Improving the Usability of Security Features in Tools and Applications

B.Rangarajan and S.M.Furnell

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The purpose of this research is to identify, investigate and improve the usability of security features in tools and application. Users and application developers can benefit by the end of this research after understanding the concepts of usability and how an alternative approach can be useful among the tech-savvy users as well as product developers who can think of making a security much more usable and effective. The main objective of the research is to investigate the issues surrounding the usability of security features in various tools and applications and try to familiarize with the issues. Further, a specific security tool is taken for study and based on which, a usability study is carried out in order to find out the users' attitude level on usability as well as how they understand the security features present in a tool. Also developers too need to focus more on usability and make the users more attracted towards using a product more freely than any constraints. The analysis section of the usability study would be helpful in identifying the common usability issues and participant's attitude level towards handling the security features present in an antivirus application. Based on which, a mock interface implementation would be designed and developed & try to make the security feature more usable. This would benefit end-users and product developers for the future works.

Keywords

Security, usability, user interfaces.

1 Introduction

In our modern technology-focussed world, the need for computer security is ever demanding. There have been numerous developments in the field of Computer and Information Security. As a result, there have been a lot of applications and systems developed and deployed worldwide, such as antivirus, Firewall, Intrusion Prevention/Detection Systems. Although, they provide a good protection level to all kinds of users and consumers, there would be a question arising in the mind whether are these products and their features usable? The answer would be fairly No from an end-user perspective. Developers on the other hand focus upon the technology that they tend to embed into a product and sometimes they forget that the product ought to be useful by a fair means of users. So the need for usable security arises when a security is not understood, learnt, clear enough for any user.

2 Research Aim & Objectives

The main aim of the research is to investigate & identify the issues that surround usability in general. Further to research on the issues surrounding usability of security tools and security features in other tools and applications. Later, a usability study would be conducted in order to get a good research based detailed study on usability issues and users' attitude towards using a security feature in a tool or application like antivirus. To accomplish this, the aims and objectives have been break down into smaller tasks so as to make the thesis a good research based and to provide a good valuable source of information on usability. Some of the main objectives of the research are listed below:

- To investigate the need for security, usability and usable security in an application.
- Further identify the key issues surrounding within the reach of security of usable security in any tool or application.
- Based on this research and a further study that is to be carried out on usability among different users will help to analyze and identify the problem areas where the users find difficult in using the antivirus application.
- This would help to improve or suggest an alternate approach to software developers in the design of usability features present in a tool or application.

3 Usability of security features

Computer and Information Security in this modern world are growing as most demanding needs in various organizations. Home users and other end-users too started seeing security as one of their real-time demand whenever they used their computers. But some of the security features of the products or the products itself are developed for the purpose of security are not usable to users. According to AOL/NCSA 2004 survey titled 'Online Safety Study', nearly 90% of the respondents did not know what action has to be taken when a scan report is shown by their anti-spyware software. Adding to this, a 33% of the users did not understand their firewall's functionality mostly and 20% of them did not understand completely. (AOL/NCSA, 2004) The reason is the products that they were using were not fully usable. So the security that was aimed at was of no use because of any usability to the users.

"*Lack of Usability can cause problems which, at one end of the scale, frustrate or annoy the user and, at the other end of the scale, might be life-threatening*" (Jordan, 1998)

Usability not only frustrates or annoys a user; it also can create great losses to the organization as a product manufacturer in terms of reputational loss, financial loss, loss of loyal customers. (Klien Research, 2010). Thus usability is very much important in a product or application. Usability can be defined by many ways. In computer perspective, usability can be referred to as Human Computer Interaction (HCI).

“Human Computer Interaction, or HCI, is the study, planning, and design of what happens when you and a computer work together. As its name implies, HCI consists of three parts: the user, the computer itself, and the ways they work together”. (Danino, 2001)

Also usability cannot be defined or considered as a single dimension factor. It is a multi-dimension factor where it needed to be characterized and categorized. Usability of a security feature depends on some of the factors like: (Usability, 2010)

- Ease of learning
- Efficiency of use
- Memorability
- Error frequency and severity
- Subjective satisfaction

4 Barriers to Usability

Although, there are a lot of factors regarding usability, there are some barriers that stand as an obstacle in achieving the usability. These barriers are both technical as well as non-technical barriers from an end-users perspective. (Johnston, Eloff, Labuschgane, 2006) They are :

- Lack of Users’ Knowledge
- Complex design interface
- Technical issues:
- Visible and simple details
- Frequent Errors or alerts

To achieve a better usability, first one has to investigate and identify the issues. Later, the cause for the issues followed by studying the issues and figuring out how to overcome it has to be analyzed. Evaluating Usability or identifying the issues surrounding usability is a different approach altogether. One cannot choose a specific method of evaluating. There are various methods like: (Klien Research, 2010)

- Usability Studies
- Contextual assessments
- Competitive analysis
- Heuristic evaluations
- Cognitive walkthroughs
- Focus Groups
- User Surveys

Thus using one of the methods specified above, one can identify and investigate the issues surrounding the usability amongst the end-users. In this research, usability survey is adapted as the evaluation method for to understand the users’ attitude level as well as knowledge level on security features of their antivirus application that they use. Also users were asked about few questions related to prototypical interface depiction of security alerts to read the users' opinions on how it could create an impact on the study for this research.

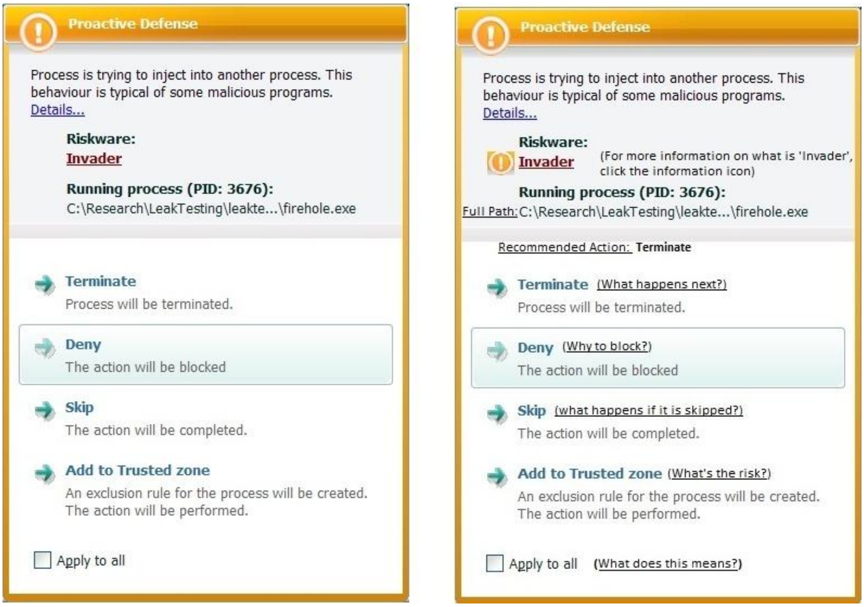
5 Usability Survey

The usability survey was conducted online and obtained responses from 108 participants around the world. It was hosted online within the Center for Security, Communications and Network Research (CSCAN) and it was held online for a period of nearly 10 days and there were a total of 133 responses out of which only 108 were completely filled. So the results of the 108 respondents were considered for the final analysis in this thesis. The majority of the participants who responded were in the age group of 18-25 and next highest participant group were aged 26-35. Participants were asked questions about their opinions on antivirus features that they use, alerts they encounter on a daily basis. Most of the participants felt that their antivirus provides sufficient information on the security alerts but many felt that the information provided by them was too difficult to understand due to insufficient information, too much technical involved, confusing information etc.

When asked about whether their antivirus product provides sufficient information on the security alerts that is encountered, 66 participants answered 'Yes' and 42 respondents felt their antivirus did not provide sufficient information on encountering security alerts. The next set of questions were based on their choices between using an antivirus, understanding the antivirus or is it both easy to use and understand with regards to their personal antivirus application. Out of all participants, 48 participants felt that their antivirus is good enough to ease of use than trying to understand what it is. Some 24 participants felt that it was easier to understand what it does than try using it. And finally 38 respondents felt that their antivirus is both easy to use as well as easy to understand. Asked about whether their antivirus software provides appropriate guidance on which action to be taken in case of a security alert, 67 participants felt they did assist them while 41 others felt that their antivirus products did not provide proper guidance in taking an action on alerts who accounts to 38% of all respondents.

Participants were asked how they usually manage to handle a security alert or any other warning messages from an antivirus. About 37% of the participants said that they would look the internet or the antivirus website for additional information while roughly 30% of them felt they would take default action or seek someone's additional help on this to take a final action. About 7% of the participants said that they would take action upon their experience related to their previous encounters and depending upon the security alert, it would be better to predict their actions. This shows the participant's attitude level. Although there were more participants who felt that they would take default action, it is clear that some users are still not comfortable in taking a decision on their own. Only very few participants he felt that they could use their experience and recall their previous encounters to tackle any security alerts that occurred again. This shows that most of the users were little bit ignorant on responding to a security alert as very few were able to handle by themselves. This could be due to either user's lack of knowledge or it could be due to insufficient information or not convincing warning message from the antivirus that had prompted the users to take upon default action.

Also many of the participants felt that automation of actions from antivirus could be helpful in handling a security alert without the intervention of the participants. About 72% of the participants felt the need for making the antivirus to take actions on their own for few default actions on default threats and reports. There are so many advancements made in the antivirus technology and features in order to make the antivirus product more effective, efficient and more usable. From a users' point of view, they would be relieved if the antivirus takes necessary action upon default alerts like that of update, scan report, virus detecting etc. But in case of a system restart or suspicious file behavior, possibility of automating the actions is quite a tough ask because most users would not like to get their work interrupted and it is not a good idea too if the antivirus takes hold of the system and tries to resolve the issues on its own. This is only for specific related problems but still it is arguable to come to a conclusion.



Proactive Defense

Process is trying to inject into another process. This behaviour is typical of some malicious programs.
Details...

Riskware:
Invader

Running process (PID: 3676):
C:\Research\LeakTesting\leakte...\firehole.exe

Terminate
Process will be terminated.

Deny
The action will be blocked

Skip
The action will be completed.

Add to Trusted zone
An exclusion rule for the process will be created.
The action will be performed.

□ Apply to all

Proactive Defense

Process is trying to inject into another process. This behaviour is typical of some malicious programs.
Details...

Riskware:
Invader (For more information on what is 'Invader', click the information icon)

Running process (PID: 3676):
Full Path: C:\Research\LeakTesting\leakte...\firehole.exe

Recommended Action: Terminate

Terminate (What happens next?)
Process will be terminated.

Deny (Why to block?)
The action will be blocked

Skip (what happens if it is skipped?)
The action will be completed.

Add to Trusted zone (What's the risk?)
An exclusion rule for the process will be created.
The action will be performed.

□ Apply to all (What does this means?)

Figure 1: Kaspersky alert (old & modified)

Some participants who were either intermediate or advanced level felt that too much additional information would also be likely to confuse a user or annoy an end-user. When they were presented with two different figures of same alert and with the second figure being the modified alert, about 82% felt that the additional information contained in the security alert were actually clear and easy to understand. When asked about their explanation to their choices, there were some few interesting things to consider. Some participants felt that the quality or level information contained is likely to help a novice or an intermediate user, but at the same time, the amount of information could eventually become too much for a user to read and he might feel difficult in understanding first of all. Also there were participants who felt that the recommendations from the antivirus on which action should be taken was really helpful not only for a novice user but also to any user who are even comfortable in using an antivirus.

When the participants were presented with a prototype of a security alert taken from that of a newer version of Kaspersky antivirus application and a modified picture as shown in figure 1, of the same alert with additional information on the actions to be taken, help regarding the actions what would happen after taking upon the certain action etc. Out of 108 participants, 89 of them felt that the figure that was modified to have additional information contained sufficient information and helped them in learning and understanding the alert in a better way. Also 79% of the participants felt that the level of detail present in the modified alert was appropriate and very few felt that it was vague and too much confusing. Asked about whether the alert would benefit the user, 67% of the participants said that it s likely to inform the user. But some advanced users felt that too many details were clustered and it was unnecessarily detailed information that even a novice user would be scared of forever. After analyzing the survey, it is found that majority of the users felt that security alerts should be meaningful, clear, provide sufficient advice on what actions to be taken and what would happen if a particular action is taken upon by the user. Also 78% of the participants felt that antivirus should be automated in handling a security alert message without requiring the intervention of the users' choice.

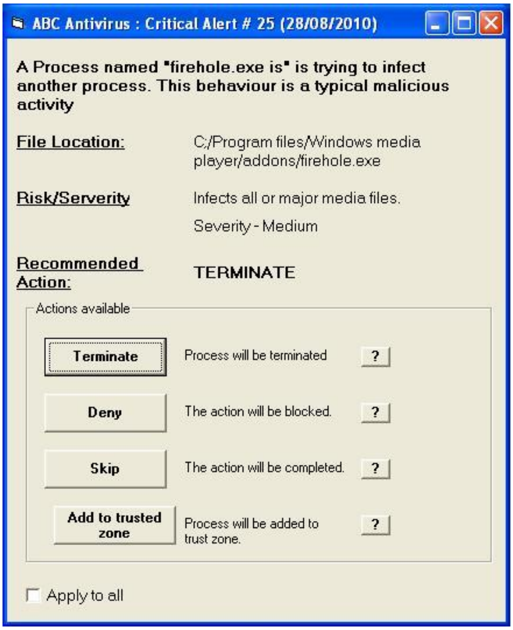
A set of participants felt that the modified alert is really helpful in understanding the information not only easily but also in a clearer way. In addition to the participants' understanding, the figure could have tweaked in a better way. As discussed earlier, the original security alert taken from figure 1 & 2, there are some things that is missing or not added. When looking closer at both those figures, it is evident that it is a security alert from an antivirus application. But looking deeper in terms of overall information, one may have a suspicion that it could be a bogus or fake threat because the title window of the alert did not have the antivirus application's name as the title and instead, it had some different name that could be misleading a user. Also, when looking at figure 2, some users felt that there was information insufficiency. It had some actions to be taken as Terminate, Deny, Skip and Add to trust zone. But it did not contain any further information what each action takes. That part of information is present in the modified security alert and that could possibly help even a novice user knowing that it is from his antivirus software only. An intermediate or advanced level user would identify it easily or comfortably.

Antivirus security alerts do not necessarily have the timestamp on which each alert is generated. For example, if an alert comes up and if timestamp is checked from the reports or events section, it would show the name of the alert and the date occurred. But for this to check, a user should normally navigate through the menus of the application and a novice user would not find it easy to look at it. So it would be a good idea to have a timestamp on the title bar itself along with the alert id or number that could be generated to help the user recall or remember the previous alert occurred and any fake alerts occurred could make the user aware of it and take appropriate actions.

6 Alternate Approach to Usability

Based on the analysis of the survey results, there are some possible alternative approach that could be taken in order to provide a better usable security in an antivirus. With the results and analysis in mind, a mock implementation of a security alert interface was developed. It had the same features like that of the original Kaspersky alert but had some extra information without being clustered. The newly developed interface has a proper title name in the alert window with alert id for the users to identify. It also provides timestamp in the top of the alert window that the user can identify next alert comes up. So on this way, fake antivirus alerts can be detected and users can be aware of it.

Also in the main window, there is additional information on what is the recommended action that could be taken and there are some help buttons for each action’s clear information in a simpler language if the user wanted to know what would happen if he had to take that particular action. Also there is a short description on the risk of the file that is suspected to be the detected threat and there is a severity of the file that is infected. This could possibly help a user of intermediate of advanced user and sometimes novice user can also benefit from this by getting to know what the infected file would do.



ABC Antivirus : Critical Alert # 25 (28/08/2010)

A Process named "firehole.exe is" is trying to infect another process. This behaviour is a typical malicious activity

File Location: C:/Program files/Windows media player/addons/firehole.exe

Risk/Serverity Infects all or major media files.
Severity - Medium

Recommended Action: TERMINATE

Actions available

Terminate — Process will be terminated ?

Deny — The action will be blocked. ?

Skip — The action will be completed. ?

Add to trusted zone — Process will be added to trust zone. ?

☐ Apply to all

Figure 2: Interface designed as part of a mock implementation

Figure 2 is the newly developed interface as part of a mock implementation. It has all the require information regarding a security alert and possible actions that could be taken by the user.

Some of the distinct features and achievements of usability from this sample interface are:

- It has a good interface design with appropriate name in the title bar of the alert.
- It has a minimal design and almost same amount of information contained as in an original antivirus security alert.
- The design is Informative and learnable for all kinds of users.
- There is no clustering of information and still all the additional information is kept intact to make a user pleased while facing it.
- Error prevention is achieved in this as users after getting to know about the actions taken can prevent from making errors.
- Clarity of language is simple and easy to understand for any kind of user.
- The task identification has been appropriate that no extra unwanted information or task is performed in this mock interface.
- Design has been done in order to facilitate all kinds of users not just a novice or intermediate IT user.

7 Conclusion

The aim of the research was to investigate, identify and improve the usability of the security features present in a tool or application. Usability of an antivirus feature not only lies with the way they are designed and implemented, but also depends on the users' attitude towards it. If only a user can change his approach towards using a product, there can be a massive shift in achieving usability or any other similar feature in a product. But one cannot blame a user for not knowing about the antivirus feature as it is not quite possible for every user to be familiar with a technical product like that of an antivirus. So the organization that develops a product should focus enough on the usable security that could be really usable among all the possible users. If not, at least for the majority of those people that come across that feature or product frequently in their work or profession. Thus going back to the saying, usability is not a single dimension factor. It needs to be characterized, categorized. Thus usability could possibly be achieved better with a good combination of organization's alternative approach and users' way of approaching a product and its feature.

Although the mock implementation looks fairly simple and easy to trade of, there are quite a few limitations on it. The mock interface is only implemented based on the previous opinions from the participants on a similar interface in the survey. So this could be evaluated among a group of participants or as a focus group to know how this implementation can have impact on usability from a users' perspective. Also, the message box that comes after choosing an action is sometimes annoying to the users. So it can be replaced by a tooltip instead just moving the mouse across the action button. Further, in this thesis there was only particular feature analyzed i.e. security alerts used for creating a mock implementation. Future work could be done on some other security features present within an antivirus or any other tool or application.

Automation of antivirus' actions upon a security alert could be done in the future as part of further improvement in this research and could be evaluated.

8 References

AOL/NCSA. (2004). *AOL/NCSA Online Safety Study*. Available: http://www.inspectagadget.com.au/board/docs/safety_study_v04.pdf. Last accessed: 03 Aug 2010

Danino, N. (2001). *Human-Computer Interaction and Your Site*. Available: http://articles.sitepoint.com/article/computer-interaction-site. Last accessed: 28 July 2010.

Jordan, P. (1998). *An Introduction to Usability*. p16.

Johnston J, Eloff J.H.P, Labuschgane L. (2006). Security and human computer interfaces. *Security and human computer interfaces*. 22 (8), p3.

Klien Research. (2010). *Which Evaluation Approach to Use?.*Available: http://www.kleinresearch.com/pdf/klein_which_approach.pdf. Last accessed 13 Aug 2010

Usability. (2010). What Does Usability Measure Available: http://www.usability.gov/basics/index.html. Last accessed: 28 July 2010