Security and human computer interfaces

J. Johnston [a], J. H. P. Eloff [a] and L. Labuschagne [b]

[a] *Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa*

[b] *Department of Computer Science, Rand Afrikaans University, PO Box 524, Auckland Park, 2006, South Africa*

Abstract

Computer users are exposed to technology mainly through user interfaces. Most users' perceptions are based on their experience with these interfaces. HCI (human computer interaction) is concerned with these interfaces and how they can be improved. Considerable research has been conducted and major advances have been made in the area of HCI. Information security is becoming increasingly important and more complex as business is conducted electronically. However, state-of-the-art security-related product development has ignored general aspects of HCI. The objective of this paper is to promote and enable security awareness of end-users in their interaction with computer systems. It thus aims to consolidate and integrate the two fields of information security and HCI. HCI as a research discipline is a well developed field of study, and the authors are of the opinion that the use of security technologies can be significantly enhanced by employing proven HCI concepts in the design of these technologies. In order to achieve this, various criteria for a successful HCI in a security-specific environment will be examined. Part of the Windows XP Internet Connection Firewall will be used as a case study and analysed according to these criteria, and recommendations will be made.

Keywords: HCI, human computer interaction; Information security; Usability; Trust; Firewalls; HCI-S

1 Introduction

Users experience computers and technology through various user interfaces — mobile phone menus; buttons, icons and windows on a computer screen; dials and knobs in cars; and back buttons and hyperlinks on the Internet. These interfaces are designed to aid the users' understanding of and productivity in using technology. For example, a well designed interface assists the user in becoming proficient in the operation of a software program in a shorter time frame. This enables the user to increase his/her efficiency in completing a certain task. The user feels in control and satisfied with the technology. On the other hand, a poorly designed interface can frustrate the user and hinder the successful completion of tasks, resulting in aversion and scepticism towards using the specific technology in the future.

This paper focuses on aspects of human computer interfaces (HCIs) that are relevant in an information security environment. An example of these is the interface of a software product such as an encryption program or a firewall. These programs deal almost exclusively with security functions. Parts of other interfaces are also intertwined with security features, such as the login interface of an Internet banking website.

Computer and information security continues to grow in importance as the world becomes more connected and an increasing amount of business is transacted electronically. According to the Computer Crime and Security Survey [RICH03], the most popular security technologies used by companies are anti-virus software (99% of companies polled use it) and firewalls (98% of companies). As a result of the proliferation of office and home computers, technologies such as anti-virus software and firewalls have now migrated into the realm of the everyday user, who is not a security expert. This means that the roles of interfaces are crucial in technologies such as anti-virus software and firewalls that convey and guide the user through security features. The user

experiences security functionality through the interface. The interface informs the user of the security functions that are available and how to use them. A user may not be aware of a security feature or may use it incorrectly. For example, a personal firewall can only protect a user's computer if it is active, and it will only be active if the user knows how to turn it on. The interface needs to ensure that the user is guided so as to minimise the potential for the user to be the 'weakest' link.

When designing an interface, there is a number of well established criteria that can be applied to increase the efficiency of using various technologies. An example of one such criterion is consistency and standards, as defined by Jakob Nielsen and Rolf Molich in 1990 [MOLICH90]. Consistency and standards mean that, in an interface, the words and actions used need to be consistent and have the same meaning throughout the interface. Consider, for example, some of the firewall products available on the market today. It is common for many of these products to use the terms 'firewall' and 'gateway' synonymously, thereby creating confusion for the average end-user.

The objective of this paper is to show how existing and well established HCI criteria can be employed to analyse and improve the security features of an interface. A number of recommendations are proposed for the modification of currently available interfaces with the ultimate aim of enhancing the usage of the security features of these products.

The first section of this paper discusses the field of HCI. This is followed by the introduction of 10 existing HCI criteria. Once a background to HCI has been established, a new term — HCI-S — is defined. The 10 HCI criteria are then modified, condensed and adapted to focus on the security aspect of HCI. These new criteria are referred to as HCI-S criteria. Windows XP's Internet Connection Firewall is analysed according to these HCI-S criteria. Proposals are then made as to how the interface of the Internet Connection Firewall can be improved.

2 What is HCI?

HCI stands for human computer interaction [MICH01]. From a computer science perspective, HCI deals with the interaction between one or more humans and one or more computers. An image which comes to mind is that of a person using a user interface program, e.g. Microsoft Windows on a workstation [HEWE96].

According to Sjoerd Michels [MICH01], HCI can be defined as: "the part of a computer program responsible for establishing the common ground with a particular (i.e. well known) user. His task is accomplished by expanding and maintaining this common ground throughout the interaction process with the application. Whenever possible, direct manipulation of familiar objects should be the leading interaction principle."

This definition mentions the 'direct manipulation of familiar objects'. This is possible if these objects are known from the real world or from other HCIs. A user is more likely to trust an object that is familiar. The definition also hints at the goal of an HCI, which is to facilitate the interaction between the user and computer. A well designed interface contributes to increased productivity and reduced errors [SCHN93]. For this paper, an 'interface' is a web interface or a traditional graphical user interface on a computer. The computer can be defined as a traditional home or office personal computer or any workstation.

The purpose of HCI is to enhance the 'user-friendliness' of a system. This is sometimes wrongfully perceived as opposing the goals of a secure system [BOTH02]. For example, confidentiality of information is desired in a secure system and is accomplished to a certain

degree by the use of passwords. Traditional thinking states that the more passwords there are and the more complex the passwords are, the better the security of a system. However, users do not remember a long complex password, which means they will write it down, leading to the potential breakdown of the security of a system. When it comes to usability principles, the fewer the passwords and the simpler the passwords are, the better. This appears to highlight a contradiction between security and usability. A balance needs to be struck where a secure usable password is created.

In the next section, existing HCI criteria will be introduced that can be used to enhance the 'user-friendliness' of a system.

3 Criteria for a successful HCI

In 1983, Apple Computers released the Apple Lisa to the public [MEYE98]. The Lisa was one of the first commercially available computers to have a graphical user interface. The introduction of graphical user interfaces has made the operation of computers much easier and has also led to huge growth in research in the field of HCI. This in turn has led to a number of principles being established [NIEL94, CARR03]. One of the key players in the field of HCI is Jakob Nielsen. He has been involved in HCI and usability for many years and has developed a list of 10 criteria for a successful HCI [NIEL02]. These criteria, listed in Table 1, have been widely accepted.

Given the established nature of these criteria, it is a good starting point to expand and modify the list of criteria so that they are relevant to an HCI in a security environment. In the next section, the process of expanding and modifying the HCI criteria will start with a definition of a security HCI.

Table 1 - Criteria for a successful HCI

No.	Criteria	Description
1	Visibility of system status	It is important for the user to be able to observe theinternal state of the system through the HCI. This can be achieved by the system providing correct feedback within a reasonable time.
2	Match between system and the real world	An HCI which uses real-world metaphors is easier tolearn and understand. This will assist a user in figuring out how to successfully perform tasks.
3	User control and freedom	System functions are often chosen by mistake. The user will then need a clearly marked exit path.
4	Consistency and standards	Words, situations and actions need to be consistent and have the same meaning. A list of reserved words can assist in this area.
5	Error prevention	It is obviously best to prevent errors in the first place through careful design. However, errors do occur and they need to be handled in the best possible way.
6	Recognition rather than recall	The user should not have to remember informationfrom one session to another. Rather, the user should be able to 'recognise' what is happening.
7	Flexibility and efficiency of use	The system should be efficient and flexible to use. Productivity should be increased as a user learns a system. The system should not control the user; rather, the user should dictate which events will occur. The system should be suitable for new and power users.
8	Aesthetic and minimalist design	Information which is irrelevant should not be displayed. The user should not be bombarded with information and options.
9	Help users recognise, diagnose and recover from errors	Error messages need to be clear and suggest a solution.
10	Help and documentation	Users tend to turn to help and documentation as a last resort. Help functionality needs to be context-sensitive and easy to search.

4 Definition of a security HCI (HCI-S)

The objective of this paper is to see how the security of a system can be improved by improving the interface. In order to achieve this objective, a new term 'HCI-S' will be introduced.

A reference to HCI-S has not been found in current literature. Therefore, for this paper, security HCI (HCI-S) can be defined as: "the part of a user interface which is responsible for establishing the common ground between a user

Table 2. Summary of HCI-S criteria.

No.	Criteria	Description
1	Convey features	The interface needs to convey the available security features to the user.
2	Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
3	Learnability	The interface needs to be as non-threatening and easy to learn as possible.
4	Aesthetic and minimalist design	Only relevant security information should be displayed.
5	Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6	Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?
	Does the interface lead to trust being developed?	
	Trust	It is essential for the user to trust the system. This is particularly important in a security environment.

and the security features of a system. HCI-S is human computer interaction applied in the area of computer security."

HCI-S deals with how the security features of a graphical user interface can be made as user-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.

HCI's focus is on making a computer system as easy to use as possible. However, security features are sometimes perceived to make a system more difficult to use. HCI-S addresses this issue and strikes a balance between security and ease of use.

5 Criteria for a successful HCI applied in the area of security

The interface criteria proposed for HCI-S are listed in Table 2.

The reason for these criteria is to assist in the development and design of interfaces used in a security environment. These criteria are based on Nielsen's HCI criteria, found in paragraph 3 [NIEL02]. They have been modified and condensed to address only the essentials in a security environment. Condensing the criteria makes them easier to remember and modifying them is necessary in order to focus on security.

In the next paragraphs each HCI-S criterion is discussed in more detail.

5.1 Visibility of system status

Visibility of system status allows the user to observe the internal state of the system. An example of this is the small 'padlock' which is displayed in the bottom right-hand corner of Internet Explorer when viewing a secure web page (Figure 1). The padlock informs the user of the status of the web page and that encryption is being used.

5.2 Aesthetic and minimalist design

A balance needs to be struck by providing enough information for a first-time user while

Fig 1 - Padlock in Internet Explorer

at the same time not providing too much information for an experienced user. Irrelevant information should not be displayed. The user should not be bombarded with information and options. As far as possible, technical terms should be avoided. For example, if the interface to a security function looks too complicated or confusing, the user may not feel confident enough to use it. By having a minimalist design, this situation can be improved.

5.3 Help users recognise, diagnose and recover from errors

Errors which occur when dealing with a security function have the potential to be more lethal than normal errors. For example, take the situation of an error occurring in the middle of a banking transaction and the following error message being displayed: "Your interactive session is no longer active" [FIRST02]. This error message is confusing and may cause a user to feel concerned about the outcome of the transaction. It is important for the error message rather to be detailed and specific, and to state what action needs to be taken and how to obtain additional assistance. A generic message for all errors is not adequate.

5.4 Satisfaction

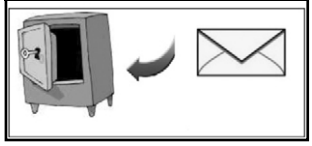
Security is usually not a primary activity for computer users, so their experience with security features needs to be pleasant and satisfying, otherwise they may neglect the security of their system. For example, if it is too much effort for users to encrypt a sensitive document, they may take a chance and email the document unencrypted. Security is also seen by many users as a very technical topic. Techniques such as humour and graphics can be used to introduce important security concepts to users in a more entertaining manner.

5.5 Convey features

The interface should inform the user in a clear manner of the available security features. For example, the security features of integrity and confidentiality are available on most e-commerce web sites. One of the ways in which these features are implemented is through SSL. The use of SSL by a web site should be conveyed to the user by the interface, along with the purpose and benefits of SSL. The use of pictures can be an effective way of conveying features, especially for a user who is not technically minded. Figure 2 shows an example of a graphic which could depict the feature of encryption.

The HCI-S criterion of Convey features informs the user of the available security features, while the criterion of Visibility of system status allows the user to 'see' if these features are active and being used.

Fig 2 - Encryption



5.6 Learnability

Security is often not a priority for a user, even though it is very important. Therefore it is essential for a security HCI to be as user-friendly and as easy-to-learn as possible. A casual user that has not used the software for a while should not have to learn everything over again [MICH01]. An interface that uses real-world metaphors is easier to learn and understand. For example, items such as keys and locks have real-world uses and meanings. These items and their meanings can be transported and used in an interface. A user that then sees these items will recognise them and have an idea of what they could be used for in the interface. This will assist a user in determining how to perform tasks successfully. An example of this is shown in Figure 3 (the logon keyhole links to the sign-in page).

An interface that is consistent and based on standards is also easier to learn. Many users are familiar with the conventions of interfaces used in the Microsoft Windows environment. Icons,

Fig 3 - Match between system and real world [FIRST02]

windows and menus all behave the same in the Windows environment, which means it is easier for a user to learn a new program based on these

standards. When it comes to security features in an interface, there are certain conventions which are used frequently, for example usernames and passwords. The user may become confused if different terminology is used, for example 'Profile' instead of 'Username' and 'Access Code' instead of 'Password'. It is therefore advisable for an interface to be consistent and to adhere to standards.

Applying the above six HCI-S criteria in the design of a security feature culminates in establishing trust. Trust is discussed in the next paragraph.

6 The six HCI-S criteria lead to trust

The successful implementation of all the above criteria will lead to trust. Trust is important because if a person is to use a system to its full potential, be it an e-commerce site or a computer program, it is essential for him/her to trust the system.

According to the Oxford English Dictionary, trust can be defined as: "the belief or willingness to believe that one can rely on the goodness, strength, ability of somebody or something" [OXFO95]. This definition can be adapted for the HCI-S criterion 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 his/her credit card details.

The interface plays an important role in fostering trust between the system and user. One way in which this can be done is by the interface informing the user in a clear manner of the risks and how these risks can be minimised. A high-quality interface which projects quality and professionalism will also foster trust. This may, however, be a false sense of trust if the technology behind the interface is not adequate.

As the Internet continues to grow, its success will depend on gaining and maintaining the trust of visitors. Trust on the Internet is not based solely on technical security features, but also on the user's feeling of control of the interactive system [DHER00].

Research performed by InteractionArchitect.com [DHER00] points to six primary factors which convey trust in an e-commerce environment. These factors are fulfilment, technology, seals of approval, presentation, navigation and brand. These factors are important because four of them relate directly to HCI-S:

Fulfilment — This relates to the HCI-S criteria of Convey features and Visibility of system status. The user needs to know which security features are available and be clearly informed when these features are being used. Fulfilment should lead to Satisfaction.

Seals of approval — Seals of approval, for example those used by VeriSign or TRUSTe, need to be in prominent positions. It is also important for their meaning to be conveyed to the user. Seals of approval would come under the HCI-S criterion of Convey features. These seals are third-party endorsements which should help to foster trust between the user and the web site.

Presentation — Aesthetic and minimalist design is important in the presentation of a web site. The result of an aesthetic and minimalist web site is that it is easier to navigate and use than a cluttered web site. This will lead to a more satisfying online experience for the user.

Navigation — An Aesthetic and minimalist design aids navigation. A site which is easy to learn (Learnability) is also easy to navigate.

From the above paragraph it can be seen that these factors overlap with some of the HCI-S criteria. This means that, by applying the HCI-S criteria of Visibility of system status, Satisfaction, Aesthetic and minimalist design, Learnability and Convey features, trust can be developed.

In the next section, the HCI-S criteria will be used to analyse the interface of a firewall. The purpose is to illustrate the application of these criteria.

7 Analysis of Windows XP's Internet Connection Firewall (ICF) according to HCI-S criteria

Microsoft has decided to incorporate a firewall called the Internet Connection Firewall (ICF)

in its Windows XP operating system. The ICF comes as standard with both the home and professional versions of Windows XP.

The ICF is aimed at home and small office computer users. Its goal is to provide a baseline intrusion prevention device in Windows XP. The ICF will hopefully protect against scans for information and block unwanted inbound packets [MICRO01]. It is a stateful firewall, which means it only allows incoming packets if they are part of a session originating in the XP computer. Any 'rogue' packets are dropped and optionally logged. The ICF can be activated on any network connection, for example an Internet connection or a local network connection. Microsoft has attempted to make the ICF a simple and unobtrusive security experience.

The reason why the Windows XP ICF has been chosen for analysis in this paper is that, according to WebSideStory, as of May 2003, Windows XP is used by more than a third of all Internet users [WEBSI03]. The next most popular operating system is Windows 98, with a 25% market share [WEBSI03]. This means that there are millions of users around the world that have the ICF installed on their computers. The usability of the interface therefore has the potential to play a huge role in the security of many computers.

In the following paragraphs parts of the ICF interface are analysed according the HCI-S criteria. Recommendations are made on how the interface can be improved according to these criteria.

7.1 ICF — Operation

The operation of the ICF is simple. Whenever a network connection, for example a dial-up connection to the Internet, is used, the ICF is active, provided that the ICF option was selected when the network connection was created.

However, many users will not be aware that the ICF is installed and operational because they are not informed of this by the interface. An ICF icon is not displayed in the systems tray and a message does not alert the users to the fact that they are now protected. The Visibility of the system status is therefore not at all clear. The fact that the users are not made aware of the ICF means that they are not encouraged to trust the system.

When a 'rogue' packet is identified by the ICF, it is dropped but the user is not made aware of this. Once again, the Visibility of the system status is poor. The user should be notified of a possible hacking attempt. The user can then decide if he/she wants to ignore any further

Fig 4 - System tray - Visibility of system status is poor

warnings. The criterion of Satisfaction is not handled well in this case. It could be a very satisfying experience to know that an attempted hack has been thwarted!

Recommendations for the operation of the ICF

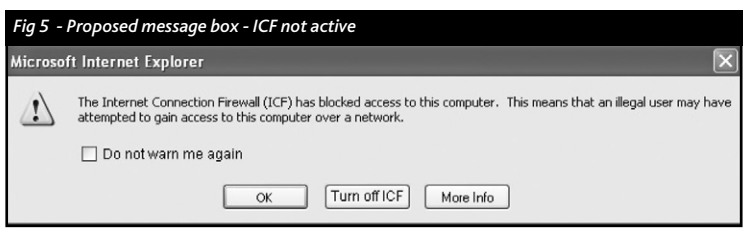
A number of recommendations based on the HCI-S criteria can be made. These recommendations aim at improving the HCI-S of the ICF.

A message box should be displayed as soon as a network connection is used that is not protected by the ICF, warning the user. The message box will aid the Visibility of system status. Figure 5 shows a proposed message box.

An icon should be clearly visible in the system tray whenever the ICF is active, for example an 'F' for firewall (Figure 6).

If the firewall drops packets, the user should be notified via a message box (Figure 7). The user

Fig 5 - Proposed message box - ICF not active



should be able to turn this option on and off. Perhaps the 'F' icon in the system tray could also flash when there is an attempted 'hack'.

7.2 ICF — Configuration

One of the configuration windows of the existing ICF interface is shown in Figure 8. This window has an Aesthetic and minimalist design. The user is not bombarded with options and information.

It also has links, such as 'Learn more about Internet Connection Firewall', to more information which should help the user to trust the ICF. The help provides comprehensive information which Conveys the security features. It is easier to trust something that is understood.

However, it is not obvious that the 'Settings' button at the bottom of the window is also for the ICF. Clicking this button brings up a window with 'Advanced Settings'. The Advanced Settings window will not be analysed in this paper.

Fig 6 - Proposed icon in the system tray

Fig 7 - Proposed message box - notifies the user that a packet has been dropped

Recommendations for the configuration of the ICF

Figure 9 is a screen shot of the proposed new interface for the ICF. The tab has been changed from 'Advanced' to 'Firewall'. Many users avoid any buttons or tabs with the word 'Advanced' on them. Some users feel that advanced settings should not be changed or explored, as they only need to be used by advanced users that are using their computer for extraordinary tasks. The ICF, however, is not an advanced feature, but rather a standard feature that should be used by all users. The proposed interface is also only focused on the

Fig 8 - Existing HCI-S for the ICF

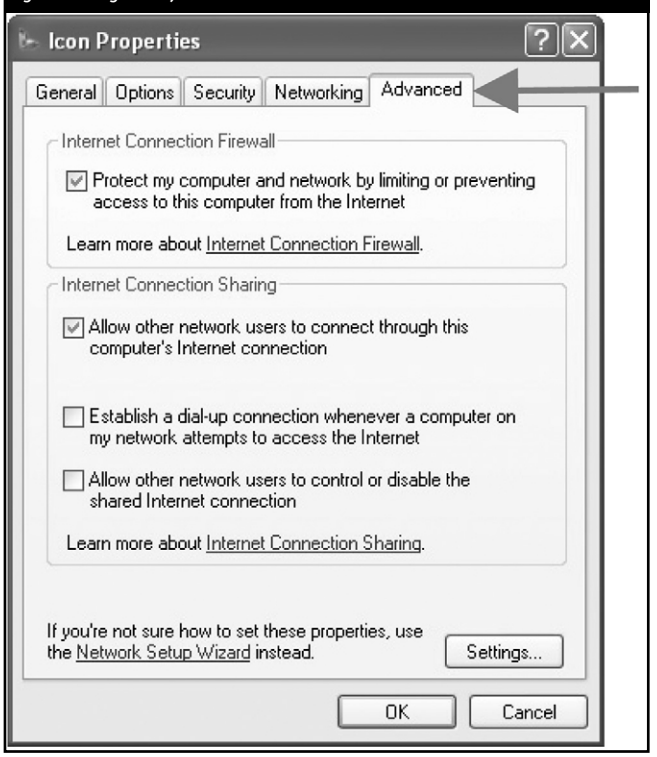
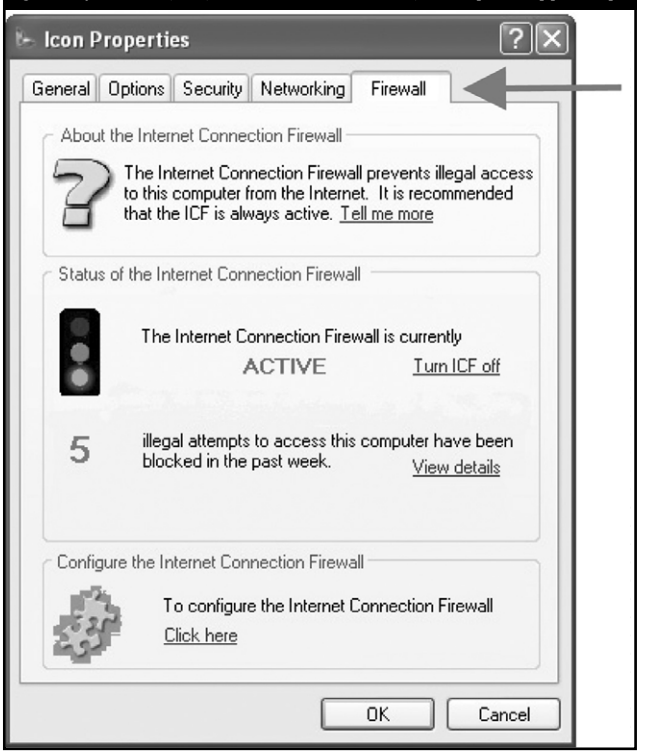


Fig 9 - Proposed interface for the Internet connection firewall [PUZZLE] [QUEST]



ICF, unlike the existing interface, which also deals with Internet connection sharing (Figure 8).

In order to view the existing interface (Figure 8) of the ICF, the user needs to go through a few steps. For example:

click the 'Start' button;

then click 'Connect to' followed by 'Show all connections';

right click on the Network Connection;

select 'Properties';

then select 'Advanced';

follow this by clicking on 'Settings'.

This process is convoluted and difficult to learn. In order to solve this problem, there are three methods to view the proposed interface (Figure 9) for the ICF:

clicking on the 'F' in the system tray;

selecting the ICF in the Windows Control Panel — this means that a new icon would need to be added to the Windows Control Panel for the ICF;

clicking on the ICF tab when the user is reviewing any network connections, e.g. Internet connections or LAN connections.

These three methods are intuitive and will aid the Learnability of the proposed interface.

The interface in Figure 9 has an Aesthetic and minimalist design. This is evident from the simple layout and the fact that it contains only relevant information for the ICF. It is not complicated and is easy to Learn. This is because the window is based on recognition and not on recall. This means that the user does not need to remember how the ICF works, but rather recognises what the functions do. The Visibility of the system status is clearly displayed by the green 'Active' statement. The user is also informed of any possible hacking attempts. This encourages the user to trust the system. As little technical jargon should be used as possible.

7.3 Summary of analysis of ICF

As has been mentioned, analysis of and recommendations on the entire ICF interface are beyond the scope of this paper. The table below summarises the research findings that have been discussed in this paper, and indicates whether the existing and proposed ICFs meet the criteria.

Table 3. Summary of research findings.

HCI-S Criteria	Existing ICF	Proposed ICF
Convey security features	YES The security features are conveyed by a comprehensive help function.	YES The 'tell me more' links inform the user of the security features.
Visibility of system status	NO It is not obvious whether the ICF is active or working. The user is provided with little feedback.	YES Visibility of system status is clear through the use of an icon in the system tray and via message boxes.
Learnability	NO It is easy for the users to learn how to turn the firewall on and off if they know where to look.	YES ICF is easy to turn on and off. The new interface has the same look and feel as Windows. This means it is easy to learn for someone who is familiar with Windows.
Aesthetic and minimalist design	YES The ICF is unobtrusive and does not annoy the user.	YES The user is only made aware of the ICF when necessary.
Satisfaction	NO Most users will not even be aware that their computers can be protected by the ICF.	YES The inclusion of an icon in the system tray should improve the users' experience and increase their satisfaction.
Do the interfaces lead to trust being developed?		
Trust	NO It is difficult for users to trust something which they are not made aware of.	YES The users are made aware of the firewall and informed of the firewall's actions.

8 Conclusion

The interface of a system is important and cannot be neglected, particularly in a security environment. By applying the HCI-S criteria, a compromise can be reached between the seemingly diverse goals of HCI and security. This will lead to a system which is easier to use and which is more secure.

The Internet Connection Firewall was used as an example of how the HCI-S criteria can be

used to improve an interface in a security environment. Only a few simple modifications, some of which have been demonstrated, need to be made which will greatly enhance the users' experience and their computer's security.

The usability of security interfaces is only part of a bigger picture. Even the most user-friendly interface could be avoided by users unless there are policies in place which enforce the use of security programs. For example, a company should have a policy of always encrypting sensitive emails.

This paper showed how the HCI-S criteria can be used to improve the security of a system by modifying the interface. This objective has been accomplished by the discussion on proposals for changing the ICF interface.

The HCI-S criteria can be used by software engineers to ensure that usability is developed into the security interface. The criteria can also be used to evaluate the interfaces of new security products. The criteria will provide direction, from a security point of view, on how an interface can be improved.

References

[BOTH02] Botha, R.A., Principal Lecturer, Business Information Systems, Faculty of Computer Studies, Port Elizabeth Technikon, South Africa. email, February 2002 (reinhard@petech.ac.za)

[CARR03] Carroll, J., (ed), 2003. *HCI Models, Theories, & Frameworks: Toward a Multidisciplinary Science*, Morgan Kaufmann.

[DHER00] D'Hertefelt, S., 3 January 2000. *Trust and the Perception of Security*, http://www.interactionarchitect.com/research/report20000103shd.htm

[FIRST02] Online banking web site for First National Bank South Africa, 2002. http://www.firstonline.co.za

[[HEWE96] Hewett, T.T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. and Verplank, W,. 1996. *ACM SIGCHI Curricula for Human-Computer Interaction*. http://www.acm.org/sigchi/cdg/cdg2.html

[MEYE98] Myers, B.A., 1998. A Brief History of Human Computer Interaction Technology, *ACM Interactions*, Vol. 5 (2), March 1998, pp. 44—54.

[MICH01] Michels, S., 1995. *Co-writing, Look and Feel!*, Masters Thesis, http://infolab.kub.nl/pub/theses/w3thesis/Hci/hci.html

[MICRO01] Morgan, D., 2001. Microsoft Corp http://www.microsoft.com/windowsxp/pro/techinfo/planning/firewall/default.asp

[MOLICH90] Nielsen, J. and Molich, R., 1990. Heuristic Evaluation of User Interfaces, *Proc. ACM CHI'90 Conf.* (Seattle, WA, USA, 1—5 April), pp. 249—256.

[NIEL94] Nielsen, J., 1994. *Usability Engineering*, Academic Press Inc

[NIEL00] Nielsen, J., 2000. Hard-to-use sites will fail, *The Irish Times*, January 2000. http://www.ireland.com/newspaper/computimes/2000/0110/compu1.htm

[NIEL02] Nielsen, J., Ten Usability Heuristics, http://www.useit.com/papers/heuristic/heuristic_list.html

[OXFO95] *Oxford Advanced Learner's Dictionary*, 1995. Oxford University Press

[PUZZLE] Puzzle pieces. http://www.sfwmd.gov/org/wrp/intro_puzzle.html

[QUEST] Question Mark. http://www.headthing.com/headthing.htm

[RICH03] Richardson, R., 2003. *2003 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, www.gocsi.com

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

[WEBSI03] Windows XP Captures One-Third of O/S Market on the Web, 13 May 2003. http://www.websidestory.com/pressroom/pressreleases.html?id=193&ctl=x08x087h27h2