Integration of Auditive and Visual Feedback in the Design of Interfaces for Security Applications

Jaime Muñoz[1], Ricardo Mendoza[1], Francisco Álavarez[1], Miguel Vargas Martin[2], Alberto Ochoa[3]

[1] Universidad Autónoma de Aguascalientes, Centro de Ciencias Básicas, Av. Universidad 940, 20100 Ciudad Universitaria Aguascalientes, México. Email: mendozagric@yahoo.com.mx, {jmunozar, fjalvar}@correo.uaa.mx,
[2] University of Ontario Institute of Technology, 2000 Simcoe St. N. Oshawa, Canada, L1H7K4. Email: miguel.vargasmartin@uoit.ca
[3] Instituto Tecnológico de León. Av. Tecnológico S/N Fracc. Ind. Julián de Obregón. C.P. 37290 Apdo. Postal No. 1-857 C.P. 37000
León, Gto. México. Email: megamax8@hotmail.com

Abstract. A well-designed user interface is important for security applications, but it is critical if the adequate use, and the effectiveness of security features, depend on it. Currently, many criteria are available to facilitate the design of a user interface, like the new HCI-S or Security Human Computer Interaction, which is focused in the design of user interfaces for security applications. Similar approaches have emerged recently, such as the use of sonification alerts to notify to the users about malicious attacks either in real time or during the analysis of network logs, in forensics. We present a guide to design an adequate security information feedback, applying the HCI-S criteria to establish the visual notifications, and complementing it with auditive alerts to achieve a better feedback.

Keywords: Feedback, HCI-S, sonification, Malicious Attacks.

1 Introduction

From a computer science perspective, human-computer interaction (HCI) deal with the interaction between one or more humans and one or more computers using the user interface of a program [1]. The concepts of traditional HCI can be used to design the interface or improve some interface currently available, considering aspects like the usability, which determines the ease of use of a specific technology, the level of effectiveness of the technology according to the needs of the user, and the satisfaction of the user with the results obtained by the use of a specific technology by means of performing specific tasks [2].

Security HCI (HCI-S) has recently being introduced (see e.g., Johnston et al. [3]). 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. A standard definition of the HCI-S is inexistent in the current

literature, for that reason we use the definition proposed in [3] which textually says "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". The HCI-S deals with how the security features of the user interface can be as friendly and intuitive as possible, because the easier a system is to use, the less likely the user will be to make a mistake or to try to bypass the security feature obtaining most reliability in the system or in the security technology [3].

Little is known about the best manner to integrate human sensorial channels to perceive some alert by a malicious attack to an information system. The most popular way of notification is the use of visual alerts. Other novel –yet relatively unexplored– techniques exist, such as olfactory, gustative, tactile, and auditive (see e.g., Garcia-Ruiz et al. [4]). After visual, auditive interfaces are probably the most advanced in terms of research work. According to Garcia-Ruiz et al. [4], the sonification has the following advantages:

- Sonification, in theory, should permit to assign a specific sound to a specific attack.
- A particular sound may be identified in a set of auditive alarms.
- Sonification combined with visual notifications permits an efficient sensorial correlation.

Our contribution consists of a set of proposed guidelines to design usable interfaces, combining visualization and sonification to present appropriately the security information feedback of a particular on-line system applying the HCI-S criteria. A number of studies exist about the combination of sonification and visual notification, but these works do not consider the HCI-S design criteria of [3] and do not include a guide to design interfaces combing visual alerts and sonification.

The remaining of this paper is organized as follows. In Section 2 we explain the HCI-S design criteria. In Section 3 we present a description of the problem within the framework of our research work. In Section 4 we describe our proposed guide to design information security feedback. In Section 5, a list of related works is presented. Finally, in Section 6 we present our concluding remarks and provide some directions for future work.

2 HCI-S Design Criteria

For a successful application of the HCI-S's concepts, it is necessary to consider the design criteria proposed by Johnston et al. [3]. These criteria facilitate the design process and the development of usable interfaces used in a security environment. The criteria are based on the ten general principles of the traditional HCI to design user interfaces [5]. The HCI-S design criteria are:

- **Visibility of system status**: The interface 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 interface must avoid the use of technical terms as much as possible. The security interface 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 interface 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 interface 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 use the specific security features in an easier and friendlier way.
- **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 [3] 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.

In the same way, research performed by D'Hertefelt [6], points to six primary factors (fulfillment, technology, seals of approval, presentation, navigation and brand) which convey trust 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

A usable interface is very important for an appropriate feedback, but it is critical if the adequate use, and the effectiveness of security features depend of it. The security features of a specific on-line system must be shown in an easy to understand manner. Bearing in mind previous works, such as those described in [7, 8, 9, 10, 11, and 12], we present a first version of a non-exhaustive classification of information security feedback which is intended to facilitate the way some security aspects are conveyed to the end user. It is well known, that an adequate feedback reduces the possibility that the final users ignores some security notification or other information related with the internal state of the system. The design guidelines are 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).

The proposed design guidelines may complement previous efforts by including sonification and the new HCI-S criteria.

4 A Guide to Design Information Security Feedback

Bearing in mind a basic model for interaction between a user and a system through an interface (see Figure 1). We divide user interaction with the system into three stages, which present a specific notification form when a malicious attack is detected, and when corresponding information of the web-service is required. We propose to incorporate auditive feedback to enhance notifications about malicious attacks.

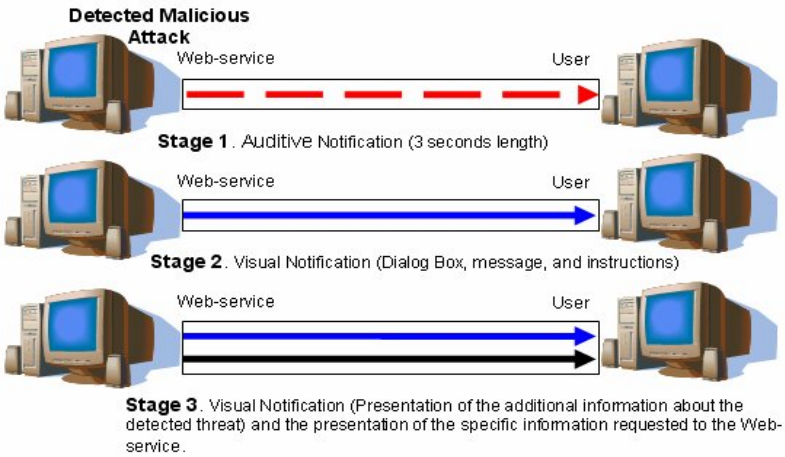

Fig. 1. Basic model for interaction between a user and a server when a malicious attack is detected.

Before continuing, we describe briefly some of the well-known network attacks considering the concepts mentioned in [13].

1. **Guessing rlogin Attack**: Here the intruder tries to guess the password that protects the computer network in order to gain access to it.
2. **Spoofing attack**: The goal of this attack is to usurp an authorized IP address to gain unauthorized access to the victim's system. The IP spoofing attack is often called Blind Spoofing, and is used against communication services taking advantage of their security vulnerabilities (e.g., rsh, rlogin, and rcp attacks). This allows the intruder to hide the origin of the attack (typically used in denial-of-service attacks). DoS attacks typically involve an attacker disabling or rendering inaccessible a network-based information resource.
3. **Scanning Attack**: The intruder goes about scanning different ports of the victim's system to find some vulnerable points from where they can launch other attacks, (e.g., port-scan).

The scanning and the spoofing attacks may be consider more risky, because usually are the preface for other attacks.

The information presented in Table 2, specifies the type of notification about the detection of malicious attacks, based on the definitions mentioned before and the risk level of each attack.

Table 2. Connection between visual and auditive feedback for malicious attacks detection.

Attack Type	Auditive Feedback Stage 1 of the Basic Model for Interaction	Visual Feedback Stages 2 and 3 of the Basic Model for Interaction
Attack attempt by guessing (e.g. guess attack)	Immediate notification to user about some malicious attack detected by means of auditive alerts like: Animal sound effects, musical notes, and beeps, among others.	Notification to user about some malicious attack detected by means of alert messages, images, and additional graphic information.
Attack attempt taking advantages over the security vulnerabilities (e.g. rsh, rlogin, y rcp)	Repetitive notifications to user about some malicious attack detected by means of auditive alerts like: Animal sound effects, musical notes, and beeps, among others.	Notification to user about some malicious attack detected by means of error or alarm messages, images, and changes in the interface appearance, and additional graphic information.
Attack attempt by searching of vulnerable connections (e.g. port-scan)	Repetitive notifications to user about some malicious attack detected by means of, a little more interruptive and specific, auditive alerts like: Animal sound effects, musical notes, and beeps, among others.	Notification to user about some malicious attack detected by means of a little more interruptive and specific error or alarm messages, images, and changes in the interface appearance, and additional graphic information.

Considering the previous points, we propose an alternative to guide designers and programmers in the design process of interfaces for security applications.

The design guide proposed is based in the combination of visual and auditive notifications, applying the HCI-S criteria [3], in a non-exhaustive classification of security information feedback (see Figure 2). The classification is divided in three levels:

- **Informative Feedback**: This level includes the interaction forms useful to notify users about: available security features, the correct way to use these features, detection of malicious attacks, and internal status of the system. It is important to mention, that the sonification of threats is incorporated in this classification's level to inform users in a more effective manner. The communication forms included in this level are related with the feedback specified in the Stage 1 of the model presented in Figure 1.
- **Interactive Feedback**: This level brings together the interaction forms useful to establish the navigation in the interface. This level includes communication forms for enabling or disabling security features, and interaction forms to present suggestions of actions to follow when some threat is detected. The interaction forms of this level are related with the feedback specified in the Stages 2 and 3 of the model presented in Figure 1.
- **Additional Feedback**: This level includes the communication forms related with the request of additional information about detected attacks or related with other security aspects.

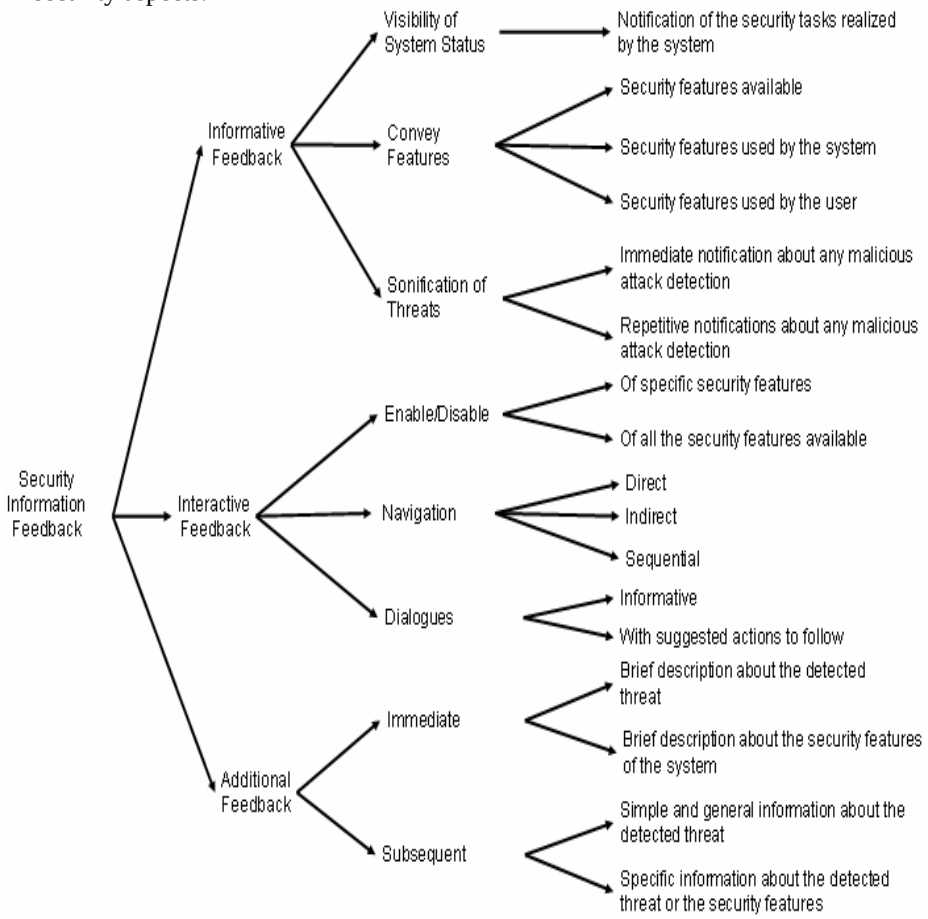

Fig. 2. The first version of our non-exhaustive classification of information security feedback.

The combination of visual alerts and sonification in the proposed design guide has the next advantages, among others, versus those that do not combine these types of notification (see e.g. [10] and [11]):

- 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 attack or error detected.
- Sonification, in theory, should permit to assign a specific sound to a specific attack [4].
- A particular sound may be identified by the users in a set of auditive alarms.
- Sonification combined with visual notifications permits an efficient sensorial correlation [4].

As a simple example of an application of our proposal, consider the next scenario: It is required an interface that informs users, in a clear manner, about detected threats, and the security features available in a specific application. Furthermore, the interface 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.

For this example, we consider the prototype sonification of threats proposed by Garcia-Ruiz et al. [4]; the prototype establishes a relationship between a potential threat and a specific animal sound effect. This relationship was complemented with the assignment of a color to each malicious attack under consideration (see Table 3). It is important to mention that the five potential threats considered by [4] are specified in a network log, this log file is available publicly and was generated by DARPA [14]. The five potential threats are related with the attack types defined previously in this paper (see Table 2).

Table 3. Relationship between color, sound effect, and threat detected.

Color	Sound Effect	Detected Threat
Yellow	Frog	Guess
Orange	Cat	Rcp
Red	Horse	Rsh
Purple	Cock	rlogin
Violet	Bird	Port-scan

Applying each of the six HCI-S design criteria, and choosing the most appropriate feedback forms of the different levels of the classification proposed (see Figure 2), the design of the user interface required by this specific example is described as follows. The design of the user interface is based on [15].

Note: It is important to mention that the size of the messages, dialog boxes, and other notifications, in the following figures, were increased to show clearly the texts of the notification's examples. In the same way, some screens of the interface are not presented to avoid redundancy; this because the same design idea is applied in all the screens that conform the user interface proposed.

1. **Convey Features:** 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. Figure 3 presents a screen of the interface. 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 communication form "*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 communication form "*Notification of the security tasks realized by the system*"). 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 communication form "*Enable/Disable of all the security features available*".

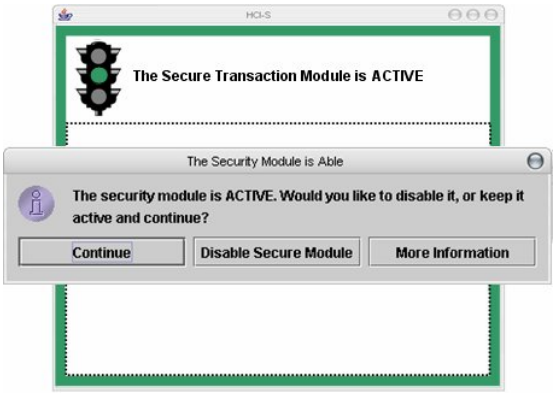

Fig. 3. Graphical example for the explanation presented in point "Convey Features".

2. **Visibility of system status**: 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 attack, and also, as well as a link to obtain additional information. Figure 4, shows the appearance of the user interface when a "guess" potential attack 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 communication form "*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 attack, see Table 3) (Application of the communication form "*Immediate notification about any malicious attack*").

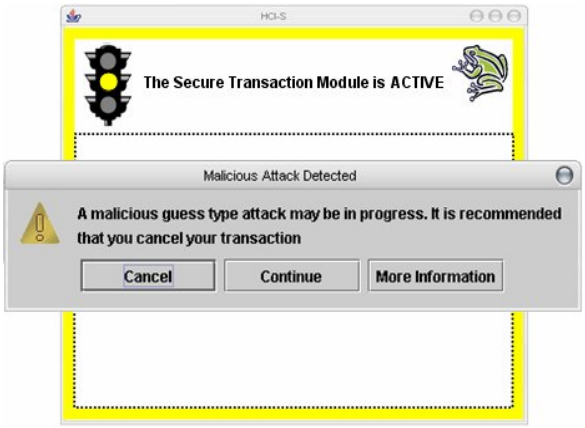

Fig. 4. Graphical example for the explanation presented in point "Visibility of the System Status".

3. **Learnability:** The interface is easy to learn and friendly because the use of colors in the frame that notify about some attack detected and the use of real-world metaphors such as traffic lights. The interface also uses animal sound effects to distinguish among detected attacks, and an image of the animal related with the attack type and the sound effect is presented at the top right corner of the screen.
4. **Aesthetic and minimalist design**: The interface 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 attacks, and the color of the interface's frame and the traffic lights complement an easy to use interface.
5. **Satisfaction:** 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 malicious attack. Figure 5, shows the screen presented when the option "More Information", included in the dialogue boxes, is selected (Application of the communication form "*Direct Navigation*"). This dialogue shows the information corresponding to an "rlogin" attack (Application of the communication form "*Simple and general information about the detected threat*"), it is included a link to send an e-mail to obtain more detailed information attack (Application of the communication form "*Specific information about the detected threat or the security features*"). Also an image of the animal related with the attack type and the sound effect is presented at the top right corner of the screen. A similar screen is presented for the rest of the attacks when additional information is required.

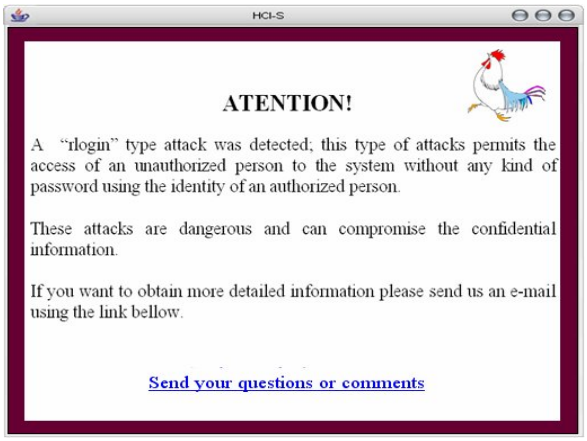

Fig. 5. Graphical example for the explanation presented in point "Satisfaction".

6. **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 attack. The users know, by means of the interface's elements, that their information has being protected by the security features of the system.

5 Related Work

In this section we present some of the most significant work related to ours. We use the following criteria to compare these researches in order to detect the advantages and disadvantages between them and our research:

- 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.

We have considered the research works of: Rode, J. et al. [9], Yurcik, W. et al. [10], Cranor Faith, L. [11], Ka-Ping, Y. [12], McCrickard, S. et al. [16], (see Table 4).

Table 4. 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, J. et al. [9]	X	X		
Yurcik, W. et al. [10]	X	X		
Cranor Faith, L. [11]	X	X		

Ka-Ping, Y. [12]	X	X		
McCrickard, S. et al. [16]	X	X		

Table 4 illustrates the criteria performed by each research work. The focus of the proposal of Rode, J. et al. [9], 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 whether or not a system is secure enough for their immediate needs. 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. [10] 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. [11] 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 in [11], is very similar to the goal of our work; nevertheless, in [11] sonification is not considered, nor is the incorporation of the HCI-S criteria.

The research of Ka-Ping, Y. [12], 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 the same way, McCrickard, S. et al. [16], 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 researches mentioned above. With the research work presented in this paper we try to perform the five comparative criteria (see Table 4), and thus provide a complement for other research works.

6 Concluding Remarks and Future Work

With the proposed design guide is possible to achieve an appropriate feedback through the elements of the interface by means of visual and auditive notifications about information related with the security and the internal state of a particular on-line system. In the same way, the guidelines are oriented to generate interfaces easy to understand and interpret by users with different experience and backgrounds (experts, advanced, and beginners) avoiding, as much as possible, the use of technical terms in the security information presented to the users.

There are several aspects to explore as future work, like 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, bearing in mind aspects analyzed in research works like [17, 18, 19] to evaluate in a formal manner our proposal and enhance it.

References

1. 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", URL: http://www.acm.org/sigchi/cdg/cdg2.html, 2004. [Accessed: 2006-09-27].
2. Flores, B., Ibarra, J., Rodríguez, J.: El Rol de la Cibermetría en el Diagnóstico de Usabilidad de Sitios Web. Memorias de la V Jornada Iberoamericana de Ingeniería de Software Ingeniería del Conocimiento JIISIC Puebla, México (2006) 175-181
3. Jonston, J., Eloff, J., Labuschagne, L.: Security and human computer interfaces. Computers & Security Vol. 22, Elsevier Ltd, No 8 0167-4048/03 (2003) 675-684
4. García-Ruiz, M., Vargas Martin, M., Kapralos, B.: Towards Multimodal Interfaces for Intrusion Detection. Audio Engineering Society: Pro Audio Expo and Convention. Vienna, Austria (2007)
5. Nielsen, J.: Ten Usability Heuristics, 2005. URL: http://www.useit.com/papers/heuristic/ heuristic_list.html [Accessed: 2006-10-12]
6. D'Hertefelt, S.: Trust and the Perception of Security, 2000. URL: http://www.interaction architect.com/research /report20000103shd.htm [Accessed: 2007-02-9]
7. Dhamija, R.: Security Usability Studies: Risk, Roles and Ethics. Position Paper for Workshop on Security User Studies, part of the ACM CHI 2007 conference. San Jose, California, USA, April 28 – Mayo 3, (2007)
8. Johnson, M. L., Zurko, M. E.: Security User Studies and Standards: Creating Best Practices. Workshop on Security User Studies, part of the ACM CHI 2007 conference. San Jose, California, USA, April 28 – Mayo 3, (2007)
9. 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. Symposium on Usable Privacy and Security (SOUPS). Pittsburgh, PA, Julio 12-14, (2006)
10. Yurcik, W., Barlow, J., Lakkaraju, K., Haberman, M.: Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements. Workshop on Human-Computer Interaction and Security Systems part of CHI 2003. Fort Lauderdale, Florida, April 5-10, (2003)
11. Cranor Faith, L.: Designing a Privacy Preference Specification Interface: A Case Study. Workshop on Human-Computer Interaction and Security Systems part of CHI 2003. Fort Lauderdale, Florida, April 5-10, (2003)
12. Ka-Ping, Y.: Secure Interaction Design and the Principle of Least Authority. Workshop on Human-Computer Interaction and Security Systems part of CHI 2003. Fort Lauderdale, Florida, April 5-10, (2003).
13. Dass, Mayukh.: LIDS: A Learning Intrusion Detection System. Thesis. B.E., Nagpur University, India (2000)
14. Massachusetts Institute of Technology Lincoln Laboratory. DARPA Intrusion Detection Evaluation: Data Sets, 1999. URL: http://www.ll.mit.edu/IST/ideval/data/1998/1998_data_ index.html [Accessed: 2007-02-16]
15. Mendoza, R., Muñoz, J., Álvarez, F., Vargas Martin, M.: Monitoreo del Desempeño de los Factores de Seguridad de una Transacción Web a través de la Interfaz de Usuario. VI

Jornada Iberoamericana de Ingeniería de Software Ingeniería del Conocimiento JIISIC, Lima, Perú, (2007) 275-282
16. McCrickard, S., Czerwinski, M., Bartramc, L.: Introduction: design and evaluation of notification user interfaces. International Journal of Human Computer Studies No 58, Elsevier Science Ltd, (2003) 509-514.
17. Chong Lee, J., McCrickard, S.: Towards Extreme(ly) Usable Software: Exploring Tensions Between Usability and Agile Software Development. Agile Conference. Washington D.C., USA, August 13-17, (2007).
18. Roth, V., Turner, T.: User Studies on Security: Good vs. Perfect. Workshop on Security User Studies, part of the ACM CHI 2007 conference. San Jose, California, USA, April 28 – May 3, (2007).
19. 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. World Conference on Educational Multimedia, Hypermedia & Telecommunications EDMEDIA. Orlando, Florida, USA, June 26-30, (2006).