Using Human Computer Interaction principles to promote usable security

D. Katsabas[1], S.M. Furnell[1,2] and P.S. Dowland[1]

[1]Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2]School of Computer and Information Science, Edith Cowan University, Perth, Australia
e-mail: info@network-research-group.org

Abstract

Faced with an increasing range of attacks, the appropriate use of available security features in computer systems and applications is becoming ever more necessary. However, although many applications provide ways in which users can protect themselves against threats, the design and implementation of these features can often be criticized from a Human Computer Interaction (HCI) perspective. This results in usability problems for novices and other non-technical users, which may compromise the level of protection that they can achieve. In this research, some standard principles of HCI have been used to devise guidelines to support the inclusion of security features within applications. Ten guidelines were created in total, and a number of existing applications have been assessed to determine their compliance. The results showed varying levels of adherence to the recommended practice, suggesting that current applications have some significant scope for improvement in their presentation of security functionality. To support this view, revised versions of user interfaces were designed for applications that achieved low scores, and the paper presents an example of the outcome to illustrate the approach.

Keywords

Human Computer Interaction, HCI Guidelines, Security

1. Introduction

There are many computer applications that provide some security functionality. This is particularly common in applications that require a connection to the Internet, where a great number of security threats emerge (Paller, 2002). An application may be able to provide significant protection from Internet threats. However if users do not know how to use it, their systems will still be vulnerable (Whitten and Tygar, 1999). In order to improve the usability of an application, Human Computer Interaction (HCI) principles should be carefully considered. There are many aspects in HCI that need attention, including the design of the user interface, the level of online help that can be provided, and the ease of use. If these aspects are not afforded sufficient attention, people may find it hard to understand a program or they may be put off by its complexity (Furnell, 2004). For example applications should not make it difficult to perform a specific task in an application, require too much time for it, or some level of technical experience. Even if some users overcome the difficulties and learn how to use a complex application, they will be likely to forget how to use it afterwards, as it will be infrequently used. Unfortunately, some applications have not applied HCI principles to the user interface and as a result, the security features are often overlooked.

Another considerable matter is that many users, and especially those that are not experienced enough with computers, are not able to customize the applications they use and simply use the default settings. They may not know that security options for the application exist, or how to modify them according to their needs. The reason for this is that the software applications that provide security options have been designed by technical people having a technical audience in mind. Designers do not always consider HCI principles and as a result, the complexity of the applications is high.

In this paper an attempt has been made to make the use of security features in applications easier. A number of guidelines have been used and applications were evaluated according to the level of attention that they afforded to the key issues. Moreover, new interfaces were created for the applications that were perceived to have bad HCI aspects, and a survey has been made in order to test the effectiveness of the new interfaces in making the use of security easier.

2. Background

In general, Human-computer interaction is "a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them" (Hewett et al. 1996). In order to examine and analyze the principles of HCI someone with knowledge only in computers is not enough. Skills from several different sciences are needed in order to study this subject. For that reason assistance has to be provided by people from computer science, psychology, sociology, anthropology, industrial design and other fields (Preece et al. 1994).

In the computer science world, Human-Computer Interaction is not explored enough in order to eliminate problems. HCI aspects help to make computer systems friendlier and easier to use by finding methods and processes for designing interfaces (Carroll, 2003). A suitable user interface that will be easy to learn and efficient to use is desirable in all computer applications. Moreover ways to implement an interface are found like algorithms that work efficiently, software toolkits and libraries. HCI is also concerned with the development of interaction techniques, new interfaces and methods for evaluating and comparing them (Mandel, 1997).

The greatest objective of HCI is to increase human creativity and improve the communication and cooperation between humans and computers. This can be achieved by designing computers and computer applications in such a way that people can fully utilize all the advanced features offered (Baecker, 2004). However, the developers may not consider the use of the functionality from the perspective of their end users and this causes difficulties in the way programs are utilized.

The extent to which a system is friendly may be minimized when security measures have to be taken (Swartz, 2004). For example, suppose that passwords have to be used in order for users to gain authenticated access. The more complex and longer the passwords, the more secure the system will be. Furthermore, the security will be increased if passwords are not the same on multiple systems, and are changed on a regular basis. On the other hand, human memory is limited, and cannot remember complex and long passwords (Krause, 2004). For the same reason, it will be hard for the users to memorize new passwords every time they have to change them. This example clearly shows that usability and security can sometimes be contrasting objectives.

As mentioned by Johnston et al (2003), HCI-S is defined as: “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 security”. Establishing such a common ground is vital in the sense that, without it, users will fail to relate to the options available to them. For example, they often do not use features that they perceive to be advanced or hard to use, and indeed from the presentation of security options in many applications, they may be perceived to be the preserve of experienced or technical users. Therefore, if guidelines can be created that improve the HCI-S aspects of an application, and if those guidelines can be applied correctly, the use of security options may be easier to apply. The purpose of HCI-S is to make a computer system more robust, reliable and secure by enhancing the application’s interface.

3. HCI-S Guidelines

There are several HCI guidelines that an application should follow in order to have correct HCI aspects. Most of the guidelines used were drawn from those proposed by Johnston et al (2003). Further guidelines were created by modifying the 10 usability heuristics proposed by Nielsen (1994). To further refine the guidelines the first principles of interaction design (Norman, 2003) were studied and a number of them were used to improve HCI-S. Ten equally significant guidelines were created and the applications were evaluated against each one of them.

1. **Visible system state and security functions:** Applications should not expect that users will search in order to find the security tools or have hidden features inside the application. Furthermore the use of status mechanisms can keep users aware and informed about the state of the system. Status information should be periodically updated automatically and should be easily accessible.
2. **Security should be easily used:** The interface should be carefully designed and require minimal effort in order to make use of security features. Additionally the security settings should not be placed in several different locations inside the application, because it will be hard for the user to locate each one of them. (Johnston et al., 2003)
3. **Suitable for advanced as well as first time users.** Show enough information for a first time user while not too much information for an experienced user. Provide shortcuts or other ways to enable advanced users to control the software more easily and quickly.
4. **Avoid heavy use of technical vocabulary or advanced terms:** Beginners will find it hard to use the security features in their application if technical vocabulary and advanced terms are used.
5. **Handle errors appropriately:** Plan the application carefully so that errors caused by the use of security features could be prevented and minimized as much as possible. However when errors occur, the messages have to be meaningful and responsive to the problem.
6. **Allow customization without risk to be trapped:** Exit paths should be provided in case some functions are chosen by mistake and the default values should be easily restored.
7. **Easy to setup security settings:** This way the user will feel more confident with changing and configuring the application according to their needs

8. **Suitable Help and documentation for the available security:** Suitable help and documentation should be provided that would assist the users in the difficulties they may face.
9. **Make the user feel protected:** Assure the user's work is protected by the application. Recovery from unexpected errors must be taken into account and the application should ensure that users will not lose their data. Applications should provide the user with the latest security features in order to feel protected. Furthermore some form of notification would be useful in case a security update is available.
10. **Security should not reduce performance:** By designing the application carefully and using efficient algorithms it should be possible to use the security features with minimum impact on the efficiency of the application.

4. Assessment of existing applications

Ten applications were used and assessed against the HCI-S guidelines designed in the previous section. In order to make comparisons on a like-by-like bases only well established software products were evaluated. Three antivirus applications were used (Norton Antivirus, Panda Antivirus and McAfee VirusScan). There were also two firewall applications, namely Agnitum's Outpost Firewall and Zone Alarm Firewall, as well as Opera and Mozilla Firefox web-browsers, Qualcomm's Eudora and Incredimail email client software, and finally Microsoft Word. This gave an overall mix of both security-specific tools, and more general applications that nonetheless included security functionality. Each application was tested according to the level of compliance with each of the 10 guidelines. A maximum mark of 5 could be achieved for each guideline so that the total mark obtained will be out of 50 (10 * 5 = 50). The same grading method was used for all the applications and the grades were from 0 to 5 as designed in Table 1:

Grade	Reason
0	Application diverges completely from the guideline
1	Application significantly diverges from the guideline.
2	Application has paid some attention to the guideline but still has major problems
3	Application has paid some attention to the guideline but still has minor problems
4	Application follows the guideline in some sections
5	Application completely follows the guideline in all possible sections

Table 1: Grading method for HCI-S guideline compliance

The evaluation version of each application was installed and a number of tests were performed in order to assess the performance of the application for each guideline. For example, the settings of the application were examined to check if they were easy to setup, if the security options could be modified easily, if the default settings were provided etc. Table 2 shows a summary of the score that each application achieved for each of the 10 guidelines. It can be noted that there are no guidelines that seem to score uniformly well or uniformly badly across all applications. As such, no consistent pattern can be observed in terms of where applications are failing to present security appropriately.

	Firefox	Outpost	Mc Afee	Eudora	Zone	Norton	Ms Word	Incredimail	Panda	Opera
Visible system state and security functions	2	3	4	3	5	2	3	4	3	3
Security should be easily used	4	3	3	3	4	4	3	5	3	3
Suitable for advanced as well as first time users	5	2	2	5	3	4	4	4	3	2
Avoid technical vocabulary or advanced terms.	2	0	4	0	2	2	1	2	4	3
Handle errors appropriately	3	2	3	2	4	2	4	3	2	4
Allow customization without risk to be trapped	2	2	0	2	1	2	1	2	1	2
Easy to setup security settings	2	5	5	2	2	2	3	5	5	5
Suitable security help and documentation	0	1	1	5	2	5	4	2	5	5
Make the user feel protected	3	4	4	5	3	3	4	2	4	3
Security should not reduce performance	3	4	1	0	1	3	4	4	4	4
TOTAL (/50)	**26**	**26**	**27**	**27**	**27**	**29**	**31**	**33**	**34**	**34**

Table 2: Score summary for assessed applications

5. Applying the guidelines

In order to demonstrate the relative ease with which HCI-S can be improved, the user interface of a subset of the applications tested in Table 2 were modified in order to follow the HCI-S guidelines (Katsabas, 2004). Presentation of the full set of the modifications made is beyond the scope of this paper, and so a specific example is presented. The software tool Mozilla Firefox obtained a relatively low score because it did not conform to most of the HCI-S criteria (Table 2). Even though the privacy options had a separate tab, the security options were among options presented in an ‘advanced’ tab. Studies in HCI have shown that options classified as ‘advanced’ scare many users, especially beginners. Therefore, grouping the security settings in an advanced tab may result in a number of users never accessing them. In order to improve the usability of the security settings a separate tab was added named “security” that contained all the options relating to security (Figure 1).

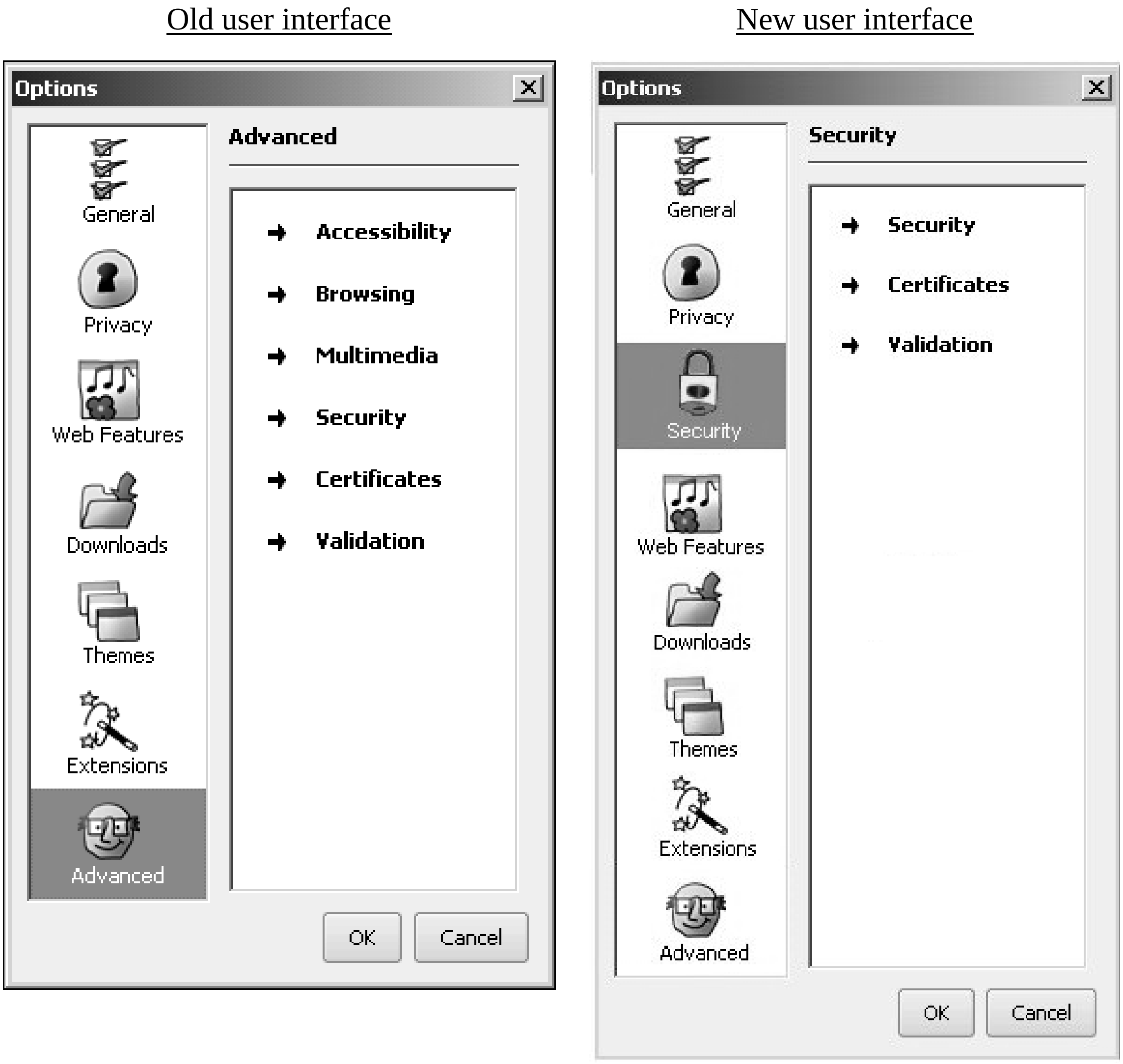

Figure 1: A new options tab was created to store the security options

6. Conclusions

The score that most applications achieved was average, this means applications followed some HCI aspects, but there are still improvements to be made in order to reach a satisfactory mark. The average mark of the applications is 29/50. This score is 21 points away from 50/50 that can be achieved by applying simple guidelines when designing an application. Additionally from the scores in Table 2 it can be observed that the values achieved in each guideline vary. Therefore there were no guidelines against which all applications performed uniformly good or uniformly bad.

All of the proposed HCI-S guidelines are considered to be achievable. To demonstrate this, improvements were made to the interfaces of the applications that obtained the lower marks. These improvements intended to redesign the graphical user interface in such a way that users would find it easier to use. Furthermore additional attention to the HCI-S guidelines was paid in the new interfaces so that use of security would be improved. Some errors were minimized, additional functionality was added using buttons and options, more information and help about security was offered, and explanations were given for specific words, abbreviations and in sentences that could be easily misunderstood by new users.

Although the research to date has provided interesting results, it has only achieved a surface level assessment of how the proposed guidelines would persuade users to use the available security. The guidelines were applied mainly in the interface of the applications, and users could only have a look at the appearance of the new interfaces, rather than actually use them. A more useful assessment of the guidelines, and the effectiveness of the new user interfaces, would be obtained if the improved applications could be used in practice. This issue will be considered as part of the authors' ongoing research.

7. References

Baecker, R. M., (2004), "*Goals and Aspects of HCI*", Wikipedia, http://en.wikipedia.org/wiki/Human-computer_interaction, [Accessed: 31 August 2004].

Carroll, J., (2003), *HCI Models, Theories, and Frameworks: Toward a Multidisciplinary Science*, Morgan Kaufmann, ISBN: 1-55860-808-7.

Furnell, S. M., (2004), "*Using security: easier said than done?*", Computer Fraud & Security, April 2004, pp6-10.

Hewett, T. T, Baecker, R. M., Card, S., Carrey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G., Verplank, W.,(1996), "*Curricula for Human-Computer Interaction*", ACM Special Interest Group on Computer-Human Interaction, http://sigchi.org/cdg/cdg2.html [Accessed: 5 June 2004].

Johnston, J., Eloff, J.H.P., Labuschagne, L., (2003), "*Security and human computer interfaces*", Computers & Security, vol. 22, no. 8, pp 675-684.

Katsabas, D., (2004). *IT Security: A human computer interaction perspective*. MSc thesis, University of Plymouth, UK.

Krause, B. R., (2004) "Security and Usability - Basic Principles, single sign-On" http://www.encentuate.com/resources/usability.htm [Accessed: 6 June 2004].

Mandel, T., (1997), *The elements of user interface design*, John Wiley and Sons, United States, ISBN: 0-47116-267-1.

Nielsen, J., (1994), "*Ten Usability heuristics*", http://useit.com/papers/heuristic/heuristic_list.html, [Accessed: 5 June 2004].

Norman, N., (2003), "*The first principles of Human Computer Interaction*", http://www.asktog.com/basics/firstPrinciples.html, [Accessed: 4 June 2004].

Paller, A., (2002), "*Why is computer security so important?*", The Ohio State University, http://www.chemistry.ohio-state.edu/compsupp/Security, [Accessed: 9 January 2005].

Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S., Carrey, T., (1994), *Human-Computer Interaction*, Addison-Wesley, Great Britain, ISBN: 0-20162-769-8.

Swartz, A., (2004) "Usability in the Real World: The Paradox of Usable Security", http://www.usabilitynews.com/news/article1875.asp

Whitten, A., Tygar, J. D., (1999), "*Why Johnny can't Encrypt: A usability Evaluation of PGP 5.0*", Proceedings of the 8th USENIX Security Symposium, Washington, D.C., USA, August 23–26, pp169-184.