Chapter 26
A Method to Design Information Security Feedback Using Patterns and HCI-Security Criteria

Jaime Muñoz-Arteaga, Ricardo Mendoza González, Miguel Vargas Martin, Jean Vanderdonckt, Francisco Álvarez-Rodriguez and Juan González Calleros

Abstract 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.

26.1 Introduction

The term "user feedback" is often referred to as to any form of communication directed from a system toward 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.

J. Muñoz-Arteaga (✉), R. Mendoza González (✉), M. Vargas Martin, J. Vanderdonckt, F. Álvarez-Rodriguez and J.G. Calleros
Universidad Autónoma de Aguascalientes, Centro de Ciencias Básicas, Av. Universidad, 940, 20100 Ciudad Universitaria Aguascalientes, Mexico
e-mails: jmunozar@correo.uaa.mx, mendozagric@yahoo.com.mx

V. López-Jaquero et al. (eds.), *Computer-Aided Design of User Interfaces VI*,
DOI: 10.1007/978-1-84882-206-1_26,

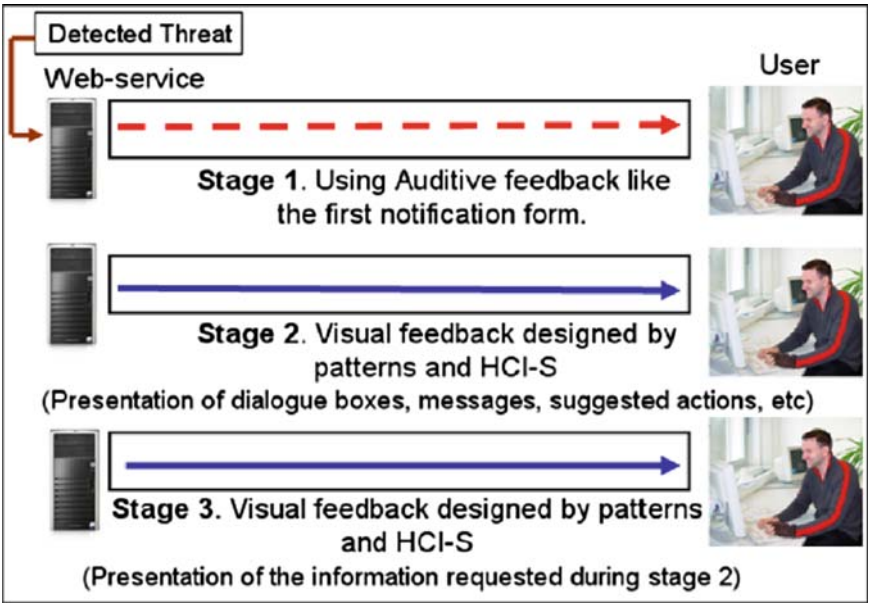

Fig. 26.1 Our model is divided into three stages: first, an additional notification form is triggered to notify end user about some security threat, possibly augmented with auditive notifications or any other kind of feedback; then, the visual feedback is effectively designed based on the design patterns that are explicitly based on HCI-S criteria; finally, the feedback is constructed

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.

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 (see Fig. 26.1).

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.

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. Subheading 26.2 explains the HCI-S design/evaluation criteria. Subheading 26.3 describes the general problem within the framework of our research work. Subheading 26.4 defines the steps of the method for designing information security feedback that is then applied in a case study in Subheading 26.5. Subheading 26.6 compares this work with respect to other relevant and related

works. Finally, Subheading 26.7 summarizes our concluding remarks and provides some potential avenues for future work.

26.2 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.).
- 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.
- 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 pictures 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 pictures or draws.
- Learnability: The UI needs to be as nonthreatening and easy to learn as possible; it may be accomplished using real-world metaphors, or pictures of keys and padlocks.
- 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."

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 26.1. 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.

26.3 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 and Zurko [14], a usable security information feedback could reduce possible errors caused by final users when important notifications are ignored, nevertheless 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

Table 26.1 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	Appropriate notification of available security features using a minimalist Web site design. This leads to a more satisfying experience for the users
Aesthetic and minimalist design	Presentation, navigation	The users must be appropriately informed about which security features are available, and when these are being used
Learnability	Navigation	A Web site with a minimalist design is easier to use and navigate
Satisfaction	Fulfillment, Presentation	A Web site that is easy to navigate is also easy to learn by the users

enough [9, 14, 19, 20]. Another problem may be the insufficient consideration of the end users by the current design specifications. Braz et al. [3] demonstrated the importance of finding equilibrium between security and usability. Nevertheless, most of the security researches do 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. An adequate feedback is necessary to reduce the possibility that the final users misunderstand security notifications or other information related with the internal state of the system [2, 5, 14, 22]. Our classification is oriented toward the design of a usable security information feedback, easy to understand and interpret by users with different experience and backgrounds (experts, advanced, and beginners).

26.4 Designing Security Feedback Using Patterns and HCI-S Criteria

It is well known that secure Web services must keep informed their end user about the internal state of the system and the technologies used by the system to protect confidential information during a transaction. We propose a classification of interactive patterns based on HCI-S criteria intended to design a usable security information feedback (Fig. 26.2).

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.
- Interaction feedback: This level brings together the interaction forms useful to establish the feedback's navigation and operation.
- 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]. We complement such relationship with visual notifications, assigning a specific color to each threat under consideration (Table 26.2). 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]. We also bear in mind the explanation of these threats presented by Dass [8].

To present a general view of our classification, we define some of the interactive patterns presented in Fig. 26.2, considering a possible recurrent problem

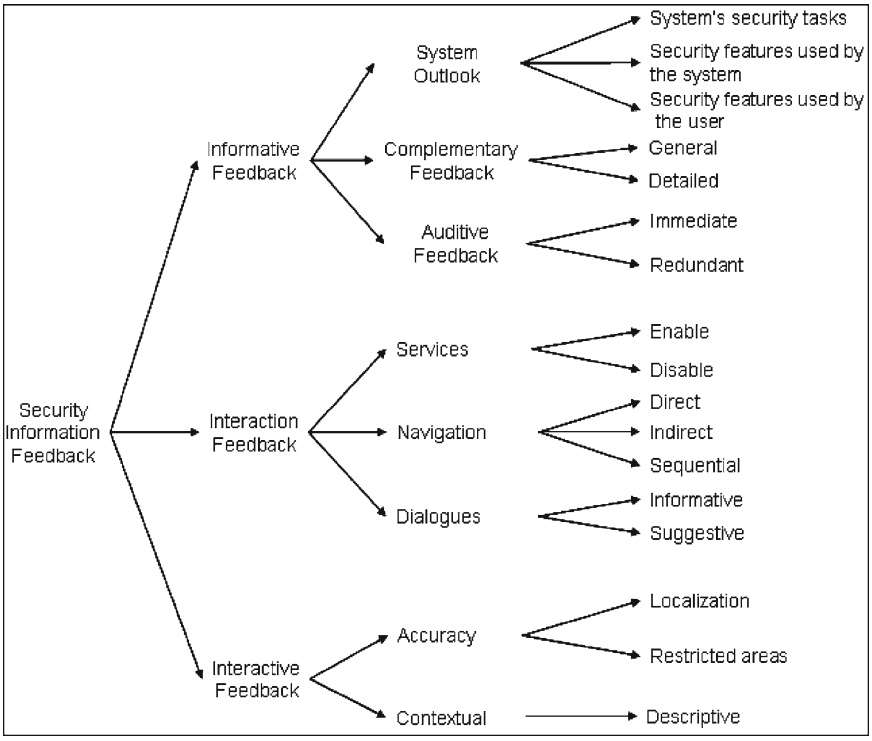

Fig. 26.2 Classification of audiovisual interactive patterns

Table 26.2 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

Table 26.3 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 give to the end users more control over the system?	By giving in specific notifications presented to the end users the option to disable the security features or to continue using it	Disabling 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, 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 passes the mouse's cursor over a specific element of the security information feedback	Descriptive

based on the HCI-S criteria, and a suggested solution offered by the patterns (Table 26.3; Fig. 26.3).

We consider that our proposal could facilitate, to designers and programmers, the planning and construction of a usable security information feedback, which could make easier for end users the comprehension and use of the security features

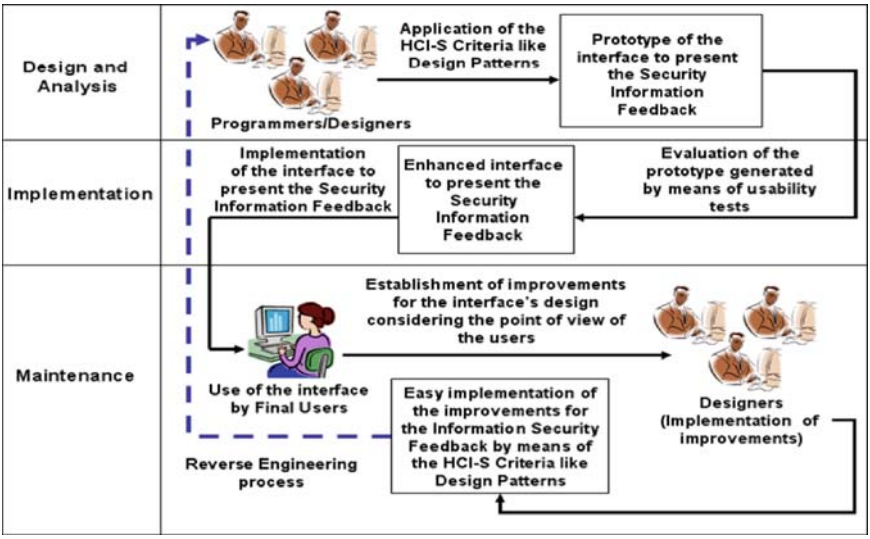

Fig. 26.3 This figure graphically depicts a general view of the application of our method. The graphical model is divided in three basic stages to represent an alternative collaboration between three types of users (end users, programmers, and designers) to improve security information feedback of a secure Web service

available in a specific secure Web service. Other advantages of the application of our proposal are that the implementation of the improvements could be easy and quick, for designers and programmers, because the feedback was originally generated by means of design patterns and considering the HCI-S criteria.

26.5 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. 26.2). The example is illustrated in Figs. 26.4 and 26.5. We complement this example with the specification of the patterns used.

1. *Patterns*: 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

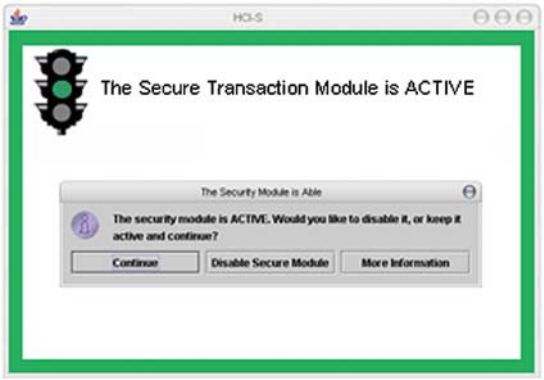

Fig. 26.4 Here is presented a graphical example. A green color is used in the frame and in the traffic lights to indicate the users that the system is protected (application of the design pattern "*Security features used by the system*"). The text "The Secure Transaction is ACTIVE" is always visible, being another 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*")

Fig. 26.5 This graphic 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, Table 26.2); yellow color 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–color–sound–picture relation (see Table 26.2)

and the message "The Security Module is ACTIVE," the users will be alerted about the protection of the system.
2. *Patterns*: 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 a sound alarm, changing the color of the interface's frame and the traffic lights, 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, as well as a link to obtain additional information.

The security feedback designed for this case study also was considered and it 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.
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.
3. *Trust*: The interface may help to achieve that the user trusts in a system, through adequate notifications, and clear suggested actions to prevent or mitigate the damage caused by the threat.

It is important to mention that the size of the messages, dialog boxes, and other notifications, presented in Figs. 26.4 and Fig. 26.5, was increased to show more clearly the texts of the notification's examples.

26.6 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. [20], Yurcik et al. [22], Cranor et al. [5, 6], Ka-Ping [16], and McCrickard et al. [17] (Table 26.4). Table 26.4 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. 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 have not considered the HCI-S design criteria, or the incorporation of sonification, which may complement this research. Similarly the work of Yurcik et al. [22] tries to facilitate the realization of specific activities related to security by means of

Table 26.4 Comparison of research works

Criteria Researches	Proposal of usable security information feedback	Presentation of security aspects to the users	Consideration of 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 et al. [5, 6]	X	X	–	–
Ka-Ping [16]	X	X	-	–
McCrickard et al. [17]	X	X	–	–
Current work	X	X	X	X

simple instructions and suggestions offered to the users through the interface elements. The research work presented by Cranor et al. [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 [16] consists of the proposal of a model of ten points to represent the interaction of the users with secure systems. The model is based on actors and their abilities, and it provides the actors some authority to assist users in determining whether a particular action is secure or not. In a similar way, McCrickard et al. [17] propose a very interesting strategy to design and evaluate usable feedback but do not consider 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 earlier. With the research work presented in this paper we try to perform the four comparison criteria (Table 26.4), and thus provide a complement for other research works.

26.7 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 nonexhaustive 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. Lee, J.C., McCrickard, S.: Towards Extreme(ly) Usable Software: Exploring Tensions Between Usability and Agile Software Development. In: Proc. of Agile Conference AGILE'2007 (Washington, DC, August 13–17, 2007). IEEE Comp. Soc. Press (2007) 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 University, Nagpur (2000).
9. Dhamija, R.: Security Usability Studies: Risk, Roles and Ethics. In: Proc. of ACM CHI'2007 Workshop on Security User Studies (San Jose, April 28 – May 3, 2007). ACM Press, New York (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. In: 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, New York (2004). Accessible at http://www.acm.org/sigchi/cdg/cdg2.html.
14. Johnson, M.L., Zurko, M.E.: Security User Studies and Standards: Creating Best Practices. In: 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. *Comput 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 J Hum Comput Stud* 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. In: Proc. of Second 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 Press, New York (2007).
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).