Web Service-Security Specification based on Usability Criteria and Pattern Approach

Ricardo Mendoza González[1]
[1]Universidad Autónoma de Aguascalientes/Centro de Ciencias Básicas, Aguascalientes, México
Email: mendozagric@yahoo.com.mx

Miguel Vargas Martin[2], Jaime Muñoz Arteaga[1], Francisco J. Álvarez Rodríguez[1] and Carlos A. Ochoa Ortíz Zezzatti[3]
[2]University of Ontario Institute of Technology/2000 Simcoe St. N. Oshawa, L1H7K4, Canada
Email: miguel.vargasmartin@uoit.ca
[1]Universidad Autónoma de Aguascalientes/Centro de Ciencias Básicas, Aguascalientes, Mexico
Email: {jmunozar, fjalvar}@correo.uaa.mx
[3]Universidad Autónoma de Ciudad Juárez/Dep. de Ingeniería Eléctrica y Computación, CD. Juárez, Chihuahua, Mexico
Email: megamax8@hotmail.com

***Abstract*—A specification is provided in this paper to assist in the design of usable and secure web-services. In particular, this specification helps design an adequate security information feedback based on User Interface Patterns, the resulting visual feedback is then evaluated against a set of design/evaluation criteria called Human-Computer Interaction for Security (HCI-S). In addition we propose in a theoretical manner including the knowledge offered by the proposed specification based on patterns in a new level for the architectural structure of WS-Security specification, which is currently one of the most popular specifications to establish secure web services.**

***Index Terms*—user feedback, HCI-S, WS-Security, usability, secure web services, design patterns.**

I. INTRODUCTION

The term "user feedback" is often referred to as to any form of communication directed from a system to the user [32]. Similarly, information security feedback is any information related with the system's security conveyed to the end user. It is very important that this feedback is displayed through a well-designed user interface. Currently, many resources are available to facilitate the design of a user interface, like the new Security Human Computer Interaction (HCI-S), which is focused in the design of user interfaces for security applications. Nevertheless many of these criteria have not been considered by most of the secure web services specifications. Ka-Ping [18] establishes that security of any computer system that is configured or operated by human beings critically depends on three principal aspects: A) Information conveyed by the user interface. B) The decisions of the users. C) The interpretation of the user's actions. The aforesaid aspects are extremely related with the concept of usability. Usability determines the following points: The ease of use of a specific technology, the level of effectiveness of the technology according to the needs of the user, the satisfaction of the user with the results obtained by the use of a specific technology by means of performing specific tasks. As described in [18]; currently there is a common assumption that security and usability are typically in conflict. Nevertheless, there are a number of proposals that refute this conflict, by means of including design principles for secure systems such as the "Principle of Least Authority". The principle of least privilege or least authority was originally introduced by Saltzer et al. [29]; it states that each system component should be granted the least authority necessary to perform its function. It has long been accepted that this simple principle is fundamental to security at the system level; it is important to recognize that it is also fundamental to usability for secure systems. Similarly, notification systems attempt to present, in an effective manner, important information to the final users. The success of these systems depends on the final users understanding the notifications shown through the interface [19]. For that reason, an adequately designed interface could increase the possibility of notification system's success.

HCI-S has being introduced in [17]. The concept of HCI-S modifies and adapts the concepts of the traditional, Human-Computer Interaction (HCI) to focus in aspects of security and to find how to improve security through the elements of the interface. Johnston et al. [17] suggest a definition of HCI-S 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 [17], the HCI-S deals with how the security features of the user interface can be as friendly and intuitive as possible. 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. This adds to the integrity of a system. HCI-S's goal is to improve the interface in order to improve the security. This leads to the system becoming more secure, robust and reliable.

Our contribution consists of a set of concepts to design usable information security feedback, combining the concept of user interface patterns and HCI-S design/evaluation criteria. These concepts will be included in a proposed new element for WS-Security specification originally presented by White [30].

In following Subsections *A* and *B* respectively we present an overview of WS-Security and HCI-S. And Subsection *C* describes the general problem within the framework of our research work.

A WS-Security

According to White [30], and Hondo et al. [15]; a number of specifications have recently been proposed to explain the implementation of security models for web services. Furthermore, some proposals are available to improve the aforementioned specifications incorporating elements like WS-Policy, WS-Policy Framework, WS-Policy Attachments, WS-Policy Assertions, WS-Secure Conversation, and WS-Trust, which correspond to the WS-Security specification (see Figure 1)

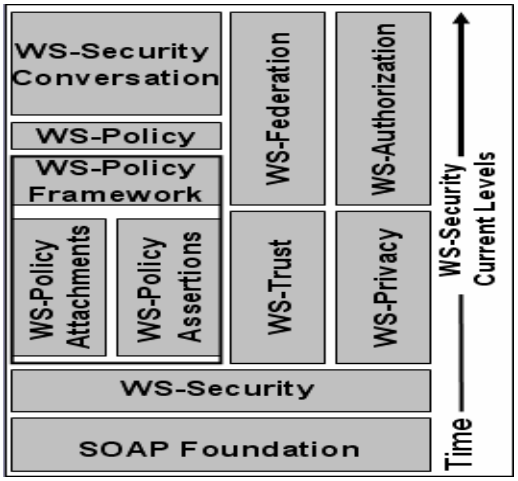

Figure 1. WS-Security current architecture. Adapted of [30].

In WS-Security (see Fig. 1) WS-Federation, describes how to manage and broker the trust relationships in a heterogeneous federated environment including support for federated identities. WS-Authorization describes how to manage authorization data and authorization policies. Providing security for WS-Security requires due diligence in the production of the descriptions, specification and profiles in a number of functional areas. These documents will change and evolve through a process that balances the needs of customers with the needs of the Web services development community.

As explained in the literature [3, 15, 30], the policy element WS-Policy has been further refined to include four documents: (1) A Policy Framework (WS-Policy), document that defines a grammar for expressing web services policies; (2) A Policy Attachment (WS-Policy-Attachment), which defines how to attach these policies to web services; (3) A set of general policy assertions (WS-Policy-Assertions); and (4) A set of security policy assertions (WS-Security Policy). The Policy Framework allows extensibility. Policy is a broad term and encompasses a range of disciplines such as security, reliability, transactions, and privacy. Similarly, the ability to express policies is not limited to the expression of general policies or security policies. The intent is for the basic policy framework to accommodate the expression of domain specific policy languages in a way that leverages different domain knowledge within a consistent web Services Framework. The Policy Framework has two additional elements, WS-Policy Attachment, which offers several ways to advertise policy assertions with Web services. It builds on the existing web Services Description Language (WSDL) and Universal Description Discovery and Integration (UDDI) specifications but also supports extensibility. And the WS-Policy Assertions, which offers a type of common policy expression. It defines a generic set of policy assertions for web services. Security is one domain and to illustrate the expression of security policies, a separate document, WS-Security-Policy proposes a language to express policies needed to communicate such policies related to supporting the WS-Security specification. It is important mention that the trust between a service requester and a service provider is established through the exchange of information between the two parties in an expected and understood manner. The WS-Security specification already defines the basic mechanisms to securely exchange messages using security tokens. The element WS-Trust builds on this model by defining how such security tokens are issued and exchanged. Finally, the element WS-Secure Conversation, builds on this concept of trust based on security tokens. It describes how security tokens can be used within the context of policy-defined trust relationships to allow multiple service requesters and service providers to securely exchange information over the duration of a conversation.

While WS-Trust defines the behavior of overall trust relationships, WS-Secure Conversation focuses on defining a security context (security token) for secure communications.

B 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. [17]. These criteria facilitate developing usable interfaces that are used in a security environment. HCI-S criteria are based on heuristics traditionally used for heuristic evaluation presented by Nielsen [24].

- Visibility of system status: The interface must inform the user about the internal state of the system in a detailed but specific manner.
- Aesthetic and minimalist design: Security interface must be simple and easy to use, maintaining a minimalist design.
- Satisfaction: The security activities must be easy to realize and understand.
- Convey features: The interface needs to convey the available security features to the user clearly and appropriately.
- Learnability: The interface needs to be as non-threatening and easy to learn as possible.

- 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. Johnston et al. [17] adapt the concept of trust 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 [12] proposes the following primary factors that convey trust in an e-commerce environment: (1) Fulfillment; (2) technology; (3) seals of approval; (3) presentation; (4) navigation and brand. These factors are related directly to HCI-S. 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. Additionally, the trust factors presented in [12], agree with the trust concepts explained by Atoyan et al. [1].

C Problem Outline

We believe that a well designed security information feedback could reduce possible errors caused by end users when important notifications are ignored. Many times the designers or/and programmers do not consider the available design criteria or guidelines during the development of the feedback. Additionally, some design guidelines are not specified enough and their application is frequently complex. See literature [11, 15, 26]. Another problem could be the insufficient consideration of the end users by the current web services specifications; i.e. WS-Security specification described in the literature [3, 15, 30]. We think the inclusion of HCI-S design/evaluation criteria in WS-Security specification could mitigate these problems and makes easier the design of adequate security information feedback. As demonstrated by Braz et al. [2], there is an importance of finding equilibrium between security and usability. In the same way the usability studies and concepts presented in the researches [4, 5, 6] argue that same need. According to Atoyan et al. [1], such design rules must be considered during the design of trust systems to increase its proper use and interpretation. Bearing in mind concepts that are described in the literature [8, 9, 16, 31]; it is necessary an adequate feedback mechanism is developed to reduce the possibility that the end users misunderstand security notifications or other information related with the internal state of the system. Our proposal is oriented towards the design of a usable security information feedback for secure web-services, by means of incorporating essential usability concepts in WS-Security specification. In addition, the proposal may complement previous efforts by including the new HCI-S criteria.

Considering concepts that are explained in the book chapter Sanz, et al. [28]; a pattern represents a proven solution for a recurrent problem at a certain environment. We think that it is possible to mitigate the detected needs in WS-Security, by applying the HCI-S criteria like design patterns to establish a usable security information feedback. The solutions offered by the patterns could be included in a new high-level element of the WS-Security's layered architecture (see original architecture of WS-Security in Fig. 1).

The remainder of this paper is organized as follows. Section II locates this work with respect to the state of the art. Section III describes the first version of our proposed relationship between HCI-S and the WS-Security specification that is further applied in a laboratory study in Section IV. Section V summarizes our concluding remarks and provides some avenues for future work. Finally, we list the references reviewed for this research project.

II. Related Work

As far as we know, we are the first researchers to attempt to relate the HCI-S design/evaluation criteria and the WS-Security specification; nevertheless we have analyzed significant HCI works intended to convey security user feedback, and previous research work on improvements for WS-Security Specifications. We have considered the HCI research presented in the literature: Rode et al. [26]; Yurcik, et al., (2003); Cranor [8]; Cranor et al. [9]; Ka-Ping [18]; McCrickard et al. [19].

The focus of Rode et al. [26] 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. Nevertheless, they do not consider the HCI-S design criteria, which may complement this research. Similarly Yurcik et al. [31], try to maker easier specific activities related to security by means of simple instructions and suggestions offered to the users through the interface elements. The research work presented in [8, 9] proposes a very interesting strategy to facilitate the creation of simple interfaces which are easy to understand and use by users, while emphasizing some challenges that designers face during the development process of security and privacy software configuration options. The research presented by Ka-Ping [18] consists of the proposal of a 10 point model 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 et al. [19] propose a very interesting strategy to design and evaluate usable feedback; however they do not consider the application of the HCI-S design criteria presented by Johnston et al. [17]. In general terms, we believe that, the application of the new HCI-S criteria may increase the usability of the aforementioned researches [8, 9, 18, 19, 26].

In addition several proposals to improve WS-Security Specification have emerged recently; we consider two important research papers presented in [3, 15] which are related with ours. The research presented in [3] establishes a set of assertions for the WS-Policy specification. The assertions are oriented to establish standard characteristics for valid policy expressions,

considering alternatives policies, such as: If a web service specification uses natural languages in the messages content, it is necessary that the web service express those accepted and preferred languages. Box et al. [3] present several elements and sub-elements are given to be incorporated in WS-Policy specification using XML (eXtended Markup Language), in order to provide important information and documentation of a particular web service. The research work presented by Haas et al. [15] provides a test suite in order to determine whether assertions are included in the Specification SOAP Version 1.2. The authors focus in facilitating the design of interoperable SOAP processors compatibles with the Specification SOAP Version 1.2 and useful to WS-Security Specification.

III. Towards an Improvement for WS-Security

According to McCrickard et al. [19], notification systems attempt to deliver current, important information to the computer screen in an efficient and effective manner. All notification systems require that the user attends to them to at least some degree if they are to succeed. Examples of notification systems include instant messaging systems, system and user status updates, email alerts and news and stock tickers. The benefits of notification systems are numerous, including rapid availability of important information, access to nearly instantaneous communication and heightened awareness of the availability of personal contacts. While the popularity of these systems has skyrocketed in recent years, the effects of incoming notifications on ongoing computing tasks have been relatively unexplored. The investigation of the costs, benefits and the optimal display of instant messages and all notifications in the context of desktop or mobile computing tasks falls in the general arena of psychological research on alerting and disruptions, but also requires research contributions from design, computer science and information visualization.

It is well known that secure web services must keep the end user informed 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 make it easier to direct operations and use of the available security features. We propose a set of design patterns based on HCI-S design/evaluation criteria in order to specify a well designed security information feedback. Previous versions of this proposal are presented in the literature [20, 21, 22, 23]. The proposed collection of patterns is divided in three principal levels showed in Fig.2.

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

- 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 present a general view of the proposed design patterns, we define some of them in Table 1, specifying a possible recurrent usability problem, and a suggested solution offered by the patterns. Complete description of these design patterns is showed in [20].

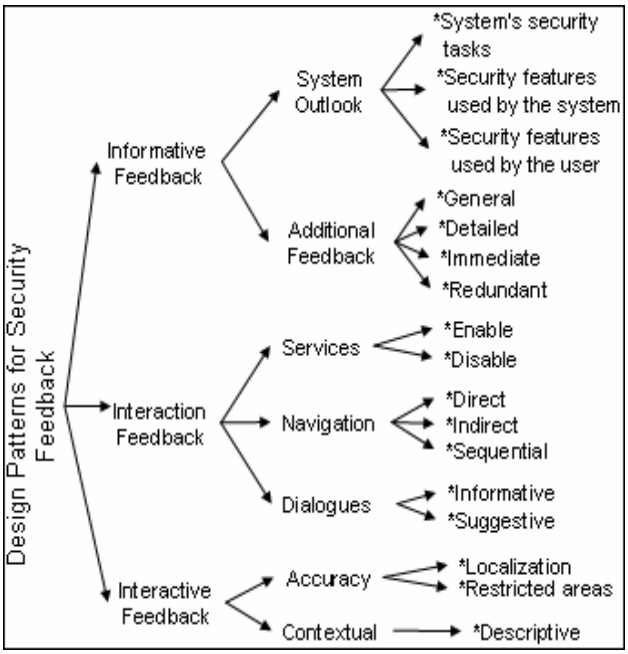

Figure 2. Collection of design patterns for security feedback.

TABLE 1.
SPECIFICATION OF SOME PATTERNS INCLUDED IN THE CLASSIFICATION

Problem	Solution	Pattern
How to inform user about a detected threat?	Using an additional feedback form to enhance the visual notifications established to inform about detected threats.	Immediate Feedback
How to give users more control over the system?	By including options to disable the security features or to continue using it, in specific notifications presented to users.	Disable of Services
How to notify about boundaries for specific interface zones?	By means of changes in the shape of the mouse's cursor user may be informed about the restricted areas in the interface and its elements.	Localization

We intend to incorporate the design solutions offered by the proposed patterns in a new element for the specification WS-security (see Fig. 3).

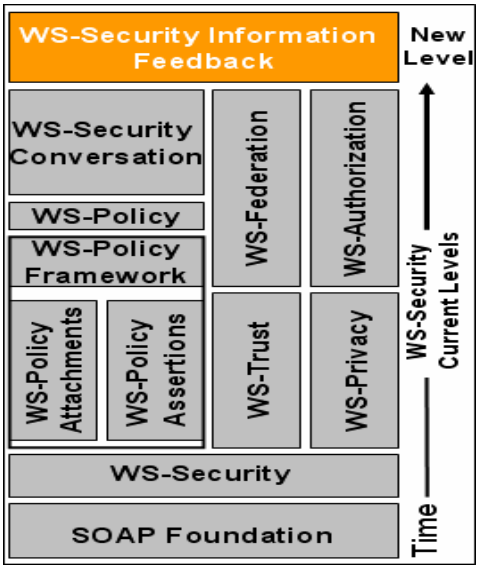

Figure 3. Proposed additional level for WS-Security. Modified of [30].

Bearing in mind that WS-Security is based in web standards like XML, and SOAP transfer messages, it is possible to express the proposed patterns more formally in PLML (Pattern Language Markup Language - http://www.hcipatterns.org/PLML+1.0.html) and the corresponding UI fragments, in UsiXML (www.usixml.org). Likewise we believe that is possible to convey certain design aspects, related with the security information feedback, through SOAP messages. In this way, the design concepts offered by the patterns proposed could be incorporated in a superior level layer, similar to the Application layer in the OSI Model. According to Internetworking Technology Handbook, this layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. It could provide several benefits to the end users, like makes easier the interpretation and use of the security features, and security notifications conveyed through the interface, even those users inexperienced in security, make easier the learning and memorization of its appearance, among others.

IV. Study Case

Following the methodologies for usability tests presented in the literature [4, 5, 6, 13] we conducted a case study in order to evaluate the usability level of specific security feedback designed applying the proposed patterns (see Fig. 2). The obtained information will indicates if the design solutions suggested by the patterns proposed represent a relevant contribution to complement WS-Security. In general terms this study consists of having users filling a typical e-commerce form of personal information. During the use of the form the participants must follow security notifications presented through the interface. We consider the following factors during the performed laboratory study:

- Participants: We recruit sixty participants, consisting twenty one women and thirty nine men varied in different ages from 21 to 54. The participants are graduates in areas including medicine, business administration, and computer science.
- Apparatus: We designed a simple e-commerce form and a set of security information feedback bearing in mind the HCI-S criteria. This prototype was created using the Java Studio Creator 2 Update 1 Free version (http://developers.sun.com/jscreator/downloads/).
- Training Materials: We presented participants with a two pages document on how to use the prototype, the paper included: The objective of the experiment, a brief introduction to the experiment, and a set of activities to realize during the experiment.
- Tasks: Participants accessed the prototype and follow the suggested actions and options presented during the use of the prototype. Subsequently, participants answered a questionnaire related with the usability of the security information feedback presented by means of the prototype.

It is important to mention that the visual notifications (change of colors, and use of images) showed by the prototype are based on literature [20, 21, 22, 23]. In the same way, three well known security threats were considered for the design of the security feedback (rsh attack, rcp attack, and guess attack). Before continuing, we describe briefly the threats considered following the classification of threats mentioned in [10].

1. Guessing 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 mask an authorized IP address to gain unauthorized access to the victim's system (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).
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 considered more risky, because usually are the preface for other attacks.

To provide a general view of the prototype used for this experiment we present the following figures (Fig. 4 and Fig. 5). Fig. 4 presents a screen of the interface. A green color is used in the frame and in the traffic lights, being other form to notify about the internal state of the system (Application of the design pattern "System's security tasks"). The feedback 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 the security features"). Using real world metaphors like traffic participants interpreting easier the security concepts conveyed through the interface. Figure 5, shows the appearance of the UI when a "guess" potential attack was 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 patterns “Dialogue with suggested actions to follow” and “Immediate Complementary Feedback”).

Figure 4. Initial appearance of the prototype interface.

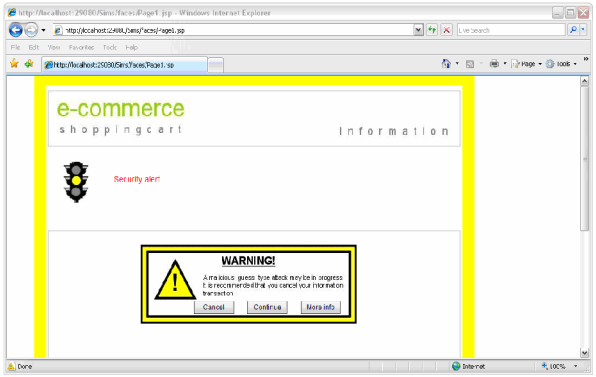

Figure 5. Appearance of the interface to notify about “guess” type threat.

By means of changing the color of the UI’s frame and the traffic lights, as well as displaying specific message avoiding technical terms the participants were 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. After using the prototype, we presented to the participants the following questionnaire which is based on the HCI-S design/evaluation criteria:

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

Each question had six possible answers: Strongly agree, agree, do not know, disagree, strongly disagree, unable to assess. This questionnaire permits gathering the opinion of real users about usability of the security feedback designed by means of the patterns proposed.

Figure 6 illustrates tendency of the participants. In order to show the tendency of the participants we assign a specific color to each answer. In example for Question 2: Forty eight participants selects the option “strongly agree”, nine select the option “agree”, two select the option “do not know”, and one selects the option “disagree”.

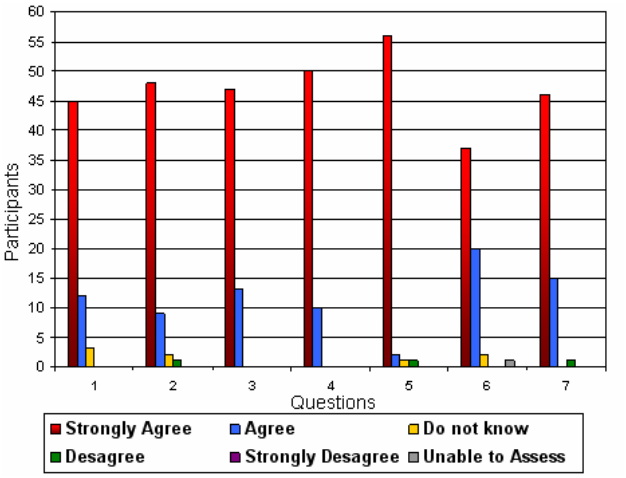

Figure 6. Tendency of the user’s opinion about the usability of the prototype.

After to analyze the result data we infer that the combination of real world metaphors and change of colors results in a very useful notification method for users informing to them about the internal state of the system in a quick and adequate way. In other way, the relation between colors and security threats results in a friendly and very useful form of notification for the users. Additionally the design solutions offered by the proposed set of patterns promote a trust environment between users and system. the security feedback designed for this study case was 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 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 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. This information reflects the effectiveness of the design concepts included in the proposed patterns and confirms the importance of a well designed security feedback. In this way, if this proved knowledge is included in WS-Security, it is possible to include usability concepts even during early design process of a secure web-service. It could represent a god alternative to establish a base to join HCI-S and WS-Security which currently are independent.

V. CONCLUDING REMARKS AND FUTURE WORK

In order to establish the basis to design a usable security feedback, we propose a set of patterns based on the HCI-S design/evaluation criteria. The proposed patterns are intended to facilitate the way some security aspects are conveyed to the end user. With this alternative, it is possible to achieve an appropriate security feedback mechanism through the elements of the interface of a particular web-service. In the same way, the security feedback designed with the proposed patterns, makes possible the correct interpretation about security notifications by users with different experience and backgrounds (experts, advanced, and beginners). The proposal presented in this paper represents a very good alternative to enhance WS-Security, because of that usability are not previously considered in the aforesaid specification. There are several aspects to explore for future work, like express more formally the proposed design concepts (i.e. using PLML and UsiXML). Considering the large-scale study described by Chiasson et al. [4], it is necessary to perform a field study to gain an understanding of how well the design concepts proposed works in a real world scenario, in order to provide a more realistic view of the usability of our proposal. In the same it is important to establish a set of quantifiable metrics to accompany the collection of patterns and increase its useful and provide a complete specification for developers.

ACKNOWLEDGMENTS

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

REFERENCES

[1] H. Atoyan, J. Duquet and J. Robert, “Trust in new decision aid systems,” Proceedings of the 18th Int. Conf. of the Association Francophone d'Interaction Homme-Machine, Montreal, ACM Press, New York, NY, pp. 115-122, April 2006.

[2] C. Braz, A. Seffah and D. M’Raihi, “Designing a trade-off between usability and security: A metrics based-model,” Proceedings of the11th IFIP TC 13 Conference on Human-Computer Interaction, Rio de Janeiro, Brazil, Lecture Notes in Computer Science, Vol. 4663. Springer, Berlin, pp. 114–126, September 2007.

[3] D. Box, M. Hondo, C. Kaler, H. Maruyama, A. Nadalin, N. Nagaratnam, P. Patrick, C. von Riegen and J. Shewchuk, “Web services policy assertions language (WS-Policy Assertions) version 2.1.”, Unpublished.

[4] S. Chiasson, R. Biddle and P. C. van Oorschot, “A second look at the usability of click-based graphical passwords,” SOUPS 2007, Best Paper Award, proceedings of Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, July 2007.

[5] S. Chiasson, P. C. van Oorschot and R. Biddle, “Graphical password authentication using cued click points,” In Proceedings of 12th European Symposium On Research In Computer Security, Dresden, Germany, Lecture Notes in Computer Science, Springer, Berlin, pp. 359-374, September 2007.

[6] S. Chiasson, P. C. van Oorschot and R. Biddle, “A Usability Study and Critique of Two Password Managers,” Proceedings of 15th USENIX Security Symposium, Vancouver, B.C., Canada, pp. 1-16, July 2006.

[7] J. Chong Lee and S. McCrickard, “Towards extreme(ly) usable software: Exploring tensions between usability and agile software development,” Proceedings of Agile Conference, Washington D.C., IEEE Computer Society Press, pp. 59–71, August 2007.

[8] L. F. Cranor, “Designing a privacy preference specification interface: A case study,” Proceedings of Workshop on Human-Computer Interaction and Security Systems, Fort Lauderdale, ACM Press, New York, NY, April 2003.

[9] L. F. Cranor and S. Garfinkel, “Security and usability: Designing secure systems that people can use,” O’Reilly, Sebastopol, 2005.

[10] M. Dass, “LIDS: A learning intrusion detection system”. PhD. Thesis, Nagpur University, India, 2000.

[11] R. Dhamija, “Security usability studies: Risk, roles and ethics,” Proceedings of Workshop on Security User Studies San Jose, California, ACM Press, New York, NY, May 2007.

[12] S. D’Hertefelt, “Trust and the perception of security,” Unpublished.

[13] M. García-Ruiz, M., A. Edwards, R. Aquino-Santos, M. Vargas Martin and R. Mendoza, “Using sonification to teach network intrusion detection: A preliminary usability study,” Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications, Vancouver, Canada, pp. 849-857, June 2007.

[14] M. Hondo, M., D. Melgar and A. Nadalin, “Web services security: Moving up the stack new specifications improve the WS-Security model,” Unpublished.

[15] H. Haas, O. Hurley, A. Karmarkar, J. Mischkinsky, M. Jones, L. Thompson and R. Martin, “SOAP version 1.2 specification assertion”. Technical Report for W3C, April 27, 2007.

[16] M. L. Johnson and M.E. Zurko, “Security user studies and standards: Creating best practices,” Proceedings of Workshop on Security User Studies, San Jose, California, April 28 - May 3, 2007, ACM Press, New York, 2007.

[17] J. Johnston, J. Eloff, and L. Labuschagne, “Security and human computer interfaces,” Computers & Security, Vol. 22, No. 8, 2003, pp. 675–684.

[18] Y. Ka-Ping, “Secure interaction design and the principle of least authority,” Proceedings of Workshop on Human-Computer Interaction and Security Systems, Fort Lauderdale, ACM Press, New York, April 2003.

[19] S. McCrickard, M. Czerwinski and L. Bartramc, “Introduction: design and evaluation of notification user interfaces,” International Journal of Human Computer Studies No. 58, Elsevier, 2003, pp. 509–514.

[20] J. Muñoz, R. Mendoza, M. Vargas Martin, J. Vanderdonckt, F. Álvarez and J. González Calleros, "A method to design information security feedback Using patterns and HCI-security criteria," Proceedings of the 7th International Conference on Computer-Aided Design of User Interfaces CADUI 2008, Lecture Notes in Computer Science, Springer, Albacete, Spain, June 2008.
[21] J. Muñoz-Arteaga, Ricardo Mendoza-Gonzalez and J. Vanderdonckt, "A Classification of security feedback design patterns for interactive web services," Proceedings of. 3rd International Conference on Internet Monitoring and Protection ICIMP'2008, Bucharest, S. Heikkinen, I. Jorstad, N. Tapus (eds.), IEEE Computer Society Press, Los Alamitos, pp. 166-171, June 2008.
[22] J. Muñoz, J., R. Mendoza, F. Álvarez, M. Vargas Martin and A. Ochoa, "Integration of auditive and visual feedback in the design of interfaces for security applications," Proceedings of Workshop on Perspectives, Challenges and Opportunities for Human-Computer Interaction in Latin America, Rio de Janeiro, Brazil, September 2007.
[23] R. Mendoza, J. Muñoz, F. Álvarez, and M. Vargas Martin, "Monitoreo del desempeño de los factores de seguridad de una transacción web a través de la interfaz de usuario," Proceedings of VI Jornada Iberoamericana de Ingeniería de Software e Ingeniería del Conocimiento, Lima, Perú, IEEE Computer Society, pp. 275-282, February 2007.
[24] Nielsen, J. "Ten usability heuristics," Nielsen & Norman Group, Unpublished.
[25] R. W. Reeder, C. M. Karat, J. Karat and C. Brodie, "Usability challenges in security and privacy policy-authoring interfaces," Proceedings of the11th IFIP TC 13 Conference on Human-Computer Interaction, Rio de Janeiro, Brazil, Lecture Notes in Computer Science, Vol. 4663. Springer, Berlin, pp. 141–155, September 2007.
[26] J. C. Rode, P. Johansson, R. DiGioia, K. Silva Filho and D. Redmiles, "Seeing further: extending visualization as a basis for usable security," Proceedings of 2nd ACM Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, ACM Press, New York, NY, pp. 145–155, July 2006.
[27] V. Roth and T. Turner, "User studies on security: Good vs. perfect," Proceedings of Workshop on Security User Studies, San Jose, California, ACM Press, New York, NY, May 2007.
[28] D. Sanz, P. Días and I. Aedo, *Ingeniería de la Web y Patrones de Diseño*, Prentice Hall Editors, 2005.
[29] J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE Vol. 63, No. 9, pp. 1278-1308, September 1975.
[30] J. White, "Security in a web-services world: A proposed architecture and roadmap," Unpublished.
[31] W. Yurcik, J. Barlow, K. Lakkaraju and M. Haberman, "Two visual computer network security monitoring tools incorporating operator interface requirements," Proceedings of Workshop on Human-Computer Interaction and Security Systems, Fort Lauderdale, , ACM Press, New York, NY, April 2003.
[32] J. Muñoz, G. Rodríguez Gómez, "Diseño de Interfaces a Manipulación Directa en Base a Patrones de Interacción", CLIHC, 2003.

Ricardo Mendoza González is a Ph.D. student at the Universidad Autónoma de Aguascalientes (Mexico). He holds a Master's degree in Computer Science (Universidad Autónoma de Aguascalientes, México, 2007), and a Bachelor of Computer Science (Instituto Tecnológico de Aguascalientes, México, 2004). M.Sc. Mendoza González has reported his work in prestigious international conferences such as CADUI, ICIMP, and IASTED CNIS, LA-Web; and international workshops such as CLIHC. He collaborates with researchers of the University of Ontario Institute of Technology (UOIT), and Université Catholiqué de Louvain (Belgium). His current research interests include several topics on: human-computer interaction, information security, usability, artificial intelligence, and software engineering.

Miguel Vargas Martin, PhD., PEng., is an Assistant Professor at the University of Ontario Institute of Technology (Oshawa, Canada), and Chief Technology Officer of Hoper Inc., an Oshawa-based research and development company that offers innovative web tools. Before that, he was a post-doctoral researcher at Carleton University and Alcatel Canada. He holds a Ph.D. in Computer Science (Carleton University), a Master's degree in Electrical Engineering (CINVESTAV, Mexico), and a Bachelor of Computer Science (Universidad Autónoma de Aguascalientes, Mexico). He has reported his work in over forty journals, book chapters, conference papers, technical reports, and pending patents, and so far has supervised almost 20 students at the graduate and undergraduate level. His current research interests include computer forensics, mitigation of denial-of-service attacks, security and human computer interaction, hidden communication channels, and web modeling and optimization.

Jaime Muñoz Arteaga, PhD., is Professor in Computer Science at Universidad Autónoma de Aguascalientes.. Universidad Autónoma de Aguascalientes. He is a researcher in Human-Computer Interaction, and web technologies. He holds a Ph.D. in Computer Science, Human-Computer Interaction (University Toulouse 1 (UT1), Toulouse, France, 2000). He has a number of collaborations with very important researches in prestigious universities around the world. Dr. Muñoz Arteaga has reported his work in journals, book chapters, conference papers, and technical reports, and so far has supervised over 40 students at the graduate and undergraduate level. His current research interests include several topics on: human-computer Interaction, mobile technologies, software engineering, and artificial intelligence.

Francisco Javier Álvarez, PhD., is Professor in Computer Science at Universidad Autónoma de Aguascalientes. He holds a Ph.D. in Engineering (UNAM, México, 2004), He has a number of collaborations with very important researches in prestigious universities around the world. Dr. Álvarez Rodriguez has reported his work in journals, book chapters, conference papers, and technical reports, and so far has supervised almost 30 students at the graduate and undergraduate level. His current research interests include software engineering (methodologies, metrics, among others), and distance education (educational internet technologies, learning environments, learning objects, among others).

Carlos Alberto Ochoa Ortíz Zezzatti, Dr. He has supervised eight PhD theses, 11 master's theses and 27 undergraduate. He participated in the organization of HAIS'07, HAIS'08, ENC'06, ENC'07, ENC'08, MICAI'08, and HAIS'09. His research interests include evolutionary computation (especially cultural algorithms), anthopometric characterization, natural processing language, and social data mining.