Usability of Windows Vista Firewall: A Laboratory User Study

Fahimeh Raja
Electrical and Computer Engineering
University of British Columbia
fahimehr@ece.ubc.ca

Robert Boeck
Electrical and Computer Engineering
University of British Columbia
robi@interchange.ubc.ca

Ganapathy Viswanathan
Electrical and Computer Engineering
University of British Columbia
gv@interchange.ubc.ca

Pouyan Arjmandi
Electrical and Computer Engineering
University of British Columbia
arjmandi@interchange.ubc.ca

ABSTRACT
In this project we conducted a user study of Microsoft Windows Vista Firewall: a lab study followed by a questionnaire to evaluate the usability of Vista's personal firewall. Our results show that the main problem with Windows Vista Firewall is that many users are unable to open the Advanced Management Interface of Windows Vista Firewall. Our overall impression was that users were relatively unhappy with Windows Vista's Firewall. The most common complaint amongst participants was that they had trouble figuring out where to perform their assigned tasks. Once they managed to determine the correct location of where they had to perform the tasks, implementing them was rather easy.

General Terms
Experimentation, Security, Human Factors.

Keywords
Microsoft Windows Vista, personal firewall, usability analysis, user study.

1. INTRODUCTION
A firewall is a software or hardware product that helps to effectively prevent unauthorized intrusions to a private network such as an end-user's computer or a company's internal network (intranet) by filtering the influx and outflux of network traffic between the private network and the internet [4,9]. The traffic filter results from defining certain rules (policies) that the firewall will check to determine whether a certain connection should be allowed or rejected. Traffic can be filtered by various methods such as examining the source and destination addresses, protocol, or packet attributes [9]. The prevention of intrusions to a private network helps to increase confidentiality and data integrity as well as to reduce denial of service attacks [4,9]. A firewall is an essential security tool for anyone who wishes to establish a connection between their private network and the internet.

The attention to computer security has increased in recent years due to the dramatic rise in complex and malicious methods of breaking down computer security mechanisms. Microsoft included a very basic firewall called "Internet Connection Firewall" with the release of the Windows XP operating system in October 2001 [12]. Unfortunately, there seemed to be very little effort in designing the firewall to be user-friendly. The firewall was disabled by default and required the end-user to have prior knowledge of this default setting otherwise he/she would have an invalid sense of security [12]. Also the firewall configuration display was relatively hard to access because it was embedded behind the network configuration screens [12]. As a result, few people utilized the benefits of the firewall [12]. After major instances of Windows-based attacks in 2003, Microsoft improved the usability and functionality of the Windows XP firewall ("Windows Firewall") to counteract the influx of Windows-based security attacks [12]. On January 30, 2007, Microsoft released Windows Vista which included a new advanced management firewall interface to allow the end-user to have more control over the functionality of the firewall. Microsoft has claimed that Vista firewall has multiple improvements regarding usability and flexibility for the end-user [12]. This claim needs to be analyzed more thoroughly through independent and possibly less biased research.

In this project, we conducted a laboratory user study on evaluating the usability of Vista firewall for personal use. We used a personal context because in general, corporations and organizations do not use Windows Vista as their operating system. Even if corporations have started using Windows Vista, the care taken for the security of their organization would lead them to use other firewalls rather than the Windows Vista Personal Firewall. This report divides itself into the following sections: Section 2 details the impact of usability in computer security. Section 3 depicts a number of security and usability issues that make firewalls interesting to study, followed by Section 4 which outlines related work of usability in computer security. Section 5 entails the heuristic evaluations performed, in order to come up with a list of "typical user tasks" for our laboratory study. Section 6 & 7 details the tasks and questionnaires used in our laboratory study. Section 8 and 9 outlines the results and discussions of our laboratory user study. Conclusions made about the usability of Windows Vista Firewall through our laboratory study are provided in Section 10.

2. USABILITY AND SECURITY
Computer security mechanisms such as firewalls have been developed with a primary focus on the theoretical aspects of securing a computer such as strong cryptography and advanced firewalls [8, 10]. Employment of a security mechanism in the real world based solely on the theoretical aspects of computer security can cause the security strength to be neutralized when the user misuses the security mechanism [7, 8, 10]. User misuse can be caused by an unclear understanding of certain important aspects of the security interface such as configuring an access control mechanism to cause secret information to be readable by everyone as a result of the user misinterpretation [3, 7, 8, 10]. However,

basing a security mechanism solely on how usable it is can reduce the overall strength of the security as well. There should be a balance between theoretical security and usability which will establish an effective method for securing end-users' assets [7, 8, 10]. Without this balance, a user's assets are susceptible to malicious attacks. For a software product to be usable, the software must effectively convey the security tasks the user must perform [10]. The user also must be able to perform the required task successfully within an acceptable amount of time (to reduce user frustration) without making any dangerous errors [10]. Also it is important that the user is comfortable in using the interface so that continued use of the software doesn't become a burden [10].

3. USABILITY OF FIREWALLS

A very interesting but under-researched security mechanism regarding usability is the firewall. Almut Herzogl and Nahid Shahmehri stated in their research on firewall usability that there are three issues that make firewalls an interesting usability research topic [3]. The issues are:

1. The level of granularity as well as the accuracy involving the end-user's decisions regarding the required firewall security tasks is very important if effective security is to be achieved. Unfortunately, most end-users are not security experts [3].
2. The end-user is usually preoccupied with other tasks when the firewall security tasks must be performed [3].
3. If the end-user does not accurately accomplish the firewall security tasks, the user's assets will be at risk [3].

If these usability issues are addressed in a usability research study, then a more clear understanding of usable security will result. Furthermore, Microsoft has claimed that Windows Vista is a superior operating system with many advanced security features [12]. This claim would need a reality check. Therefore, we decided to conduct a usability study of Windows Vista Firewall.

4. RELATED WORK

A "cognitive walkthrough" approach was used by Almut Herzogl and Nahid Shahmehri to analyze the usability of thirteen personal firewall products on Windows XP [3]. To establish the level of usability regarding each firewall, they created uses cases and misuses cases that were then applied to each firewall. The first use case consisted of the experimenters allowing a specific application to establish an outbound connection to a host on the internet using WinSCP. The second use case involved the experimenters setting the necessary firewall rules such that the Cerberus FTP Server can only connect to one specified host. The first misuse case consisted of sequential port scans using Netcat and observing how the default firewall configurations present its response to the user in such a situation. The second misuse case consisted of the replacement of firefox.exe (network-enabled) with winscp.exe and observing whether the firewall can detect such a change as well as how the firewall presents such information to the user. Upon analyzing the results of the use and misuse cases, Almut Herzogl and Nahid Shahmehri made several suggestions to improve the usability and security of firewalls. They suggested that the visibility and the ease of learning how to safely operate the firewall must be increased. Also the authors suggested that the principle of least privilege should be practiced whenever possible as well as allowing the user to correct possible erroneous decisions at a later date by periodically reminding them.

Avishai Wool analyzed the usability problems that are common in professional firewalls used by network administrators [13]. The author also discussed the benefits of using direction-based filtering in firewalls and the usability problems that arise from the direction-based filtering mechanisms that are offered by vendors. The author specifically points out that the administrators have an increased chance of making erroneous decision when the level of clarity involving the low-level functionality of the firewall is not adequate.

In addition to using a similar "cognitive walkthrough" approach proposed by Almut Herzogl and Nahid Shahmehri [3], Whitten and Tygar evaluated the usability of PGP 5.0 using a laboratory experiment [11]. The evaluation of PGP 5.0 was set against four usability guidelines which the authors found to translate directly to design priorities of software products. The authors' laboratory experiment was used to help confirm their cognitive walkthrough results involving various security risks and usability issues in a less closed and more realistic user environment. The authors concluded that PGP 5.0 lacked in many aspects of the usability guidelines they developed.

"Laboratory Experiments" and "Field Studies" were used by Chiasson et al. [1] to analyze the usability of click-based graphical passwords. The laboratory experiment consisted of a group of people that were explicitly told to repeatedly create graphical passwords while being closely observed by the experimenter. The laboratory experiment confirmed the authors' opinion that using graphical passwords improve success rates, password-entry times, and generated a favorable response from the participants. The field study was used to observe how graphical passwords worked in practice. The results of the field study were very similar to that of the laboratory experiment. The authors' concluded that investigating alternatives to common standards in design and implementation of password utilities would be beneficial to the end-user's security.

5. HEURISTIC EVALUATION

Before our user study, we performed a heuristic evaluation [5]. Our heuristic evaluation involved having two of the four experimenters examine the interface and judge its compliance with recognized usability principles (the "Heuristics") [6]. Based on this heuristic evaluation, we found several problems in Windows Vista firewall and came up with a list of "typical user tasks" for our laboratory study to validate our findings in our heuristic evaluation (see Section 6.2).

6. LABORATORY STUDY

We conducted a laboratory study in order to evaluate the usability of Microsoft Windows Vista Firewall, and to confirm that the problems we found in our heuristic evaluation were real problems. The methodology of our study was approved by The University of British Columbia's (UBC) Psychology Research Ethics Committee.

6.1 Participants

Twelve participants (2 females, 10 males) took part in this study. All were undergraduate students from the Electrical Engineering and Computer Engineering (EECE) as well as the Computer Science (CS) departments of UBC. The average age of participants was 22 years (minimum age = 20, maximum age = 24).Their average technical knowledge of computer security was 2 out of 5 (where no technical knowledge of computer security = 0, and an expert of computer security = 5).All of the participants were adequately experienced with using a computer and firewall, but only 42% of them had previously used Windows Vista. Most

importantly, none of the participants had any prior experience with Vista's firewall.

6.2 Tasks

Each participant completed a one-hour session as a part of our study. Upon the completion of appropriate consent forms and the demographic information of the questionnaire (age, gender, education, background in security and familiarity with Windows Vista's firewall), the users were introduced to the theme of our project. Subsequently, they were asked to perform the following tasks with Administrator privileges on the test computer:

1. Accessing the Firewall: In order to access the firewall, the user could navigate through Control Panel → Windows Firewall in order to gain access to the simple firewall or navigate through Control Panel → Administrative Tools → Windows Firewall with Advanced Security in order to obtain a more detailed view of the firewall (such as the configured rules, the different network adapters available, and so on). Regardless of whether the user opened the simple firewall or the firewall with advanced security, they were asked if they were aware that Windows Vista contained both. Independent of the answer to this question, the participants were asked to access the one that they did not originally open within 10 minutes. During this period, they were allowed to use any help available within Windows Vista or on the Internet.
2. Determining the Current State of the firewall: The users were asked to comment on the present status of the firewall. Moreover, we were interested in knowing how they determined this. This is a task that is infrequently done but is important. From time to time, the user may need to know what state the firewall is in, and whether his/her computer is in a secure state (or not).
3. Turning the Firewall On / Off: There are two options available on the simple firewall interface to perform the above mentioned function, namely the "Turn Windows Firewall on or off" link in the sidebar of windows firewall and the "Change Settings" link in the middle of that window. These links result in popping up the same window where the user can turn the firewall on/off under the "General" tab of Windows Firewall. There is also a "Windows Firewall Properties" link in the firewall with advanced security to perform this task which the user could simply click on in order to turn the firewall on/off. If the user did choose the simple firewall to perform this particular task, he/she was asked for the reasons behind the selected option.
4. Blocking all Incoming Connections: In order to block all incoming connections, the user should click on the "Change Settings" link of Windows Firewall, click on the "General" tab, and check the available checkbox for this purpose. Upon performing this task, the users were asked if there would be a more appropriate place for selecting this feature. If a particular user answered "yes", her/his suggestions and comments were noted. This is once again an example of a task that is frequently not done (the user may perceive some threats to her computer and, in response, might block all incoming connections) but is important. All incoming connections are blocked in the above mentioned mode and no outside program would be able to access the computer.
5. Allowing a Specific Program through the Firewall: The users were asked to allow a certain program (such as *Yahoo Messenger*) through the Windows Vista Firewall. There are two options on the simple firewall interface that allow a program to accept incoming connections and make outgoing connections. The "Allow a program through Windows Firewall" link in the sidebar of windows firewall window and the "Change Settings" link in the middle of the same window. Both of the above mentioned links navigate to the same window, where the user could click on the "Add Program" button under the Exceptions tab to add a program to the list of allowed programs. This is a task that is important and frequently performed. The user would need to be able to add custom programs in order for the programs to communicate freely with the outside world.
6. Run a specific program (such as *Windows live messenger*) that we made a rule for (which was probably blocked from accessing to the Internet): The purpose of this task was to see how the user reacts when he / she is encountered with a pop-up window asking him / her to cancel or allow the program to access the Internet. This task is specifically important because at this point of time, the user is typically busy with other tasks and could make a fast decision that might be harmful for his / her computer.
7. Opening a specific Port on the Firewall: The user may decide to host a server program that needs to accept requests and relay back information. However, this sort of program requires a specific port to be opened on the firewall. In order to do this, the user should click on the "Change Settings" link of Windows Firewall, click the "Exception" tab, and finally click the "Add Port" link. This is also a task that is frequently done and highly important. An exposed port could be a major system vulnerability. Thus, the decision needs to be made with care and be carefully managed.
8. Configuring an Inbound/Outbound Firewall Rule: In order to configure firewall rules, the user should open the "Firewall with Advanced Security", click on the "Inbound/Outbound Rules", and finally click on the "Add New Rule" link.
9. Using Firewall's Help: The user was asked to click on some of the help links offered within the Windows Vista Firewall interface to observe their thoughts about the help function in Windows Vista Firewall.
10. Commenting on the names of one link, and one button in the firewall interface before clicking on them – specifically the "Properties" button under the "Exception" tab in the simple firewall interface and "Filter" link in the firewall with advanced security interface: Upon using a heuristic analysis we were unable to determine the functionality of the "Properties" button and "Filter" link prior to observing the contents within them because the definition of the words "Properties " and "Filter" are quite abstract. Words/phrases with a more concrete definition that are not open to misleading interpretations should be used.

6.3 Data Collection

Both quantitative and qualitative data were collected during the lab study. The *Quick Screen Recorder* software [2] was installed and used to capture the computer screen in order to record all user activities, time stamps, and the total time elapsed during the experiments. Participants' responses to the demographics and post-test questionnaires were also collected. Additionally, two experimenters sat with each participant throughout the sessions. The experimenters recorded comments made by the participants regarding usability problems and their general observations.

7. QUESTIONNAIRE

The questionnaire was divided into five main sections. Section 1 focused on the demographics of the user. Section 2 focused on the users' previous knowledge of computer security. Section 3 focused on what the user experience with the interface. Examples of questions in this section are shown below:

Question 1: Have you noticed any differences between Windows XP Firewall and Windows Vista Firewall?

Question 2: With respect to the version of Windows Vista Firewall that you worked with, please indicate the extent to which you agree / disagree with the following statements (Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), Strongly Agree (5)):

1. The software is easy to use.
2. I will be able to learn how to use all the facilities if offered in the software.
3. The contents of the menus and toolbars match my needs.
4. Finding the options that I want in the menus and toolbars is easy.
5. It is easy to make the software do exactly as I want.
6. Discovering new features is easy.
7. The software is satisfying to use.

Question 3: When the firewall pop-up window appeared, did you understand the potential vulnerabilities of you decision?

Question 4: What do you think the vulnerabilities were?

Question 5: If you feel that you did not have enough knowledge of the vulnerability, why did you not click on the "More Info" link on the pop-up window?

Sections 4 and 5 focused on the Firewall configuration experience, and suggestions for Improvement and User feedback respectively.

8. RESULTS

8.1 Laboratory Study

The results obtained for each of the tasks mentioned in Section 6.2 were categorized and summarized as shown below:

1. Accessing the Firewall: Three of our participants (25% of the population) went directly to the simple firewall interface in the control panel. Eight (66% of the population) of the participants first looked for a shortcut on the desktop or the taskbar, and then went to the control panel. Of these eight participants, six of them found the simple firewall interface directly in the control panel and two of them found it in the Security Center Windows Vista. One of our participants, who did not know where to access the firewall, simply typed "firewall" in the *run* option of the *Start* menu of Windows Vista and accessed the firewall with advanced security. This was quite interesting since we did not know about this feature ourselves; none of the participants knew about the existence of two different Firewalls (Simple and Advanced) on Windows Vista. Ten of the participants could not find the interface for Windows firewall with advanced security in less than ten minutes. They were surprised when we told them that they could find it in the "*Administrative Tools"* link of the Control Panel. Moreover, we were surprised that there was no useful help in Windows Vista, on the Internet, and even worse on the Microsoft Website for Windows Vista. One problem regarding the advanced firewall is that in the simple firewall interface, there is a tab called "advanced" and 50% of our participants thought that it was the firewall with advanced security on Windows Vista.
2. Determining the Current State of the Firewall: Every participant could correctly identify the current state of the firewall since it is explicitly described in the main Window of both interfaces. But only 42% (5 out of 12) of our participants noticed the two other hints in this window (a tick with a green line for a secure state and a cross with red line for an insecure state).
3. Turning the Firewall On / Off: Every participant turned the firewall off successfully. However, we noticed that 75% of the population used the "change settings" link in the main window instead of the "Turn firewall on/off" on the sidebar of that window. These participants said that they did not notice the "Turn firewall on/off" because it was on the side bar and "change settings" was in the center of the window. Furthermore, all of the participants could tell that after turning the firewall off, the computer was no longer in a safe state because it explicitly said "it is not recommended to turn the firewall off". There was also a warning in the main window of Windows Vista Firewall.
4. Blocking all Incoming Connections: Every participant could block all the incoming connections but they had problems in finding out exactly where to perform this task. This was due to the fact that there are three tabs in the "change settings" of the simple firewall interface as follows: general, exceptions and advanced. For blocking all incoming connections one should go to the general tab where there are two prominent options for turning the firewall on/off. There is also a check box for turning the firewall on (for this particular purpose) which is not obvious at all. Therefore the participants went to the exceptions tab where they could change the settings for programs and ports.
5. Allowing a Specific Program through the Firewall: All participants could successfully add *Yahoo messenger* to the list of programs which would be exceptions, and be allowed through the firewall. But the problem was that they first looked for the program in the list of exceptions and they expected to find it in the list. Similar to the second task, there are two options in the main window to perform this task; the user could go to the "change settings" link or to the "allow a program through the firewall" link. Once again, despite the obvious link to do this task, most of our participants (75% of the population) chose "change settings" to perform it.
6. Run a specific program (such as *Windows live messenger*) that we made a rule for (which was probably blocked from accessing to the Internet): Surprisingly, all participants allowed the program to have access to the Internet. None of them clicked on the cancel button of the pop-up window, which proved that none of them thought that this could possibly be harmful for the computer.
7. Opening a specific Port on the Firewall: All of our participants successfully added a port to the list of allowed ports in the firewall. We think it was easy for them to find where to perform the above mentioned task because it is in the same tab as where they added *Yahoo Messenger* to the list of program exceptions.
8. Configuring an Inbound/Outbound Firewall Rule: All participants could easily add a rule in the firewall with advanced security, since there is a prominent link named "add rules" which shows all the steps for this task.

9. Using Firewall's Help: All participants thought that Windows Vista's Firewall help is not useful because it does not directly answer their questions and all the links just go to a "frequently asked questions" (FAQ) section. Even worse, the FAQ does not answer many questions. An example of such a question is: How to access the firewall with advanced security?
10. Commenting on the names of one link, and one button in the firewall interface before clicking on them – specifically the "Properties" button under the "Exception" tab in the simple firewall interface and "Filter" link in the firewall with advanced security interface: Only 42% of the participants could correctly guess the functionality of the button "Properties". This button takes the user to a window that contains some description of the selected program in the list of exception programs. All our participants told us that they thought this button was useless because they thought they could change the properties, but to do this they had to go to the firewall with advanced security. Only 33% of our participants could correctly identify that the link called "Filter" just changes the view of the window (for example filter by private domain will show only the rules which are applied to the private domain) and the remaining participants thought that this link would filter some connections or programs through the firewall. They thought that this link is somehow related to some functionality of the firewall instead of just displaying some specific categories of the rules.

8.2 Questionnaire

The only difference that all participants mentioned between Windows XP's firewall and Windows Vista's firewall was the firewall with advanced security. On average they agreed that Vista's firewall was easy to use but 92% (eleven out of twelve participants) mentioned that it was not easy to find the firewall with advanced security. The overall impression of the participants was that if they could find the desired option, it was easy for them to follow the task.

Table 1: Summary of user experience(Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), Strongly Agree (5))

Statement	Mean	Median
The software is easy to use	3.67	4
I will be able to learn how to use all the facilities if offered in this software.	3.5	3.5
The contents of the menus and toolbars match my needs.	2.1	2
Finding the options that I want in the menus and toolbars is easy.	1.83	2
It is easy to make the software do exactly what I want.	3.5	3
Discovering new features is easy.	1.92	2
This software is satisfying to use.	3.42	3

9. DISCUSSION

It is important to solidify our experimental results by comparing them against a trustworthy frame of reference. As such, we have chosen to take some standard usability guidelines into account [10] in order to generate appropriate suggestions for improving Vista's firewall.

As can be seen from the results of both our laboratory study and questionnaire, the users could hardly access the firewall with advanced security. After the experiments, all of our participants stated that the most important problem with Vista's firewall is that they did not know where to find the firewall with advanced security and they could not find it even after searching for it on the Internet. One of the participants said "I could find everything just by using Google but it is amazing that I could not find it [Vista's firewall with advanced security]". This definitely contradicts the usability principle that a user should be sufficiently comfortable with an interface to continue using it.

Most of our participants first looked for the firewall interface on the taskbar or on the desktop; as such, based on the provided shortcut guideline of usable software, we suggest adding a shortcut to the simple firewall interface on the taskbar and adding a link in the main window of the this interface to the firewall with advanced security. This way the user can simply access both sets of firewalls in Windows Vista. This is again intended as a compliance with the user's comfort in using an interface. Moreover, there should be a link from the firewall with advanced security to the simple firewall so that if the user first goes to the firewall with advanced security, he/she could easily switch to the simple one. This will definitely give him/her much more control and freedom which is another standard usability guideline.

Vista's firewall is quite adequate at meeting the principle of providing sufficient feedback for the user to accurately determine the current state of the system. Consequently, our subjects could easily determine the current state of the firewall both at the beginning of the experiment and during the period of performing tasks. In Vista, current state is clearly described and displayed by appropriate colors and signs. Most of the users did not notice the link for turning the firewall on/off on the side bar of the main window of the simple firewall. Although this link explicitly speaks the user's language and is simple, we think it is unnecessary to have this link here and it may be sufficient to only have a radio button to turn the firewall on/off; there is even a better solution: the user can right click on the firewall icon on the taskbar and turn it on/off. This will ensure the usability guideline that a user must be able to easily figure out how to successfully perform those tasks.

One of the usability problems with Windows Vista's firewall is that the user cannot quickly find the appropriate icons, menus and options to perform specific tasks. For example, for blocking all incoming connections, he/she has to go to the advances tab of the "change settings" window where this option is not prominent at all and does not catch the user's eye. When the user goes to this tab, the false impression is given that the only thing that can be done is turning the firewall on/off. On the other hand, since the user can block or unblock specific programs and ports on the exceptions tab, he/she might think that this is the right place to search for blocking all incoming connections. Therefore, we suggest putting the check box for blocking all incoming connections under this tab. This change is again in accordance with the guideline that a user must be comfortable with an interface to continue using it.

One of the strengths of Vista's firewall is that when a user finds the appropriate place to do the desired task, it is easy to follow it up step-by-step. Its GUI is user friendly, the colors are appealing,

and it is easy to distinguish text from the background. As previously mentioned, none of the participants were satisfied with Vista's help functions. One major aspect of a usable system is the quality of its help and documentation. To rectify this, we recommend having a link in the help file which will directly answer the questions posed by the user.

One useful conclusion that we have made from the experiments is that the average user has a very limited knowledge or appreciation of the vulnerabilities associated with security tasks. This dawned on us when we observed that every user either ignored our hoax pop-up window or allowed it to download unknown information onto the computer, without any hesitation whatsoever. Therefore, we think it is crucial for every user to possess some basic familiarity with potential vulnerabilities and thus propose a formal method of enhancing the user's education in this area.

We can confidently say that our experiments were quite successful since we managed to compile a comprehensive list of improvements to be made to Vista's firewall. It is also worth mentioning that all participants completed the assigned tasks relatively comfortably and aside from finding the advanced security firewall, all other tasks were completed within the given time frame. In fact, the average time to complete each experiment was thirty-eight minutes, even though we allocated one hour per experiment. Finally, our overall impression was that users were relatively unhappy with Windows Vista's firewall. The most common complaint among participants was that they had trouble figuring out where to perform their assigned tasks; once they managed to determine the correct location, implementing the tasks were rather easy for them. We thought this might be due to the fact that most users had not used Windows Vista in the past and they were overwhelmed to begin with.

10. CONCLUSION

We have presented the results of a usability study of Windows Vista Firewall using a heuristic evaluation and a laboratory experiment. The heuristic evaluation revealed certain usability problems inherent in Windows Vista's firewall. We then were able to generate a list of appropriate tasks for the participants of the laboratory experiment to perform. The laboratory study confirmed our hypotheses from the heuristic evaluation. By closely monitoring the actions and observations of our subjects, we determined that Vista's firewall has substantial room for improvement. In its current state, it opposes some of the standard usability guidelines such as the lack of comfort in using its interface, the lack of effective help and documentation and most importantly the user's lack of freedom and control. Consequently, we have made numerous suggestions for improvement and hopefully these can serve as a basis for enhancing the standard usability criteria currently desired in security systems.

11. REFERENCES

[1] Chiasson, S., Biddle, R., and Oorschot, P.C. Van. 2007 "A Second Look at the Usability of Click-Based Graphical Passwords", In *Symposium on Usable Privacy and Security (SOUPS) 2007*, July 18-20, 2007.

[2] Etrusoft, "Quick Screen Capture" software, retrieved on 19 November 2007. http://www.etrusoft.com/

[3] Herzogl, A. and Shahmehri, N. 2007. Usability and Security of Personal Firewalls, LinkopingsUniversitet.

[4] Komar, B., Beekelaar, R., and Wettern, J. 2001. Firewalls for Dummies, John Wiley & Sons, Incorporated.

[5] Nielson, J., and Molich, R. "Heuristic evaluation of user interfaces", In Proceedings *ACM CHI'90 Conf. (Seattle, WA, 1-5 April),* 249-256.

[6] Nielson, J. 1994. "Heuristic evaluation", In *Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods*, John Wiley & Sons, New York, NY.

[7] Rozinov, K. 2004. Are Usability and Security Two Opposite Directions in Computer Systems?.Polytechnic University.

[8] Sasse, M.A.,Flechais, I. 2005. "Usable Security: What is it? How do we get it?" In L. Faith Cranor& S. Garfinkel [Eds.]: Security and Usability: Designing secure systems that people can use. pp. 13-30. O'Reilly Books.

[9] Vicomsoft. Firewall Q&A. Retrieved on 19 November 2007.

[10] Whitten, A., Tygar, J.D. 1998. Usability of Security: A Case Study.

[11] Whitten, A., Tygar, J.D. 1999. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0.", In *Proceedings of the 8th USENIX Security Symposium (Security'99)*. Usenix.

[12] Wikipedia, Windows Firewall, retrieved on 19 November 2007.http://en.wikipedia.org/wiki/Windows_firewall

[13] Wool, A. 2004. "The use and usability of direction-based filtering in firewalls", *Computers & Security*, 23(6):459-468.