Assessing the Usability of Security Features in Tools and Applications

F.Moustafa and S.M.Furnell

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Today's Security Software Tools and Applications such as Firewall, Anti-spyware, and Anti-Virus are developed in such a fashion that they provide only partial guidance to the end-users. Because of which though end users have advanced security software tools in hand they were unable to utilize the security features inbuilt. This research focuses on improving the usability of security features in Tools and Applications. The research evaluates 6 security programs and 3 web browsers for usability issues. User's perception/understanding on those usability issues were surveyed among 30 participants. The evaluation and survey results reveal that security awareness among end users and usability awareness among product vendors are in developing stage. The major usability issues addressed in today's security products are inappropriate help documentation, overloading the window with rarely needed features/information, using high technical vocabulary terms, missing of most frequently used actions in home page, protection-less password protection settings and hectic default configuration settings. The suggested solutions and alternative interface styles are provided for these potentially confusing interfaces to improve the usability of the security features in selected tools and applications.

Keywords

Usability, Security, Guidelines, Web Browsers, Firewall, Anti-virus, Anti-spyware

1 Introduction

It is evident that today's technology-based solutions are presented in such a way that user cannot understand and utilize them effectively though good safeguard features are available in hand. The security requirements of the product will be fulfilled only when the end users are influenced by its usability. The International Organization for Standardization (ISO) defines Usability as "effectiveness, efficiency and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment". These factors depend upon the user and their technical level (Furnell, 2007).

Human Computer Interaction (HCI) is the study of interaction between users and computers. The main goal of HCI is to improve the interactions between users and computers; to design the user-friendly interface which breaks the barrier between the user's need and computer tasks. The study was initially conducted by Saltzer and Schroeder (1975) resulted that end users were unable to take security decisions which made them to compromise security than usability. After 3 decades of

experiment with HCI guidelines, Johnston, Eloff and Labuschagne (2004) refined HCI guidelines to HCI-S guidelines. These guidelines helped to improve the interface usability so that the system becomes more secure, robust and reliable.

Furnell *et al* (2006), pointed some desirable key points that will instigate the usability are understandable, locatable, visible and convenient. These factors should be investigated in current products for deficiencies. In 2005, the team conducted survey on 340 end users to investigate their understanding on some generally used tools and applications and how comfortable they feel in configuring security-related settings; responding to security-related events and messages; specifying policy and access rights.

The team focussed on the security related features within Windows XP firewall, Internet Explorer, MS word etc. The finding revealed that every security product should have training on how to use its security features and also recommended to improve the interface with clearer language and additional help facility. Finally the group recommended for further research on alternative interaction styles that might guide the user to secure their system in more intuitive ways.

In the another study Furnell (2007) compared the IE7 and Word 2007 interfaces with Nielsen's Usability Heuristics and concluded that usability is not served according to user's perceptive and added that some of the usability problems were rectified in the current version of security tools than their earlier versions.Not only end users, who suffer from usability problems, but also system administrators. This can be witnessed from the survey conducted by Furnell *et al.* (2004) on 160 system administrators revealed that above 50% of the administrators faced difficulty during installation of security analysis tool and 71% faced difficulty during configuration of the same.

Other than collecting information on general usage of security tools and applications, investigating each security product for usability under different circumstances also gains valuable results. Dapeng performed his survey on personal firewall usability with 18 users (technical users and 10 non-technical users). He considered 6 firewalls which were used widely and concluded that personal firewalls were designed for end users and should it be designed for all level of users. Also provided suggestions on how the interface should be for each level of user (Dapeng, 2007).

Few of his suggestions upon improving the interface were, expert users should be prompted with security warnings quite often so that they know about their potential risk on computer; normal users should be prompted with only appropriate security prompts with detailed information about modification of files during execution. Whereas, beginners should be informed about those security prompts which pose high security risk.

The aim of this research paper is to improve the usability of security features in Tools and applications. This paper includes the evaluation criteria of this research followed by survey outline. The next section of this paper, presents the survey results followed by the evaluation analysis and discussion of selected security tools and applications. The research findings are presented to summarize existing usability

issues followed by the suggestions to improve the usability on the security tools and applications.

2 Evaluation Methodology

The security products selected for evaluation in this research are

1. Apple Safari 3.1.2 (525.21)
2. Mozilla Firefox 3.0.1
3. Windows Internet Explorer 7 (7.0.6001.18000)
4. Comodo Firewall pro version 3.0 (Free)
5. Outpost Firewall Pro 6.5.2358.316.0607 (Trial Version)
6. Kaspersky Anti-Virus 7 (Trial Version)
7. Norton Anti-Virus 2008
8. McAfee Security Centre 2009 (Trial Version)
9. Webroot software Spy Sweeper 5.5 (Trial Version).

Home Page of a Security program should clearly inform the user about the entire system status and available security features. The home page should display all the frequently used options/ navigation links. Other than home page, there are few actions and requirements often used by end users. Things to be considered in the security product interfaces are

1. Recommended configuration settings should be set as default during installation.
2. Home Page should clearly present the system status.
   a) The System Status- Is the computer secured or Not
   b) Quick link to scan/update the program
   c) Date of last scan/update was performed
   d) Indication if any intrusion attempts/virus detected/actions blocked
      - Link to view the problem
      - Link to action to be taken for the problem
   e) The Essential Security Tools/options
   f) Help
3. Security options and warning information should be stated clearly and precisely in plain language to avoid risk
4. User control and freedom – undo and redo
5. Proper feedback for user's action
6. Handle errors appropriately
7. Password protection to protect the unauthorized change of security settings
8. Appropriate help
9. Security should not reduce performance
10. Safe uninstall

Each security product was evaluated based on these 10 evaluation criteria. The research found many interesting usability issues within the security tools. The most common usability issues were picked for the survey questionnaire. The questionnaire consists of 19 questions and these questions focussed on 3 categories; Personal details, Security and Usability awareness & Understanding and suggestions.

We considered collecting survey from people who spend ample time with computer would be preferable. Data entry work place and university campus were selected. The project aims and objectives were printed and distributed to 33 participants for getting acceptance to participate in the survey. 30 interested participants gave their approval through signature, after which questionnaire was distributed as hard copy. The completed survey forms were then collected back from the participants after two days.

3 Survey Results and Discussion

Age range of the participants were collected which is shown in figure 1. This clearly states that majority of the participants were from 21-30 age range followed by 31-39 age range. Figure 2 clearly says that majority of participants were students followed by 26% of employees.

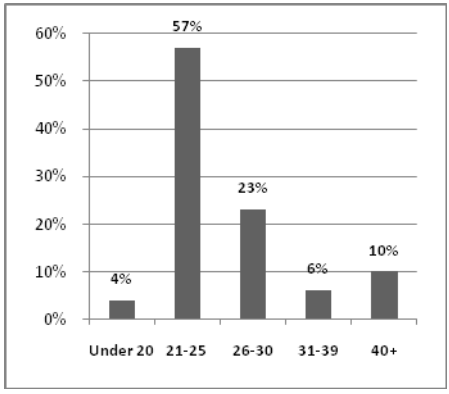

Figure 1: Age range of Respondents

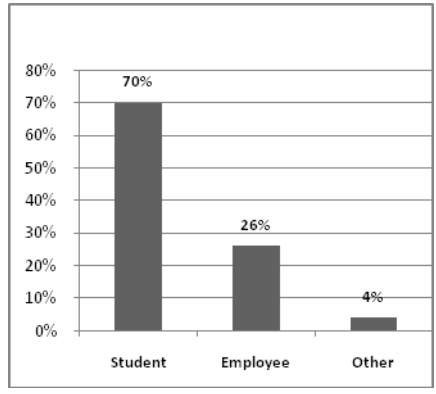

Figure 2: Identification of Respondents

The survey results reveal that 83% of the participants were intermediate user, followed by 10% of expert user and the rest were beginners.

The survey results on security awareness i.e. when end users were asked about storing personal information in their computer. The results revealed that 57% of the respondents do not store personal information in computer, followed by 23% of the respondents store only username and not password. And 17% of the respondents store both their username and password. Observing this result it is evident that security awareness among the end users is in progressing stage.

The survey results on usability awareness i.e. when end users were asked about compromising between usability, security and system performance. The results revealed that 63% of the end users would compromise advanced security features if usability and system performance are good. 20% of users would compromise usability if advanced security features are available and 17% of the user would compromise system performance if advanced security features are available.

Observing this result it is evident that usability awareness among end users is in satisfactory level, but still need to be considered for further improvement.

When respondents were asked about their prefered format for displaying the description of a security option, 40% suggested that they need help description at the tooltip followed by 23% of the end users suggested that clicking on the help icon should navigate them to specific security option. 13% of the respondents suggested that they need help description in the same window without clicking anything and another 13% suggested for main help document. The rest of the respondent preferred help description in the same window after clicking individual help icon provided for each security option. Observing this result, it is evident that majority of the users prefer their software to navigate them to appropriate help document rather than browsing through lengthy help document.

When the end users were presented with interface which had high technical vocabulary term *scan archives*, the results revealed that only 50% of the end users could understand the meaning of archives. 30% of the respondents could not understand the meaning of archives, followed by 20% understood partially. This result reveals that interfacing high technical vocabulary terms in setting window will impede the user from making any configuration settings.

Similarly, when end users were presented with interface which had system oriented term *Turn ON bloodhound Heuristics,* the results revealed that only 3% of the end users could understand the term and the majority of the respondents could not understand the meaning of *bloodhound Heuristics.*

When the end users were asked about the automated scanning of the failed scheduled scan, their responses were shown in Table 1. Observing this result, it is evident that 43% of the end users expect that failed scheduled scan will restart automatically when their system restarts, which is not actually the case in today's security products.

Consider you scheduled your anti-virus program to scan your computer on every Monday at 2 pm as. By mistake you turned OFF your computer at 1.45pm and then turned ON at 2.10pm. So, now when you log on to your computer, Will the anti-virus program start scanning your computer for virus?	Amount in %
Yes	43
No	33
Do Not Know	23

Table 1: Result on scheduled scanning

From the survey results, it is clear that the usability in today's security product is still a dream goal for the end users. However, adding security features in today's security products is always a goal for security product vendors. Security awareness among end users and usability awareness among product vendors should go in parallel, failure of which will lead to decrease in usability of the product and increase in vulnerabilities.

4 Research Findings

The overall study of this research found many interesting usability issues:

The survey results of this research clearly proves that the security awareness among the end users is in developing progress, and still need to be developed for further improvement. However, usability awareness among the security product vendors is in under-developing stage. The survey results itself revealed that most of the security software interfaces were not designed based on the usability guidelines; instead they were built to enhance the security features within.

From the evaluation of web browser products, it is observed that security options of browsers are unsecured by exposing the personal information like username and password. Though it benefits the user in some case, it also exposes their personal information to strangers. This research provided suggested solution for this issue by providing additional options and master password feature. Also browser information window fails in its function to inform the user about its progress in the logical way that end user could understand.

From the evaluation of 6 security software, it is observed that many security tools do not qualify the evaluation criteria of this research and usability guidelines of Nielsen, Shneiderman and Furnell *et al*. The home page of the security product which is suppose to inform the user about system status and suppose to possess the frequently used options, is not fulfilled in many of the today's security products.

A surprising factor is that most of the security products do not have a 'Help**'** option in the home page. Even if they provide the one, it does not have appropriate document in appropriate way the user needs. Either they provide very less information or overload the settings window with full of help information. This research provides the suggested solution for help format by surveying the end user's perception on help format.

The most frequently used options like Scan, Updates, etc., should be accessible to end users in home page itself. But the research found that not most of the security products do it. Instead of providing the necessary tools in the home page, they accumulate the page with rarely used services/functions like Highlights, Tip of the day, etc.

The next usability issue encountered in majority of the security products is 'Default settings' **(**For resetting the product to factory setting**)** option, which is not even visible in one of the security product. Even if they provided the one in the software, it is presented with high technical vocabulary terms and not in plain language. Other than default settings option, the settings window for scanning the computer, adding applications to firewall list, etc., also designed with system oriented terms and had not enough options for ease use of those settings. If this persists, then modification of settings might leave the user to risk, which in turn reduces the usability of the product.

Next issue is password protection of the security settings, which is interfaced in the way that it actually does not protect the security settings. Today's security products are interfaced in such a way; if password protection is enabled, the software will prompt for the password only to enter the settings window and it no more prompt for the password for further modifications of the settings. This interface would attract the strangers to modify the settings of the software in the absence of the administrator.

Also the alert windows which are suppose to inform the user about the intrusion attempts, existence of virus/worms, etc., should inform the user about the threat details. The research found that most of the security products alert window appears only at the moment the attack encounters, and it no more appears to user even in the home page. If the attack was encountered in the short absence of the user, then the user might not know about the threats fought by his/her security software. Today's security products inform the user about the system status only partially.

When user feels that no more he/she needs the product, the software should assist in clean un-install of the product. But few of the security products do fail in this clean un-installation by still running the product supported toolbars/features in the system without informing the user during un-installation. This action might frustrate the user, who actually needs everything of everything to be cleaned/un-installed. These usability issues found in evaluated security tools and applications were analyzed.

5 Research suggestions

The suggested solutions to improve these usability issues are

- Focussing on the interface of the home page, this should clearly visualize the entire security status and should possess the frequently used options.
- Focussing on the help format and its contents, this should clearly present what explanations do actually the user needs in the right place.
- Focussing on relative visibility of the page, the interface window should possess only relevant information and should not contain irrelevant/rarely needed information.
- Focussing on appropriate words for security options, by thinking of the word that actually user uses to represent an action.
- Focussing on not using high technical vocabulary terms in settings window.
- Focussing on including all the basic function that the user needs like resetting the product, providing help document, etc.,
- Focussing on security of the settings that the user made; the product should allow only the authorized modifications.
- Focussing on informing the user about system status at the right time; especially most important alert windows should be displayed until user closes it.
- Focussing on clean un-installation of the product to get positive feedback about the product as well to let the user's to use the product later.

If the above mentioned lists were checked in the security products, then the usability of the product could increase.

6 Conclusion and the Future

Current versions of selected security products were investigated for improving the usability features of tools and applications. The most common usability issues were picked for the questionnaire and distributed among 30 participants. The survey was conducted on different level of end users from novice to expert users. The survey results and evaluation results were compared and analyzed. The hectic interfaces under different security products were discussed for usability issues.

The major usability issues addressed in today's security products are not appropriate help document, overloading the window with rarely needed features/information, using high technical vocabulary terms, missing of most frequently used actions in home page, protection-less password protection settings and hectic default configuration settings. The suggested solutions and alternative interface styles are provided for these hectic interfaces to improve the usability of the security features in selected tools and applications.

The research found security awareness among end users is in progressing stage. As security awareness increases among the end users, it would directly increase proportion of security products. So the security product vendors were trying to increase the usability of the product by revising the usability issues of their previous product.

The future work of this research could be performed on the upcoming versions of the same security products evaluated in this research. Usability issues pointed in this research could be re-evaluated in the upcoming versions. If the occurrence of the same usability issue was detected, alternative interfaces could be designed. The functional prototype of alternative interfaces could be created using a simple development environment such a Visual Basic.

7 References

Dapeng. J, *Personal Firewall Usability- A survey*, [Online] Available: http://www.tml.tkk.fi/Publications/C/25/papers/Jiao_final.pdf [Date accessed: 24 Jan 2008]

Furnell, SM (2007) 'Making security usable: Are things improving?', Computers & Security 26(2007), 434-443.

Furnell, SM. and Bolakis, S. (2004). "Helping us to help ourselves: assessing administrators' use of security analysis tools", *Network Security*, February 2004, pp7-12.

Furnell, SM., Jusoh, A., and Katsabas, D. (2006) 'The challenges of understanding and using security: A survey of end-users', Science Direct, Computers & Security 25(2006), 27-35.

Johnston, J., Eloff, J.H.P and Labuschagne, L. (2004), 'Security and Human Computer Interfaces', *Computers and Security* 22(8), 675-684.

Saltzer, J and Schroeder, M. (1975), 'The Protection of Information in Computer Systems', *in Proc. IEEE* 63(9), 1278-1308.