on Nielsen's heuristics traditionally used for heuristic evaluation [18]:

- **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 [15] 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 [10] 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, seals 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.
Learnability	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 [9], and Johnson et al. [14], 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 [9,14,20]. 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 [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 [5,14,22]. 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. The HCI-S patterns are more formally expressed in PLML (Pattern Language Markup Language - http://www.hcipatterns.org/PLML+1.0.html) and the corresponding UI fragments, in UsiXML (www.usixml.org).

4 Designing Security Feedback Using Patterns and HCI-S Criteria

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 classification of interactive patterns based on HCI-S criteria intended to design a usable security information feedback (Fig. 2).

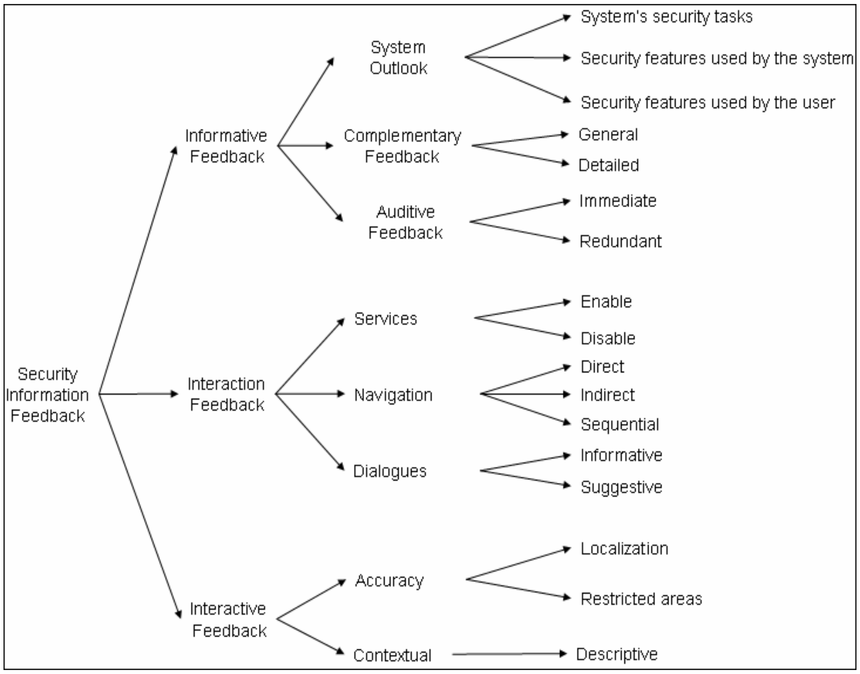


Fig. 2. Classification of audiovisual interactive patterns.

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 interactive 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 interactive 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 interactive 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 [12]. This prototype establishes a relationship between five potential threats and a specific animal sound effect. We complement such relationship with visual notifications, assigning a specific color to each threat under consideration (Table 2). It is important to mention that the five potential threats considered in [12] are specified in a network log, this log file is available publicly and was generated by DARPA [7].

Table 2. Enhanced sonification prototype with visual feedback.

Color	Sound Effect	Detected Threat
Yellow	Frog	guess
Orange	Cat	rcp
Red	Horse	rsh
Purple	Cock	rlogin
Violet	Bird	port-scan

Before continuing, we describe briefly the threats presented in Table 2, which are directly related with three common network threats [8].

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).

In order to present a general view of our classification, we define some of the interactive patterns presented in Fig. 2, considering a possible recurrent problem based on the HCI-S criteria, and a suggested solution offered by the patterns (Table 3).

Table 3. Description of some interactive patterns included in the classification proposed.

Problem	Solution	Interactive Pattern
How to permit the user to get specific information about the security of the system?	By giving in the notifications presented to the end users links to obtain, by e-mail, specific information about the security features, the detected threats, among other security topics.	Detailed complementary feedback
How to inform to the end user about a detected threat?	Using an additional feedback form to enhance the visual notifications established to inform about detected threats.	Immediate auditive notification
How to inform to give to the end users more control over the system?	By giving in specifics notifications presented to the end users the option to disable the security features or to continue using it.	Disable of services.
How to facilitate to the end users the access to the elements of the interface?	By means of an minimalist and aesthetic design it is possible to present, in an adequate form, the security information feedback and keep accessible and visible its active elements in the interface.	Direct navigation

How to facilitate the interpretation of a security alert and the reduction of damages caused by some detected threat?	By means of specific messages (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.	Suggestive dialogues
How to indicate to the end user the limits of specific elements of the interface?	By means of changes in the shape of the mouse's cursor the end user may be informed about the frontiers between the elements of the system interface and the elements of the security information feedback.	Localization
How to provide to the end users basic information about specific security information feedback elements?	Showing messages, without technical terms and irrelevant information, when the user pass the mouse's cursor over a specific element of the security information feedback.	Descriptive

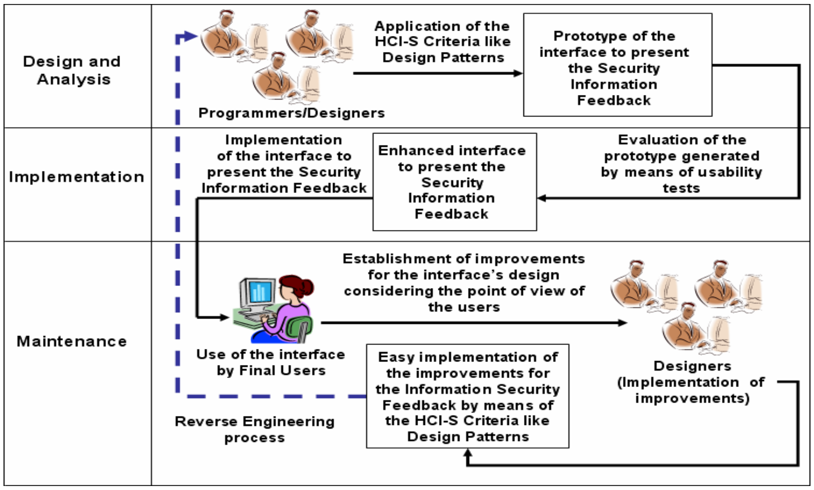

Design and Analysis
Programmers/Designers
Application of the HCI-S Criteria like Design Patterns
Prototype of the interface to present the Security Information Feedback
Implementation
Implementation of the interface to present the Security Information Feedback
Enhanced interface to present the Security Information Feedback
Evaluation of the prototype generated by means of usability tests
Maintenance
Establishment of improvements for the interface's design considering the point of view of the users
Use of the interface by Final Users
Designers (Implementation of improvements)
Easy implementation of the improvements for the Information Security Feedback by means of the HCI-S Criteria like Design Patterns
Reverse Engineering process

Fig. 3. General Process.

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, we think 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 included in the interface of a secure web service could to facilitate the learning and interpretation 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.

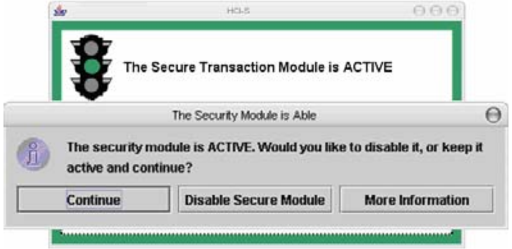
- The security feedback generated could to increase the end users' trust during transactions of personal information, or during the buying and payment of products. This because the end users will be notified appropriately if some security problem is detected.

Fig. 3 graphically depicts a general view of the application of our method. 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.

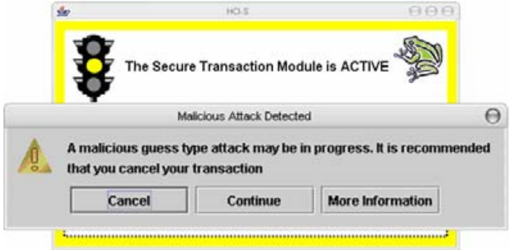
5 Case study

As a case study we considered the next scenario: "It is required an UI that informs users, in a clear manner, about detected threats, and the security features available in a specific application. Furthermore, the security information feedback must include suggested actions to avoid or mitigate the damage caused by some detected threat, as well as provide options to obtain additional information about the detected threat, and the security features of the system". The design of the security feedback required by this specific example was generated applying the most appropriate design patterns of the classification proposed (Fig. 2). The example is illustrated in Table 4.

Table 4. Presentation of the security feedback designed with our method for the case study.

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? **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. A green color 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*").
 HCI-S The Secure Transaction Module is ACTIVE The Security Module is Able The security module is ACTIVE. Would you like to disable it, or keep it active and continue?   **Fig. 4.** Graphical example for solution of the problem: "How to convey the security features of the web service clearly".
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. Fig. 5 shows the appearance of the UI when a "guess" potential threat is detected, in this case, yellow color is used in the frame and in the traffic lights. The interface also 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 speaker at the top right corner of the screen. In this dialogue, a frog sound is generated (a frog sound is mapped to this threat, Table 3) (Application of the design pattern "*Immediate notification of threats*").

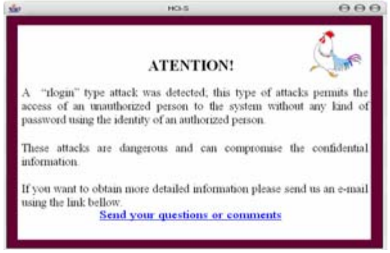


The Secure Transaction Module is ACTIVE

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

Fig. 5. Graphical example for the solution of the problem: "How to present a clear visibility of the system status".

Pattern's Name: Direct navigation, Immediate additional feedback, and Subsequent additional feedback.
Problem: How to present suggested actions to follow in a comprehensible manner?
Solution: The suggested actions are relatively easy to perform and understand. These suggested actions are presented to the users without technical terms and in some cases using graphics, pictures and sounds, in an entertaining manner. The interface also includes the option "More Information" to obtain additional information about some threat. Fig. 6, shows the screen presented when the option "More Information", included in the dialogue boxes, is selected (Application of the design pattern "*Direct Navigation*"). This dialogue shows the information corresponding to an "rlogin" threat (Application of the design pattern "*Immediate additional feedback*"), it is included a link to send an e-mail to obtain more detailed information threat (Application of the design pattern "*Subsequent additional feedback*"). Also an image of the animal related with the threat type and the sound effect is presented at the top right corner of the screen.



ATENTION!

A "rlogin" type attack was detected, this type of attacks permits the access of an unauthorized person to the system without any kind of password using the identity of an authorized person.

These attacks are dangerous and can compromise the confidential information.

If you want to obtain more detailed information please send us an e-mail using the link bellow.

Send your questions or comments

Fig. 6. Graphical example for the solution of the problem: "How to present suggested actions to follow in a comprehensible manner".

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.

It is important to mention that the size of the messages, dialog boxes, and other notifications, presented in figures 4 to 6, were increased to show more clearly the texts of the notification's examples.

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, J. et al. [20], Yurcik, W. et al. [22], Cranor Faith, L. [5,6], Ka-Ping, Y. [16], and McCrickard, S. et al. [17] (Table 5). Table 5 illustrates the criteria performed by each research work. The focus of Rode's proposal [20] 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.

Table 5. Comparison of research works.

Criteria **Researches**	**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. [20]	X	X		
Yurcik et al. [22]	X	X		
Cranor F. [5,6]	X	X		
Ka-Ping [16]	X	X		
McCrickard et al. [17]	X	X		
Current Work	**X**	**X**	**X**	**X**

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, W. et al. [22] try to facilitate the realization of specific activities related to security by means of simple instructions and suggestions offered to the users through the interface elements. The research work presented by Cranor Faith, L. [5,6] proposes 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 in [6], is very similar to the goal of our work; nevertheless, in [6] 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, Y. [16], 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, S. et al. [17] 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 [9, 14, 16, 20, 22], we present a first version of a non-exhaustive classification of information security feedback based in patterns. Our proposal is intended to facilitate the way some security aspects are conveyed to the end user. 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 interactive 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 visual 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 increasing the number of elements of the classification, and improving the classification, to be a component of a formal specification for the feedback of security information design. Also, it is necessary to perform a number of usability studies that consider aspects analyzed in research works such as those presented in [4,21] to 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.

References

1. Atoyan, H., Duquet, J., Robert, J.: Trust in New Decision Aid Systems. In: Proc. of the 18th Int. Conf. of the Association Francophone d'Interaction Homme-Machine IHM’2006 (Montreal, April 18-21, 2006). ACM Press, New York (2006) 115–122

2. Berry, B., Hobby, L. D., McCrickard, S., North, C., Pérez-Quiñones, M. A.: Making a Case for HCI: Exploring Benefits of Visualization for Case Studies. In: Proc. of World Conf. on Educ. Multimedia, Hypermedia & Telecom. EDMEDIA'2006 (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: Proc. of 11th IFIP TC 13 Conf. on Human-Computer Interaction INTERACT'2007 (Rio de Janeiro, September 10-14, 2007). Lecture Notes in Computer Science, Vol. 4663. Springer, Berlin (2007) 114–126
4. Chong Lee, J., McCrickard, S.: Towards Extreme(ly) Usable Software: Exploring Tensions Between Usability and Agile Software Development. In: Proc. of Agile Conference AGILE'2007 (Washington D.C., August 13-17, 2007). IEEE Comp. Soc. Press, 59–71
5. Cranor, L.F.: Designing a Privacy Preference Specification Interface: A Case Study. In: Proc. of ACM CHI'2003 Workshop on Human-Computer Interaction and Security Systems (Fort Lauderdale, April 5-10, 2003). ACM Press, New York (2003)
6. Cranor, L.F., Garfinkel, S.: Security and Usability: Designing Secure Systems that People Can Use. O'Reilly, Sebastopol (2005)
7. DARPA Intrusion Detection Evaluation: Data Sets, Massachusetts Institute of Technology, Lincoln Laboratory, Boston. 1999. Accessible at http://www.ll.mit.edu/IST/ideval/data/ 1998/1998_data_index.html
8. Dass, M.: LIDS: A Learning Intrusion Detection System.B.E. Thesis, Nagpur Univ., (2000)
9. Dhamija, R.: Security Usability Studies: Risk, Roles and Ethics. Proc. of ACM CHI'2007 Workshop on Security User Studies (San Jose, April 28 - May 3, 2007). ACM Press (2007).
10. D'Hertefelt, S.: Trust and the Perception of Security, 2000. Accessible at http://www. interactionarchitect.com/research /report20000103shd.htm
11. Dustin, E., Rasca, J., McDiarmid, D.: Quality Web Systems: Performance, Security, and Usability. Addison-Wesley, New York (2001)
12. García-Ruiz, M., Vargas Martin, M., Kapralos, B.: Towards Multimodal Interfaces for Intrusion Detection. Audio Eng. Society: Pro Audio Expo and Convention (Vienna, 2007)
13. 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, 2004
14. Johnson, M.L., Zurko, M.E.: Security User Studies and Standards: Creating Best Practices. Proc. of ACM CHI'2007 Workshop on Security User Studies (San Jose, April 28 - May 3, 2007). ACM Press, New York (2007)
15. Johnston, J., Eloff, J., Labuschagne, L.: Security and Human Computer Interfaces. Computers & Security 22, 8 (2003) 675–684
16. Ka-Ping, Y.: Secure Interaction Design and the Principle of Least Authority. In: Proc. of ACM CHI'2003 Workshop on Human-Computer Interaction and Security Systems (Fort Lauderdale, April 5-10, 2003). ACM Press, New York (2003)
17. McCrickard, S., Czerwinski, M., Bartramc, L.: Introduction: design and evaluation of notification user interfaces. Int. Journal of Human Computer Studies 58, (2003) 509–514
18. Nielsen, J.: Ten Usability Heuristics, Nielsen & Norman Group, Mountain View (2005). Accessible at http://www.useit.com/papers/heuristic/ heuristic_list.html
19. Reeder, R.W., Karat, C.-M., Karat, J., Brodie, C.: Usability Challenges in Security and Privacy Policy-Authoring Interfaces. In: Proc. of 11th IFIP TC 13 Conf. on Human-Computer Interaction INTERACT'2007. LNCS, Vol. 4663. Springer, Berlin (2007) 141–155
20. Rode, J., Johansson, C., DiGioia, P., Silva Filho, R., Nies, K., Nguyen, D. H., Ren, J., Dourish, P., Redmiles, D.: Seeing Further: Extending Visualization as a Basis for Usable Security. Proc. of 2nd ACM Symposium on Usable Privacy and Security SOUPS'2006 (Pittsburgh, July 12-14, 2006). ACM Press, New York (2006) 145–155
21. Roth, V., Turner, T.: User Studies on Security: Good vs. Perfect. In: Proc. of ACM CHI'2007 Workshop on Security User Studies (San Jose, April 28 - May 3, 2007). ACM P.
22. Yurcik, W., Barlow, J., Lakkaraju, K., Haberman, M.: Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements. In: Proc. of ACM CHI'2003 Workshop on Human-Computer Interaction and Security Systems (Fort Lauderdale, April 5-10, 2003). ACM Press, New York (2003)