A Classification of Security Feedback Design Patterns for Interactive Web Applications

Jaime Muñoz-Arteaga
Universidad Autónoma de Aguascalientes Centro de Ciencias Básicas, Av. Universidad 940 20100, Ciudad Universitaria, Aguascalientes (Mexico)
jmunozar@correo.uaa.mx

Ricardo Mendoza González
Universidad Autónoma de Aguascalientes Centro de Ciencias Básicas, Av. Universidad 940 20100, Ciudad Universitaria, Aguascalientes (Mexico)
mendozagric@yahoo.com.mx

Jean Vanderdonckt
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

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 two or more channels required to achieve an effective feedback in case of a security issue are explicitly incorporated in the development life cycle. With this proposal we intend to complement previous efforts finding equilibrium between usability and security for interactive web applications.

1. Introduction

The term "feedback" is often referred as any form of communication directed from a system towards the user. In a similar way, information security feedback is any information related with 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 consist in 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 [21]. 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 of a specific technology to perform specific tasks.

Security HCI (HCI-S) has recently being introduced [14] 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. A standard definition of HCI-S is inexistent in the current literature. Therefore, we use the definition proposed in [14] 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 with Johnston et al. [14], 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 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.

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 (Figure 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 composed.

978-0-7695-3189-2/08 $25.00 © 2008 IEEE
DOI 10.1109/ICIMP.2008.21

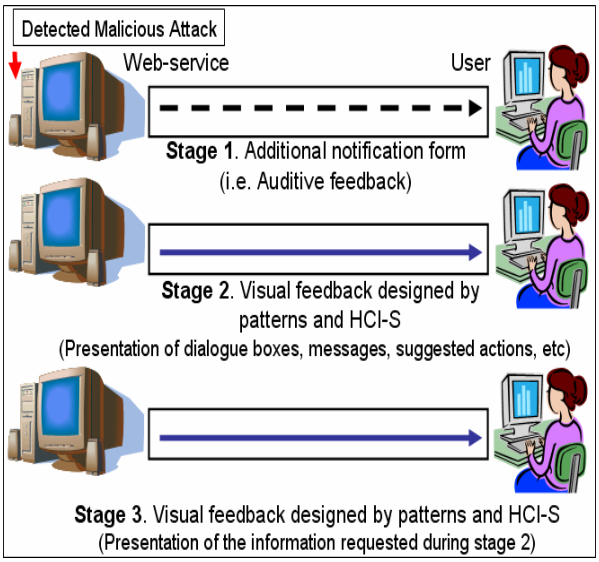

Figure 1. Audiovisual feedback when a threat is detected.

Using auditive notification like additional feedback benefits from the following advantages versus those alerts that do not combine visual and auditive channels:

- 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, and permits an efficient sensorial correlation [12].
- Auditive feedback, in theory, should permit to assign a specific sound to a specific threat [12].
- A particular sound may be identified by the users in a set of auditive alarms [12].

So far, the importance of integrating security and usability in the UI development life cycle has been widely recognized [3,11,14] both from the user studies point of view [13] and the usability challenges posed by this integration [18]. 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 [3,6,9,19], but their effective integration remains the designer's responsibility.

In order to address this shortcoming, this paper introduces a method for designing usable user feedback based on user interface 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 further applied in a case study in Section 5. Section 6 locates this work with respect to the state of the art. Section 7 summarizes our concluding remarks and provides some avenues for future work.

2. HCI-S Design/Evaluation Criteria

For a successful application of the HCI-S's concepts, it is necessary to consider the design criteria proposed by Johnston et al. [14]. These criteria facilitate developing usable interfaces that are used in a security environment, based on Nielsen's heuristics traditionally used for heuristic evaluation [13].

- **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 [9] 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.

3. Problem outline

We believe that usable security information feedback could reduce possible errors caused by end 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 [5,6,8,15]. Another problem may be the insufficient consideration of the end users by the current web services specifications (i.e. WS-Security specification) [22]. These problems could be mitigated by means of including HCI-S criteria like patterns in WS-Security specification.

Braz et al. [2] 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. According to 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 end users misunderstand security notifications or other information related with the internal state of the system [5,13,20].

Our proposal is oriented towards the design of a usable security information feedback for secure web-services. In addition, the proposal may complement previous efforts by including the new HCI-S criteria like design patterns.

4. Classification of security feedback design patterns

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 (Figure 2).

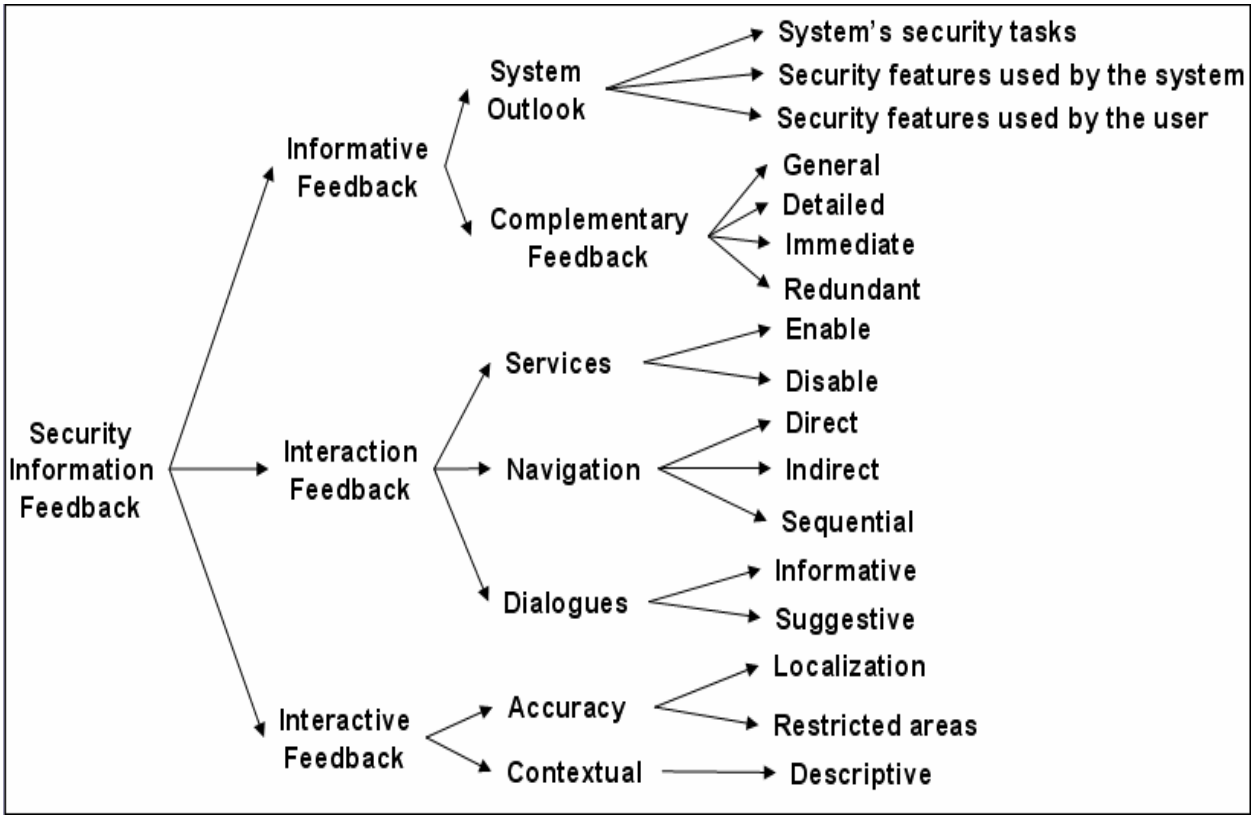

Figure 2. Classification of security feedback design patterns for interactive web applications.

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

- **Informative Feedback**: This level includes the design 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 design 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 design 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.

In order to provide a general view of the proposed set of patterns we describe some of them in Table 1. For this description we consider a suggested solution offered by the patterns, and a possible recurrent problem related.

Table 1. 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 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 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 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

5. Case study

In order to exemplify the application of the design concepts offered by the set of patterns proposed we consider the following scenario: It is required an UI that informs users, clearly, about detected threats, and the security features available in a generic e-commerce site. 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.

The e-commerce site of the DAN'S Comp store (http://www.danscomp.com/) was used in this study case just to provide an example. We show the possible appearance of the site after the application of our proposed set of patterns (see Table 2).

Table 2. Example for the application of the patterns proposed.

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 and the message "The Security Module is ACTIVE" the users will be alerted about the protection of the system. Figure 3 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*").

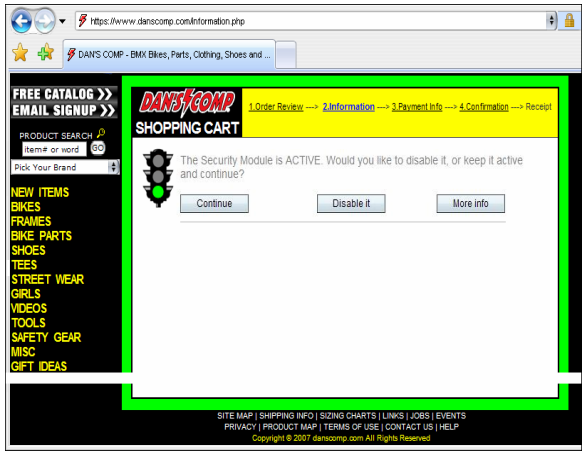

Figure 3. Graphical example .

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 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 UI 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 design pattern "*Dialogue with suggested actions to follow*").

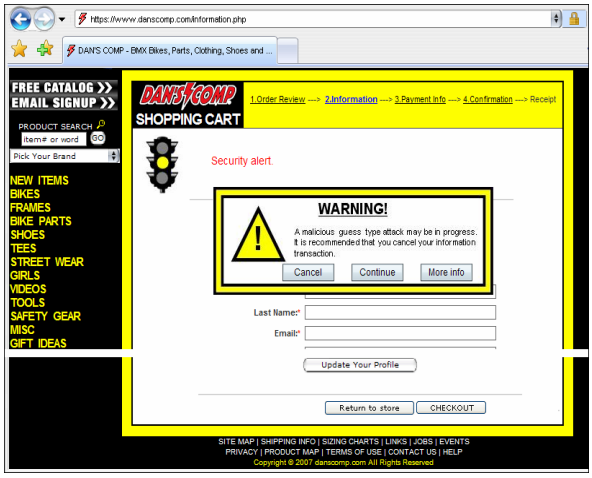

Figure 4. Graphical example.

6. Related Work

In this section we present some of the most significant work related. 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 additional feedback forms to reinforce visual notifications.

We have considered the research works of: Rode, J. et al. [20], Yurcik, W. et al. [20], Cranor Faith, L. [5,6], Ka-Ping, Y. [15], McCrickard, S. et al. [16]. Table 4 illustrates the criteria performed by each research work.

The focus of Rode's proposal [19] 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. Similarly Yurcik et al. [20] 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. Cranor [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 research of Ka-Ping, Y. [15], 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. McCrickard, S. et al. [16] propose a very interesting strategy to design and evaluate usable feedback, but do not considered the HCI-S criteria.

In general terms, we believe that, the incorporation of HCI-S criteria like design patterns, and two or more feedback forms, could enhance the usability in the mentioned researches.

With the research work presented in this paper, we try to perform the five comparative criteria (Table 3), and thus provide a complement for other research works.

7. Concluding remarks and future work

We present a first version of a non-exhaustive classification of security feedback design patterns for

interactive web applications. Our proposal is intended to facilitate the way some security aspects are conveyed to the end user. With this alternative is possible to achieve an appropriate feedback using HCI-S design/evaluation criteria like patterns. Additionally, the set of patterns proposed suggest the use of additional feedback forms to increase the usability in the feedback designed. In the same way, the security feedback designed could be easily interpreted by users with different experience and backgrounds (experts, advanced, and beginners).

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 that consider aspects analyzed in research works such as those presented in [3,16] to formally evaluate our proposal.

In the near future, we also would like to investigate how other interaction modalities (e.g., sound, speech, or haptic feedback) could complement or supplement the existing ways to provide feedback to the end users.

8. References

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

[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", *World Conf. on Educ. Multimedia, Hypermedia & Telecom, EDMEDIA'06*, Orlando, June 26-30, 2006.

[3] Braz, C., Seffah, A., M'Raihi, D.: "Designing a Trade-off between Usability and Security: A Metrics Based-Model", *11th IFIP TC 13 Conf. on Human-Computer Interaction INTERACT'2007*, Rio de Janeiro, September 10-14, LNCS, Vol. 4663. Springer, Berlin, 2007, pp. 114–126, 2007.

[4] Chong Lee, J., McCrickard, S.: "Towards Extreme(ly) Usable Software: Exploring Tensions Between Usability and Agile Software Development", *Agile Conference AGILE'07*, Washington D.C., August 13-17, IEEE Comp. Soc. Press, pp. 59–71, 2007.

[5] Cranor, L.F.: "Designing a Privacy Preference Specification Interface: A Case Study", *ACM CHI'2003 Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, April 5-10, 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, MIT Lincoln Laboratory, Boston, 1999.

[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", *ACM CHI'2007 Workshop on Security User Studies*, San Jose, April 28 - May 3, ACM Press, 2007.

[10] D'Hertefelt, S.: "Trust and the Perception of Security",

2000. Accessible at: http://www. Interactionarchitect.com .research/

[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] Johnson, M. L., Zurko, M.E.: "Security User Studies and Standards: Creating Best Practices", *ACM CHI'2007 Workshop on Security User Studies*, San Jose, April 28 - May 3, ACM Press, New York, 2007.

[14] Johnston, J., Eloff, J., Labuschagne, L.: "Security and Human Computer Interfaces", *Computers & Security 22, Vol. 8*, pp. 675–684, 2003.

[15] Ka-Ping, Y.: "Secure Interaction Design and the Principle of Least Authority", *ACM CHI'03 Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, April 5-10, ACM Press, New York, 2003.

[16] McCrickard, S., Czerwinski, M., Bartramc, L.: "Introduction: design and evaluation of notification user interfaces", *Int. Journal of Human Computer Studies, Vol. 58*, 2003.

[17] Nielsen, J.: "Ten Usability Heuristics, Nielsen & Norman Group", Mountain View, 2005. Accessible at http://www.useit.com/papers/heuristic/ heuristic_list.html

[18] Reeder, R.W., Karat, C., Karat, J., Brodie, C.: "Usability Challenges in Security and Privacy Policy-Authoring Interfaces", *11th IFIP TC 13 Conf. on Human-Computer Interaction INTERACT'07*. LNCS, Vol. 4663. Springer, Berlin, pp. 141–155, 2007.

[19] 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", *ACM Symposium on Usable Privacy and Security SOUPS'06*, Pittsburgh, July 12-14, ACM Press, New York, pp. 145–155, 2006.

[20] Yurcik, W., Barlow, J., Lakkaraju, K., Haberman, M.: "Two Visual Computer Network Security Monitoring Tools Incorporating Operator Interface Requirements", *ACM CHI'03 Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, April 5-10, ACM Press, New York, 2003.

[21] 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.

[22]White, J. "Security in a Web-services World: A Proposed Architecture and Roadmap", Technical Report, April, 2002.