42

HUMAN COMPUTER INTERACTION: AN INFORMATION SECURITY PERSPECTIVES

M.M. ELOFF, J.H.P. ELOFF

eloff@rkw.rau.ac.za
RAU Standard Bank Academy for Information Technology
Rand Afrikaans University, Johannesburg, South Africa

Key words: Information Security, Usability, Awareness, Interactive, Response, Visibility, Human Computer Interaction, Trust

Abstract: The use of computers is becoming increasingly more important in everyday life, not only in the work environment, but also in domestic environments. As computer usage increases, so do the things that can go wrong. The Internet has opened up many new ways of communication – sending documents and other personal information via email for whatever reason. Not all users are information security experts, but also require assurance that they can trust the computer. Human computer interaction (HCI) should be as secure and productive as possible. An investigation into currently available HCI research results, literature and efforts from product suppliers revealed that almost no attention is given to the information security aspects during the design and development of human computer interfaces for IT-products. The purpose of this paper is to highlight the usability of security features in software used on a daily basis.

INTRODUCTION

"A chain is only as strong as its weakest link." To realise security within the realm of human computer interaction, the weakest link, namely the human should be strengthened. Research efforts have addressed information security as a study field extensively, from topics such as cryptography, firewalls through to information security management and ethics. [PFLE97] On the other hand, the topic of human computer interaction (HCI) researches the relationship between computers and people and how the one influences

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*
© IFIP International Federation for Information Processing 2002

and interacts upon the other. [SCHN93] An investigation into currently available HCI research results, literature and efforts from product suppliers revealed that almost no attention is given to the information security aspects during the design and development of human computer interfaces for IT-products. It is also true that information security experts have designed countermeasures without really considering the usability thereof from an end-user perspective.

Can HCI be used to enhance the usability of information security features in IT-products? If so, how? To address information security through the study of HCI is a novel, new and interesting research area. This approach to address the implementation of information security features in IT-products through HCI can be graphically presented as follows:

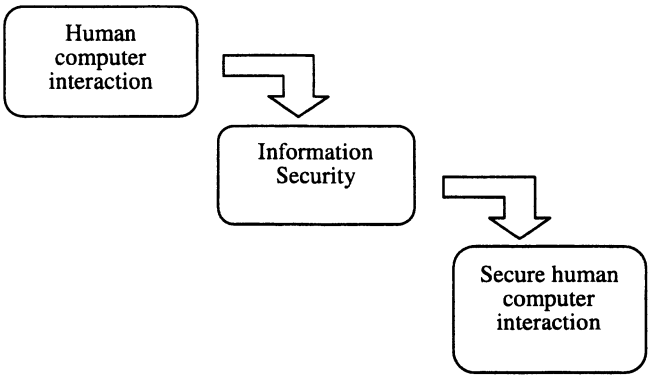

Figure 1. Influence of Human computer interaction on Information Security

Secure human computer interaction is a much-desired feature for e-Commerce environments. Users want to have the assurance that the interface through which they enter their credit card information, for an electronic transaction, will provide the necessary **information security services** to protect their information against unauthorised reading and modification. Successful and secure **human computer interaction** is further dependant on features such as the user seeing and understanding how his/her credit card information is secured when using the interface.

The remainder of this paper is structured as follows:

- A brief overview of human computer interaction
- A brief overview of information security
- A discussion on how HCI can contribute to information security by identifying criteria to evaluate interfaces used to implement security on a user level.
- A critical discussion of some of the built-in security options available in everyday software.

1. HUMAN COMPUTER INTERACTION

It is a well-known fact that excellent user interfaces can contribute to increased productivity, reduced fatigue and errors. Well-designed interfaces can also contribute to users performing well and allowing them to experience a sense of accomplishment and a positive regard towards the designer of the interface. [SCHN93] The three main components in human computer interaction are humans, computers and how they relate to each other. Each one will be defined briefly. [KOTZ00]

- Human – the user is any member Homo sapiens that uses technology, to accomplish a specific task.
- Computer – the physical hardware that runs the specific software.
- Interaction – the way the human uses, communicates with and reacts to the technology.

The resources that the user draws on in this interaction process can be termed human resources. The three main categories are: [KOTZ00]

- Perception - The process, act, or result of gaining insight or knowledge by using the senses.
- Cognition - The mental process or faculty of knowing, how the information is processed.
- Physiology - The biological science of the functions, activities, and processes of humans.

All these resources are used during human computer interaction. In order to ensure the most advantageous interaction, the computer, must convey "clear" messages to the user, allowing him an unambiguous response and vice versa. This includes on the visual perception side aspects such as font type and size, colour contrast and the like. To address the cognitive resource, messages displayed should be unambiguous with appropriate and clear response options for the user. [KOTZ00]

Awareness of the above-mentioned HCI features during the design and development process of information security products, or information security features in IT-products, will enhance the awareness and usability of information security services, such as the confidentiality service when sending email.

2. INFORMATION SECURITY

According to the ISO7498-2 standard, produced by the International Standards Organisation (ISO) Information Security can be defined in terms

of the five security services, namely identification & authentication, authorisation, confidentiality, integrity and non-repudiation [ISO99]. These services are required to ensure that information are protected and secured during its storage, transmission and usage. A brief definition of the Information Security services follows [PFLE97], [VONS97]:

- Identification & authentication - The identification and authentication is the first step towards enforcing information security. A subject requesting access needs to present a token that uniquely identifies it. On presentation of such a token, it should be verified to ensure that it does, in fact, belong to the subject who presented it.
- Authorisation - The next step is to determine if the authenticated subject has the right to access the computer facilities in question. In terms of the authorisation process, control is, therefore, exerted over the access rights of all authenticated subjects.
- Confidentiality - All information must be strictly accessible to authorised parties only. Protecting the confidentiality of information, therefore, gives the assurance that only authorised parties will have access to the information in question.
- Integrity -Information should not only be kept confidential, but its integrity should also be guaranteed. Only authorised parties should be able to change the content of protected information, ensuring that it can be deemed accurate and complete.
- Non-repudiation – This service ensures that no action performed to affect IS, for example, changing the content of a chunk of information, could be denied at a later stage.

From a HCI perspective it is important to note that these information security services should be addressed in the development of IT-products. These services must be available, visible, and usable. If HCI aspects such as cognition, perception and physiology are used as design parameters for security features it will foster trust and improve security awareness in general.

3. HCI FOR INFORMATION SECURITY TECHNOLOGY

"People are often the weakest link in the security chain and are chronically responsible for failure of computer systems" [SCHN00]. If it weren't for people, we most probably would not have needed security! Is it possible to improve or enhance the implementation of information security

by focussing on the human aspects? This is by all means possible, provided some critical aspects are taken into consideration.

The first problem to realise is that to secure interaction between people and just about anything is a difficult task. People loose their keys, misplace wallets, give their passwords to impostors acting as technicians or even write them down next to their computers to name but a few examples.

Secondly, complexity is the worst enemy of security. To win people over to a proper use of information security features, these features must be trusted and easy to use.

Information security is the easiest to implement when it is visible to the user and the user has to interact with the security feature and make decisions based on it [SCHN00]. But on the other hand, users do not want to see for e.g. how a file is encrypted. Any information security implementation therefore must be trustworthy and do some of the "work" in the background.

Examples discussed in the remainder of this paper will be evaluated according to the following criteria:

- Complexity – is it relatively easy to use an information security feature, even for a novice?
- Visibility and interaction – is the information security feature visible and does it require interaction from the user?
- Unambiguous – are the interface and possible outcomes clear to the user and does he know what he have to do and what he will get? This includes clear messages and instructions.
- Information security awareness facilitated – to what extend can the interface contribute to information security awareness?
- Which information security services are addressed by the interface?

In the next paragraph some information security features available in Microsoft software are discussed and evaluated using the above-mentioned criteria.

4. INFORMATION SECURITY FEATURES AVAILABLE IN EVERYDAY SOFTWARE

Each example will be evaluated according to the criteria explained in the previous paragraph to determine if it is a 'good' interface that can enhance information security awareness and usability.

4.1 Information Security Feature to Protect a Word Document Using Passwords

Microsoft Word has the option to protect a document by allowing the user to set two possible passwords. Under Tools on the Menu bar, select Options and click the Save-tab, or under File, select Save-as and click Options. The user will be faced with the following screen: [WORD97]

The first password allows users who know the specific password, to open, read and modify the document. This prevents unauthorised users from opening the document. The user also has the option of changing the password settings. The second password option allows the user to modify the contents of the document, or to open the document read-only if he doesn't know the password.

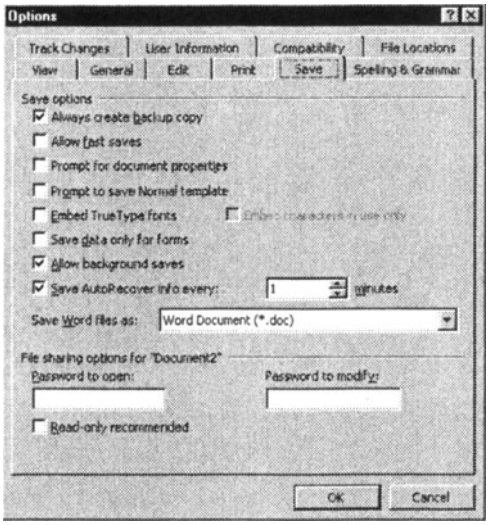

Figure 2 Screen for file sharing options in Word

The user must remember that if he assigns password protection to a document and then forgets the password, he cannot open the document, remove protection from it, or recover data from it. It is recommended to keep a list of passwords and their corresponding document names in a safe place. [WORD97]

Does the user's interaction with this information security feature enhance security awareness and usage? This interface is critically evaluated using the criteria as discussed in the previous part of this paper.

Complexity This interface is relatively simple and easy to use, provided the user knows that it exist. If the user does not know about these facilities,

he will have to use the Help function and search under "security". However, if a user has a number of documents that need to be protected and he/she uses two different passwords for each document as well as different sets of passwords for each document, things can get complicated. The user will have to remember all the passwords or write them down and store in a safe place. As Schneier stated, this might not be a healthy situation, requiring the user to remember all the passwords, or write them down with the document names and keep safe. [SCHN00] The user might even be tempted to use the same password for all the documents, which is even worse!

Visibility and interaction This interface is in the normal contrasting colours of Microsoft and requires the user to confirm the password(s). On opening a protected document he will be prompted to enter the password(s). This increases the visibility of the information security and requires interaction from the user. The user is not burdened to know exactly what is going on behind the screens in implementing the information security feature.

Unambiguous The 'information security'-outcome of this interface is not very clear. The first impression the user gets is that using the first password allows the document to be opened, read and copied, but not changed, while the second password allows the document to be modified. This may create a false sense of security as the user may be under the impression that the document is safe from prying eyes – he used a password to protect against modification! Further more the document can be deleted without any password protection without the user realising it. Nowhere is he warned against such a threat.

Security awareness facilitated This interface can create a false sense of security with users – "use password, is safe". Unless the user knows the advantages and limitations of using this security feature, he might be disappointed when the contents of a document might be compromised. However, using a password for document protection enhances information security awareness as the user demonstrates the need to protect the integrity and confidentiality of a document.

Security services addressed Using the first or both password options addresses the information security requirements of authentication, integrity and confidentiality. Using the second password option only, ensure integrity but not confidentiality as the document can still be opened and read. It is also possible to delete a password-protected document using Windows Explorer. This will result in the document being unavailable.

In conclusion, perhaps this feature was more intended towards document sharing and to restrict or keep track of modifications rather than as a document security feature. The software designers must take the specific information security requirements into consideration and ensure that the user

knows what he/she will get when using one or both of the two password options.

4.2 Information Security Features in Outlook Express

Various information security features exist in Outlook Express, the electronic mail software developed by Microsoft. Some examples include setting security zones, sending secure messages, obtaining a digital ID and add it to your mail account and sending digitally signed and/or encrypted messages. [OUTL99] Due to the length of the paper only setting security zones will be evaluated.

Security zones enable users to decide whether to allow active content, such as ActiveX Controls and scripts, to run from inside HTML e-mail messages. The user can choose one of two zones: moderate Internet zone that allows most active content to run, or a more restrictive security zone. On the Tools menu of Outlook Express, click Options, and then select the Security tab. In the Security Zones section, choose one of the Internet Explorer security zones to use. The majority of Outlook Express users uses Internet zone while the Restricted sites zone creates a more secure environment.

Next, this interface is evaluated according to the defined criteria.

Complexity This interface is also relatively simple and easy to use, provided the user knows that such a feature exist and how to get there. If the user does not know about these facilities, he will have to use the Help function and search under "security". Once in "Help" things can then get more complicated, because of all the different security topics available. Unless the user knows about digital IDs and how to use it, the interface screen to set security zones can be confusing.

Visibility and interaction The security interface requires the user to select one of the security zones. No further interaction is required from the user. This interaction is not very visible, except when active content messages are received that are not allowed to run from inside HTML e-mail messages. The visibility and interaction for this interface is therefore lower than for example the password settings for document sharing in Word.

Unambiguous The security outcome of this interface is not clear to the user until he/she receives e-mail with active content.

Security awareness facilitated The majority users rely on the default settings of the software and unless they experience a security problem, may never use this screen.

Security services addressed Information security services implemented by this feature include confidentiality and integrity. This might not be so obvious to the end-user.

In conclusion, this interface is intended for the more advanced user, who might already be security aware. This feature will not be used on a regular basis, and is therefore not really contributing to security awareness and usage.

4.3 Password Protected Screen-saver in Windows

Windows have the option to set a password that will be required to clear the screen-saver. In this way files will be protected from prying eyes whenever the user leave his computer with the screen-saver on. [WIND95]

From Start, select Settings and Control Panel. Select Display and click the Screen-saver tab. From this screen click the Settings button, resulting in the following screen:

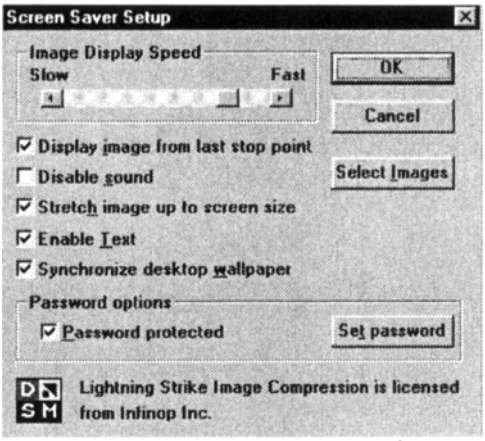

Figure 3 Screen-saver set-up for Windows

Tick the Password protected box and set the password using the Set password button. The user will be requested to confirm the password by re-entering it. The screen saver starts if the computer is idle for the number of minutes specified in the Wait box. To clear the screen saver after it has started, move the mouse or press any key. The user will then be prompted to enter the password.

When a password is assigned to a screen saver, people who do not know the password cannot clear the screen saver, and therefore cannot easily gain access to the information on the computer.

For this feature to work satisfactory, the user must set the 'wait' time before the screen saver comes up, to his requirements. If the wait time is to short, he will get frustrated because of all the times he have to enter the password. If it is set too long, it will not contribute to security as unauthorised users may get access to his computer.

Next this interface will be evaluated according to the defined criteria.

Complexity This interface is simple and easy to use. If the user knows how to change the settings for a screen-saver, then setting the password is just another option available.

Visibility and interaction The password-setting interface has the same appearance as all the other Microsoft interface screens. After setting the password, the user will be required to enter the password every time the screensaver was activated. This requires interaction from the user on a regular basis, which makes security therefore visible. The visibility and interaction for this interface is therefore higher than for example the password settings for document sharing in Word.

Unambiguous The security outcome of this interface is clear. The user must enter the password every time the screensaver was activated.

Security awareness facilitated This interface undoubtedly contributes to security awareness as the user demonstrates the need to protect the integrity and confidentiality of all the information on his computer.

Security services addressed All the discussed security services are addressed, because the user must know the password to clear the screen saver and gain access to the computer.

5. CONCLUSION

In this paper three examples of interfaces relating to information security were discussed. Each example was evaluated according to the criteria defined in the paper. The use of passwords where the user is required to enter the password when accessing specific information, is the best way of instilling security awareness and usage amongst users, provided that the user is forced to use a quality password. The human factor is one of the most important when addressing information security. The interaction that the user has with the computer can be a deciding factor in the success or failure of implementing information security. Developers need to keep the human factor in mind, then secure human computer interaction will be a possibility.

6. LIST OF SOURCES CONSULTED

[BS7799] BS7799 Code of Practice for Information Security Management, BSI **1999**.

[ISO99] International Standards Organisation, Nov 1999 http://www.iso.ch

[KOTZ00] Paula Kotzé, 2000, Peopleware: Changing the Mindset of Computer Science and Engineering, Inaugural Lecture, Dept of Computer

Science, UNISA,19 October **2000**

[OUTL99] Outlook Express 5, **1995-1999**, Microsoft Corporation

[PFLE97] Charles P. Pfleeger, **1997**, Security in Computing, Second edition, Prentice Hall

[SCHN00] Bruce Schneier, **2000**, Secrets & Lies, John Wiley & Sons Inc, USA

[SCHN93] Ben Schneiderman, **1993**, Sparks of Innovation in Human-Computer Interaction, Human-Computer Interaction Laboratory

[VONS97] Von Solms SH, Eloff JHP, **1997**, Information Security, Rand Afrikaans University,

[WORD97] Microsoft Word 97, **1983-1996**, Microsoft Corporation

[WIND95] Microsoft Windows 95, **1981-1996**, Microsoft Corporation