Guidelines to Design Usable Security Feedback for Identity Management Applications

RICARDO MENDOZA-GONZÁLEZ
1Postgraduate Studies
Universidad Politecnica de Aguascalientes
Calle Paseo San Gerardo 207, Fracc. San Gerardo, CP 20342, Aguascalientes
Mexico
2Systems and Computing
Instituto Tecnologico de Aguascalientes
Av. Adolfo Lopez Mateos 1801, Ote. Fracc. Bona Gens, Aguascalientes
Mexico
SANDRA JIMENEZ-GONZÁLEZ
Universidad Politecnica de Aguascalientes
Calle Paseo San Gerardo 207, Fracc. San Gerardo, CP 20342, Aguascalientes
Mexico
ricardo.mendoza@upa.edu.mx; mendozagric@acm.org

Abstract: - In this paper we propose a set of design-guidelines oriented to mitigate the typical high-level design challenges, and usability-flaws in identity management applications (IMA’s). Our approach is oriented to help developers in order to achieve usable well-designed user interfaces for IMA’s. We present a set of design guidelines following and adapting a part of a previous contribution consisted of a simple methodology to specify usability in IMA’s joining HCISEC criteria and interactive patterns. Then we show the effectiveness of our proposal by using an illustrative example as a proof-of-concept together with a preliminary study.

Key-Words: - : Identity Management Applications, Security Information Feedback, Design Patterns, Usability, Trustworthy Environment, User-centered Design

1 Introduction
According to Dhamija, and Dusseault “The identity management systems are complex applications oriented to facilitate the management of personal information, credentials, identifiers, and the presentation of this information to other parties by means of powerful web features. In many management schemes, an identity provider (IdP) issues identities or credentials to users, while a relying party (RP) depends on the IdP to check the user credentials before it allows users access to Web site services” [1, pp. 24]. By separating the role of and IdP from the RP, identity management systems let users leverage one identifier across multiple Web services [1, 2]. Security and technology requirements demanded for these systems, and current contact with common users, involve many usability considerations. Identity management systems are responsible for the creation, use, and termination of electronic identities. However, identity management as a formal discipline is a fairly new concept. In addition, identity management represents an important area of research that deserves more study by the security usability community being some of our motivation for why we are interesting in this topic [2].

In line to the above and according to [3], it is very important to distinct between identity management systems (IMS), and identity management applications (IMA). The authors define an IMS as the infrastructure in which IMA’s, as components, are coordinated. IMA’s are tools for individuals to manage their socially relevant communications which can be installed, configured, and operated at the client and/or server side.

Bearing in mind that the IMA could be completely managed at the user’s side it is very important that interface is designed as intuitive a simple as possible. To achieve this goal it is necessary to consider usability in all the stages of the system’s life cycle. Standard ISO 9241-11 defines usability as: “Extent to which a product can be used by specified users to achieve specified goals..."
with effectiveness, efficiency and satisfaction in a specified context of use” [4]. Usability is an essential concept to design adequate feedback which represents any system-user communication form. Thus, information security feedback could be referred as any information related to the system’s security conveyed to the end user through the UI (User Interface) [5]. An appropriate user feedback is very important in any secure system, but it is critical if the adequate use, and the effectiveness of certain security features, depend on it. Currently, many criteria are available to facilitate the design of a security-related user interface. One of the principal approaches is the HCISEC design criteria which were introduced by Johnston et al. [6]. These criteria are based on the traditional Nielsen’s usability heuristics [7]. The concept of HCISEC modifies and adapts the concepts of the traditional HCI to focus in aspects of security and to find out how to improve security through the elements of the interface [6]. According to Johnston et al. [6] HCISEC deals with how the security features of the UI can be as friendly and intuitive as possible, because the easier a system is to use, the less likely is that the user will make a mistake or try to bypass the security feature, resulting in a more reliable system.

To achieve a successful application of the HCISEC concepts, it is necessary to consider the following design criteria, which facilitate developing usable interfaces that are used in a security environment [6]. These criteria are based on Nielsen’s heuristics traditionally used for heuristic evaluation (see e.g. [7]):

- Visibility of system status: The UI must inform the user about the internal state of the system (e.g., using messages to indicate that a security feature is active, etc.). The warning or error messages must be detailed but specific including a suggested corrective action for some security problem, and links to obtain additional information or external assistance.
- Aesthetic and minimalist design: Only relevant security information should be displayed. The user must not be saturated with information and options, and the UI must avoid the use of technical terms as much as possible. The security UI must be simple and easy to use, maintaining a minimalist design.
- Satisfaction: The security activities must be easy to realize and understand without the use of technical terms in the information showed to the user. In some cases, it is convenient to use humor situations or figures to present important security concepts to the user in an entertaining manner.
- Convey features: The UI needs to convey the available security features to the user clearly and appropriately; a good way to do it is by using figures or pictures.
- Learnability: The UI needs to be as non-threatening and easy to learn as possible; it may be accomplished using real-world metaphors, or pictures of keys and padlocks. The meaning of these metaphors may be incorporated to the security interface indicating users how to easily use the specific security features.
- Trust: It is essential for the user to trust the system. This is particularly important in a security environment. The successful application of the previous criteria should typically result in a trusted environment. The concept of trust can be adapted for the HCISEC criteria of trust [6] to “the belief, or willingness to believe, of a user in the security of a computer system.” The degree of trust that users have in a system will determine how they use it. For example, a user that does not trust a web site will not supply their credit card details.

In summary, we believe that our strategy of combining HCISEC Criteria, Design Patterns, and Usability Metrics could be incorporated along the basic development cycle in order to design adequate interfaces for IMA’s. This proposal could be used even to evaluate and enhance existing interfaces. The remaining of this paper is organized as follows. In Section 2 we present a description of the problem within the framework of our research work. In Section 3 we describe our proposed guidelines including an illustrative example as a proof-of-concept together with a preliminary usability study. Finally, in Section 4 we present our concluding remarks and provide some directions for future work.

2 Problem Formulation

According to Dhamija [8], and Johnson et al. [9], a usable security information feedback could reduce possible errors caused by final users when important notifications are ignored, nevertheless the most of the designers or/and programmers do not consider the available design criteria because their application is frequently complex and the criteria are not specified enough. Perhaps, the general problem is that the majority of designers of information security applications, such as IMA’s, do
not use systematic approaches to integrate usability in the interfaces of the systems developed. In the same way, Braz et al. [10] demonstrated the importance of finding equilibrium between security and usability. According to [11, 12, 13] this problem frequently occurs due to the complex application of the security-tools. Other researchers (cf. [14, and 15]) point the need of design methods and rules based on strategies that make easier the application of knowledge oriented to achieve most usable and trustworthy environments.

Specifically linked to IMS/IMA’s, Dhamija, and Dusseault [1] detected the following seven basic flaws:

- **Identity management is not a goal in itself:** Identity management is rarely a user’s primary goal. Security aspects are minor for users, user-friendly systems are more important.
- **Users follow the path of least resistance:** Systems are more likely to be adopted if they’re easy to download, install, and configure. This includes the authentication process and password interfaces, which must become as easy as today’s standard login to successfully compete.
- **Cognitive scalability is as important as technical scalability:** A management system must to reduce cognitive burden for users, avoiding the “Password fatigue” and its security repercussion.
- **User consent could lead to maximum information disclosure:** The number of trust decisions users have to make should be reduced. Don’t try to achieve consent by overwhelming users with more warnings, dialogs, and indicators.
- **Is needed both: User and system authentication:** System should support mutual authentication and help users detect spoofing attacks. Possibility to be attacked must be considered during the system design process.
- **RPs want to control the customer experience:** The use of additional applications may to introduce user confusion. Web sites must to offer some control over the customer relationship, security of their accounts, and user experience.
- **Trust must be earned:** Expert security reviews and usability analyses are essential before deploying identity management systems. It is possible to create a trustworthy environment by means of well-designed systems.

In this way it is possible to infer that the following aspects could represents a further challenge for HCI and Identity Management communities:

- The lack of specifications oriented to conceive usable, secure, and trustworthy identity management applications (IMA’s).
- The lack of design guidelines, best practices, or strategies to design usable IMA’s directed to be readily incorporated into the basic development life cycle.
- The lack of guidelines that provide support to different types of users (Developers, programmers, end users) throughout the entire design process.

Bearing in mind previous narrow circumstances, it is necessary to provide a support for security applications based on usability principles which must be considered during the design-process of trust-systems (e.g. IMA’s) to increase its proper use and interpretation by users. We think that an adequate feedback would substantially reduce possible user’s errors when security notifications are misunderstood. In this way the general objective for this research rises: Establishing a non-exhaustive collection of design-guidelines oriented to help developers in order to achieve usable well-designed user interfaces for identity management applications (IMA). This objective appears to indicate several specific goals, such as:

- To analyze the seven flaws in identity management suggested by Dhamija, and Dusseault [1] to identify those related to usability and user-interface design.
- To set up a collection of guidelines based on HCISEC to reduce the identified usable-identity management gaps, suitable for easy application into the development life cycle stages.
- To show the effectiveness of the proposed guidelines by using study cases as a proof-of-concept.

We proposed a set of design guidelines intended to facilitate the design of a usable security information feedback, easy to understand and interpret by users with different experience and backgrounds (experts, advanced, and beginners). We present a detailed explanation of our proposal in the following section.

### 3 Problem Solution

Before proceeding we should mention the general idea of what a pattern is supposed to be, “A pattern is a proven solution to a recurrent problem in a certain environment” [16]. The patterns take this experience and transform it into knowledge applicable as an alternative to solve a specific issue.
This knowledge could be organized in a number of ways such as classifications, collections, or sets of guidelines [16, and 17].

As mentioned before, we fundamentally considered previously realized patterns approaches presented in [5, and 18] to shape a collection of guidelines oriented to inlay usability into the design of identity management applications (IMA’s), and match with the most of the usability-related flaws in IMA’s identified in [1] and briefly described in section 2.

The novelty of our proposal consists in joining HCISEC [6] with patterns-paradigm to mainly impact on security in IMA’s and its users through a well–designed usable interface, in order to encourage a trustworthy environment. Another relevant aspect of the proposal is that the set of guidelines can be used both to generate new adequate interfaces, and to assess the usability of existing applications as a, basic but very reliable, usability check-list. Additionally the knowledge offered by the design guidelines was structured to be easily composed and specified in a more formal fashion using a pattern language, e.g. [19, and 20].

It is very important to mention that as far as we know, we are the first researchers in try to enhance and evaluate usability of identity interfaces.

Table 1 presents the proposed set of guidelines oriented to bolster usability in identity management applications IMA’s.

<table>
<thead>
<tr>
<th>Usability-related flaws in IMA’s [1]</th>
<th>Guideline</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity management is not a goal in itself</td>
<td>Extolled but Transparent Identity management</td>
<td>Identity management activities must be transparent to the user, nevertheless all the benefits offered by IMA’s must be conveyed to the user in a proper way by means of including UI elements oriented to facilitate the direct operation and use of the available security features.</td>
</tr>
<tr>
<td>Users follow the path of least resistance</td>
<td>Procurement and Commissioning</td>
<td>Including free-download links in browsers, and other widely popular web applications, such as social networks. In addition, the configuration options must be as simple as possible minimizing the number of options. Many times the use of pictures, figures, real-world metaphors, or even humor, contributes to facilitate the use and interpretation of systems including their configuration options.</td>
</tr>
<tr>
<td>Cognitive scalability is as important as technical scalability</td>
<td>Agility and Simplicity</td>
<td>Incorporating simplifications such as automated form-filling, retained settings across several web sites. Additionally, all forms must be designed in a minimalist and aesthetic fashion maintaining the cognitive load as low as possible.</td>
</tr>
<tr>
<td>User consent could lead to maximum information disclosure</td>
<td>Security-decisions Burden</td>
<td>In the event of a serious security problem users should not be responsible for deciding. Actually the number of user decisions in any security issue must be as low as possible. It is necessary to avoid the presentation of critical security and privacy configuration options. In fact, it is very important to keep as low as possible the number of security notifications.</td>
</tr>
<tr>
<td>Is needed both: User and system authentication</td>
<td>Insight of a Trustworthy Environment</td>
<td>Specific visual identifiers could to complement the web authentication technology. Certainly several forms of interactive feedback may to help users in web authentication.</td>
</tr>
<tr>
<td>RPs want to</td>
<td>Usage of</td>
<td>Notify users, in a simple and friendly manner, about the use of</td>
</tr>
</tbody>
</table>
control the customer experience Consistent Look-and-Feel external applications. If possible, use the same or very similar design for all the screens even in those of external applications.

Trust must be earned Encourage a Trustworthy Environment Several authors, e.g. [1, 5, 6, 7, 8, 9, 10, 11, 18] share the idea that a well-designed interface contributes to establish a trustworthy environment. The application of the entire guidelines leads to this point.

3.1 Case Study
In order to analyse both the application of the previous set of guidelines (see Table 1) and their positive impact, we made a comparative evaluation between eight IMA’s, and a suggested prototype was entirely endowed from the knowledge offered by the proposed guidelines (See Figure 1 at the end of the paper). The prototype was based on the user interface of Sxipper¹ (an IMA Firefox plugin). We choose Sxipper¹ due to its simple usage, and friendly look and feel.

Figure 1 graphically depicts the appearance of our prototype called “crIDential”. Figure 1 A) shows the profile-edit section that includes three principal parts: Contact (Information such as Name, Last Name, and e-mail), Localization (Information such as Country, State, and Time), Details (Information such as Gender, and Birth Date). Figure 1 B) Present the Sharing subsection of Profile. This is the most important section of the prototype since it allows users to share his information with others (Companies, personal sites, organizational sites, among others). Additionally, in this section user could create a specific profile considering the following categories: Private, Shopping, Entertainment, General, Professional, and Other, in order to classify web sites and to provide users with an organized and easy way to share his personal information with other sites. Before updating the user profile, the application suggested to verify the entered data; see Figure 1 C). Figure 1 E) shows a small screen that allows users to select (online) one of the specific profile created, depending on his preferences and web site's purpose. Finally, Figure 1 D) presents an always visible icon integrated to the browser in order to inform user about the availability of the application.

For this study were considered the following IMA’s:
1. Mozilla Navigator (selected from [3]).
2. Cookie Cooker (selected from [3]).
3. Yodlee 7 (selected from [3]).
4. Microsoft Passport (selected from [3]).
5. ADSelfService Plus ² (randomly selected, on-line available).
6. Sxipper¹ (randomly selected, on-line available).
7. Tivoli Identity Manager³ (randomly selected, on-line available).
8. Quest One Identity Solution⁴ (randomly selected, on-line available).

The selected Identity Management Applications are available online in the following URL’s:
http://www.sxipper.com¹,
http://www.manageengine.com², http://www-01.ibm.com³,
http://www.quest.com⁴.

The comparative evaluation was conducted according to the testing methodologies presented in [21, 22, 23, 24] as follows:
• We invited 72 participants, consisting of women and men between the ages of 20 and 40. The vast majority of the participants had the basic digital competences [25] but they are not experts on Information Technologies or Computer Science.
• In order to obtain the perception of the participants about the effectiveness and usability of our proposal, we (arbitrarily) distributed the IMA’s to the participants in blocks of 9 to 9 including our anonymous-prototype (It means that each application was evaluated 8 times by different participants). The applications were evaluated using a 0 to 10 scale (Being 0 the worst score, and 10 the best score) considering the following items:
1. Suitable security-decisions burden.
2. Nourishing trustworthy environment.
3. Visibility of system status.
4. Comprehensible application usage.

Previous list was based on the HCISEC criteria [6] which are on line to the Nielsens’s basic usability requirements [7]. Figure 2 graphically depicts the average scores given by the participants to each of the considered IMA’s.

3.2 Data Analysis
After reviewing the study data, we found that the prototype used was very well received by the participants achieving good grades in important
factors such as: Security decision burden, visibility of the system status, comprehension, navigation, and appearance; outperforming most of the considered Identity Management Applications (IMA’s).

In line with the above, the analysis performed revealed that most accepted IMA’s interfaces were: The suggested prototype, Mozilla Firefox, and Skipper (See Figure 2, at the end of the paper), thus we focus on this sub-group.

We could observe that the bigger discrepancy between the three interfaces comparison occurs for Nourishing Trustworthy Environment evaluation, being Mozilla Firefox the highest evaluated. This was expected since the Mozilla Firefox security qualities are one of its strongest points. Nevertheless, the suggested prototype was able to capture a good acceptance of the participants obtaining a very close score in relation to Mozilla for this particular aspect. Although the prototype was a very similar rating to the Mozilla (considered as the best IMA in the study presented in [3]) the perception of the participants categorized the prototype as more usable and comfortable, friendly, and more understandable; these aspects appear to lead to a trustworthy environment.

We also note that participants perceived the system-configuration tasks as the must unwelcome. This perception may impact the adequate usage of several IMA’s which includes a number of configuration options (e.g. Tivoli Identity Manager, Quest One Identity Solution, and Microsoft Passport), producing important gaps in information security and privacy.

Additionally, we could observe a similarity between participants’ perception and the evaluations provided by the wide study presented in [3], particularly in aspects related to: Comprehensible Application Usage, Adequate and Friendly Look-and-Feel, and Agile and Comfortable Navigation.

We perceive that the participants were an inclination to do not trust in applications with inconsistent look-and-feel, even more in those applications that do not included logos or other identity-company information.

4 Conclusion
This paper attempts to tackle the problems identified in [1], namely that current identity management systems suffer from a number of (mostly usability-related and incentive-related) flaws, a really important problem space to address. In response to this challenge, we provide a tool for designers and developers with guidance in designing a usable interface for Identity Management Applications (IMA’s).

In order to provide an evaluation of the significance of the proposed approach, we performed a usability study that consisted of the comparison of a prototype IMA’s interface entirely designed by using the proposed guidelines, against eight current available IMA’s. In this study seventy two users expressed their view on: usability, information comprehension, trust, navigation, etc. for each IMA’s interface (see sub-section 3.1).

After the analysis of the collected information, was possible to infer that the proposed guidelines may to contribute to achieve a well-designed interface for IMA’s. We firmly believe that a well-designed interface represents a very feasible solution for some of the principal flaws detected in IMA’s (see sub-section 3.2).

Even though the number of IMA’s considered seems low, Bevan [26] points out that it is possible and feasible to carry out usability analysis for one application with one user in terms of cost-benefit and case study. Moreover, one user can start testing the computer interface in early stages of web-applications development. Nevertheless, more usability testers should be used before completing the development of a fully-fledged website. Nielsen and Landauer [27] have found that few users can uncover most of the usability problems in a computer interface. These researchers have found that five users can be used to test the usability of an interface to uncover about 75% of its usability problems contributing to achieve a well-designed interface.

The results of this research may be the basis for reducing the gap caused by the lack of truly systematical (or methodological) approaches aimed to enhance the design process of IMA's and its interfaces.

IMA's are very important in the era of web and social networks as they come to expedite the authentication of millions of users who daily exchange confidential information between multiple applications for various. Therefore we think that it is essential to achieve well-designed IMA’s, this is a very important job to do.

There are several aspects to explore as future work for this research, such as to perform a wide study using standard usability questionnaires in order to compare the prototype to newer IMA’s. Other important point consist of structure the proposed guidelines in a more formal fashion using a standard patterns language (e.g. [19, and 20] in order to establish a set of essential best practices oriented to design usable and secure IMA’s
interfaces. We think this aspect represents an important further research-challenge.

References:
[23] Chiasson, S., Biddle, R., and van Oorschot, P. C., A Usability Study and Critique of Two


Figure 1. General appearance of the suggested prototype.
Figure 2. Feedback of the Participants.