Usability Study of Windows Vista's Firewall

Pooya Jaferian
Department of Electrical and Computer Engineering
The University of British Columbia
pooya@ece.ubc.ca

Abstract

Windows Vista is shipped with a built-in personal firewall. The firewall has lots of new features over its predecessor, XP's firewall. But, previous studies showed that Vista's firewall have a set of usability problems. The goal of this paper is to address the lack of a complete and validated prototype of improved Vista's firewall interface. By providing a high-fidelity prototype that could be evaluated against Vista's firewall, the weaknesses of current interface can be shown with enough evidence, and suggested improvements could be used to fix the usability flaws in the Vista's firewall.

1. Introduction

Windows Vista™ is new Microsoft's operating system for desktop computers, which is released in January 2007. Vista offers many improvements over its predecessor Windows XP in its end-user features, core technologies and security-related techniques. One of the major improvements of Vista is its new built-in personal firewall. The new firewall provides lots of new features over previous XP Service Pack 2 firewall which is discuss more in detail in section xx.

Despite providing a set of complete features to manage incoming and outgoing connections to a computer, previous studies shows that many users fail using Vista's firewall effectively[1,2,3]. This problem is rooted in a set of usability problems in Vista's firewall. These usability problems can result in two major consequences: First, the users can not use full capabilities of the firewall; therefore, they could not manage the security of their computer effectively, and since they do not know how to manage the firewall, they may turn the firewall off in case of interference of firewall with their work. Second, the users may make mistakes in managing their firewalls. These mistakes can open the doors for external intruders to the users' computers.

These two problems, shows the importances of providing new and improved user interface for Vista's firewall. As the Vista will be the main OS for desktop computers, at least until release of the Windows 7, Microsoft's next desktop OS, the usability study of firewall, finding its problems, and proposing solutions are important problems. Hopefully, Microsoft will address these issues in the future releases Vista's service pack.

In this paper, we first introduce major tasks that may result in dangerous errors by the user. Then we will build a high fidelity prototype of the improved firewall interface using ESS[9] method. Then we will compare the prototype with the actual Vista's firewall by performing a user study. Then we will analyze the result to see if our prototype improves firewall's usability.

The rest of the paper is organized as follows. In section 2, related work is studied. In section 3, we give overview on windows Vista's firewall for those who are not familiar with it. In section 4, we detail our usability study methodology. In section 5, we give details about our research execution by showing the steps for building our prototype as well as details of our laboratory experiment. In section 6, we provide the result of our experiment. Section 7, discuss about the limitations of our work and possible future directions for research. The paper is concluded with section 8.

2. Related Work

Jaferian et al. [1] perform a usability study of Vista's firewall using respondent method. In their work, they conduct a survey of 30 participants about general knowledge of them of personal firewalls and their expectations from a good firewall. Then they recruit 8 undergrad students; let them work with Vista's firewall and subsequently interview them about their experience with vista's firewall. Finally, they highlight some weaknesses of Vista's interface and suggested some improvements.

Raja et al. [2] perform a laboratory experiment by defining a set of tasks and asking users to perform those tasks. Based on performance of the users, they find weaknesses in Vista’s firewall interface, and suggest improvements.

Chebium et al. [3] perform a usability study of Vista’s firewall based on the work done in [1] and [2]. They first perform a heuristic evaluation of Vista’s firewall and find weaknesses in firewall’s interface. Then, they built a medium fidelity prototype and evaluate the prototype by doing a user study. Consequently, they suggest improvements on their medium fidelity prototype.

3. Background

The goal of the Windows Vista’s firewall, like other personal firewalls, is to manage the connection to or from the host computer.

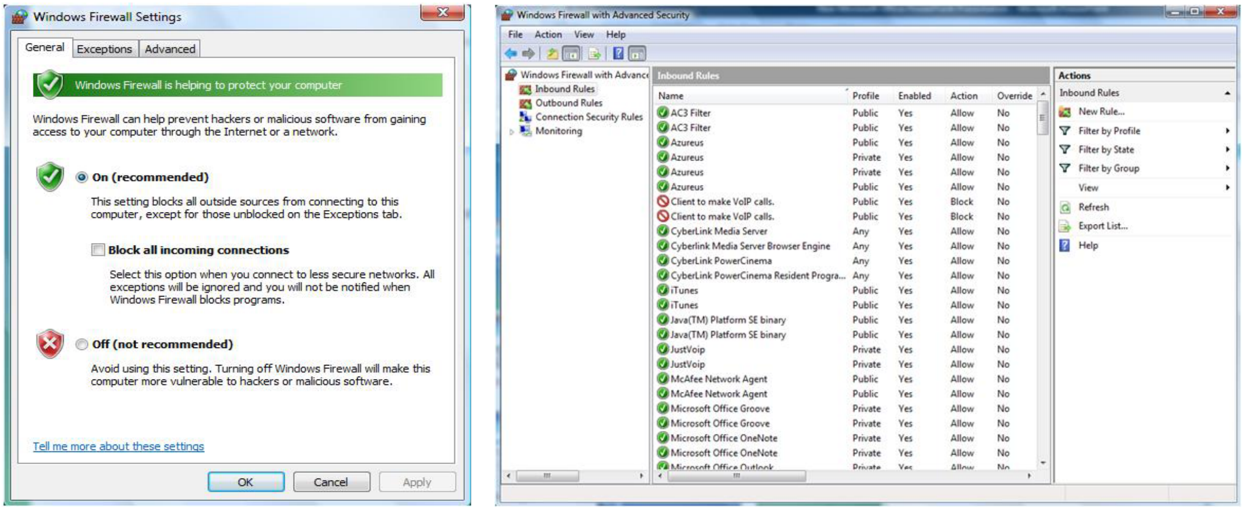
As a general rule, the Vista’s firewall blocks all inbound connections to the computer and allows all outbound connections by default. In order to change the default behavior of the firewall, the firewall should be configured by defining a set of rules that allow a certain inbound connections or block a certain outbound connection.

For the purpose of configuration, Vista’s firewall consist two different interfaces. First interface, named “Windows Firewall”, is accessible in windows control panel. It allows user to turn the firewall on or off, block all incoming connections, define exceptional programs or ports for which inbound connections are allowed, and enable or disable the firewall on a certain network connection. Second interface named “Windows firewall with advanced security” provide environment for defining fine grained rule for application or ports. Each rule can be customized to applicable on a certain network connection, profile, users, and IP addresses. Also rules can be created for outbound connections as well as inbound connections in this interface. In Figure 1, the user interface for the firewall is shown.

An important concept in Vista’s firewall is the concept of Profiles. In windows Vista, when a user connects to a new network, Windows asks user to select a profile for the network from a list of 3 profiles (Public, Private, and Domain). By selecting appropriate profiles, a user can classify her connections based on their type (and their security).

Profiles are also useful in the Vista’s firewall. Firewall can show different behavior in different network profiles. This means that the rules in the firewall are specific to a certain profile. An important issue with the profiles in Vista’s firewall is that simple interface provides management of profiles transparently. This means that when a program tries to accept inbound connections, Vista asks user to unblock the program. If user decides to unblock, the firewall automatically generate a rule for the profile that matches the current connection of the user. But the information about profiles is not shown to the user in simple interface of the firewall.

The transparency of profiles in the simple interface could make users commit dangerous errors which will be discussed in later sections.



Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● **On (recommended)**

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

□ **Block all incoming connections**

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

○ **Off (not recommended)**

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings
OK
Cancel
Apply
Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Profile	Enabled	Action	Override
AC3 Filter	Public	Yes	Allow	No
AC3 Filter	Public	Yes	Allow	No
Azureus	Public	Yes	Allow	No
Azureus	Private	Yes	Allow	No
Azureus	Private	Yes	Allow	No
Azureus	Public	Yes	Allow	No
Client to make VoIP calls.	Public	Yes	Block	No
Client to make VoIP calls.	Public	Yes	Block	No
CyberLink Media Server	Any	Yes	Allow	No
Cyberlink Media Server Browser Engine	Any	Yes	Allow	No
CyberLink PowerCinema	Any	Yes	Allow	No
CyberLink PowerCinema Resident Progra...	Any	Yes	Allow	No
iTunes	Public	Yes	Allow	No
iTunes	Public	Yes	Allow	No
Java(TM) Platform SE binary	Public	Yes	Allow	No
Java(TM) Platform SE binary	Public	Yes	Allow	No
JustVoip	Private	Yes	Allow	No
JustVoip	Private	Yes	Allow	No
McAfee Network Agent	Public	Yes	Allow	No
McAfee Network Agent	Public	Yes	Allow	No
Microsoft Office Groove	Private	Yes	Allow	No
Microsoft Office Groove	Private	Yes	Allow	No
Microsoft Office OneNote	Private	Yes	Allow	No
Microsoft Office OneNote	Private	Yes	Allow	No
Microsoft Office Outlook	Private	Yes	Allow	No

Figure 1 - (a) Windows firewall UI (b) Windows firewall with advanced security UI

4. Methodology

We first identified the tasks in which users' errors result in dangerous situations. Then, we specify these tasks in detail by performing Hierarchical Task Analysis (HTA) [10]. By applying HTA, we specify each task as a goal that is decomposed into series of sub-goals. To reach the goal, user should accomplish each sub-goal. The flow of the scenario is determined by attaching plans to the sub-goals. After scenario specification, we will design the prototype based on the External Sub-goal Support (ESS) method proposed in [9].

After building the high fidelity prototype, we perform a laboratory experiment [7] of the two interfaces. Eight participants are recruited for the study. Four participants assigned to the Vista's original interface, and the rest are assigned to the high fidelity prototype (ESS interface). As a first step of the study, participants answered a questionnaire about their knowledge and experience about Windows Vista, its firewall, as well as firewalls in general. Consequently, we presented a brief introduction about windows vista's firewall to make participants familiar with the firewall. Following the presentations, we ask participants to perform 4 predefined tasks on their assigned user interface. All the actions of the users are recorded using a screen capture program. Each user has 6 minutes to complete each task.

After the user study is finished, the information about Time to Completion and Number of Errors is recorded from the experiment data.

Based on the two measured value, we can compare the two interfaces, and show which one prevents user commit errors and help user completing the task fast.

5. Research Design

5.1. Task Analysis

As mentioned before, in this step, we identify general usage scenario's that can result users make dangerous errors. We define dangerous errors as errors that put the system in an insecure state.

We believe that the system can be leaved in an insecure state when user manages firewall rules. To identify these insecure states we analyzed the ways that firewall rules can be changed. This analysis is shown in Figure 2 and Figure 3. As shown in Figure 2, inbound connections can be managed by users using two scenarios.

First, when a new program tries to establish an inbound connection. In this scenario the Vista's firewall shows a message box that asks user if she like to unblock the inbound connection and allow the connection. As shown in Figure 4, Vista's firewall provides an expressive message that give user required information to decide about keep blocking or unblocking the program. Therefore, we find this interface suitable for its goal.

Second, when user is removing previously created rules. Consider the case where user found that program X is a malicious program. User previously decided to unblock X when Vista's firewall asked user about unblocking the program using the message box in Figure 4. Also the user did this action two times. First while using a public connection and second while using a private connection. Therefore two rules are created in the firewall that allows accepting of inbound connections in public and private profiles. To remove the rule, if user uses the simple interface of the firewall, she can only access the rule that is created for the connection which is currently used by the user. Therefore, user will only disable or remove one of the two created rules, without being aware about the second rule. As a result when user connects her computer to a network that matches the profile of the second rule, program X can make inbound connections and put system in a dangerous state.

As shown in Figure 3, when user decides to block an outgoing connection using the firewall, he can make one main mistake. The user may get confused with the general approach of the Vista's firewall that allows all outgoing connections. Therefore the user may think that all the outbound connections are blocked by default; therefore there is no need to define a rule in the firewall. Also, as outbound rules are not shown in the simple interface of the firewall, when user face a rule for inbound connections, she may think that this rule is for allowing both inbound and outbound connections. Therefore, she disables the outbound rule to prevent both inbound and outbound connections.

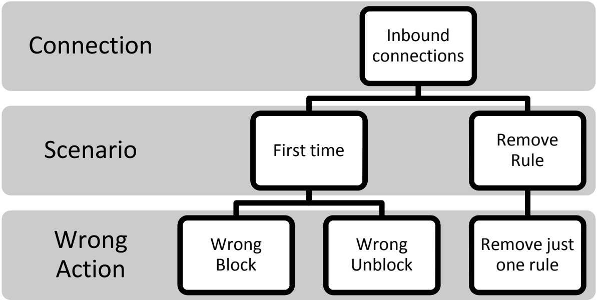


Figure 2 – Managing inbound connections

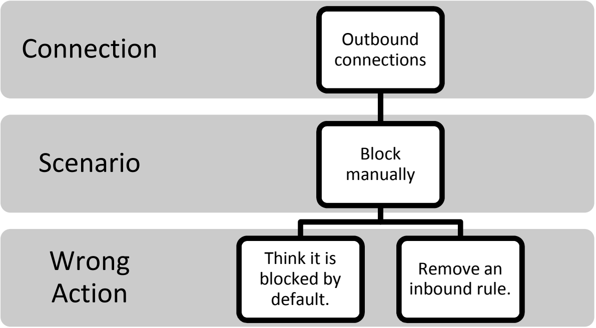
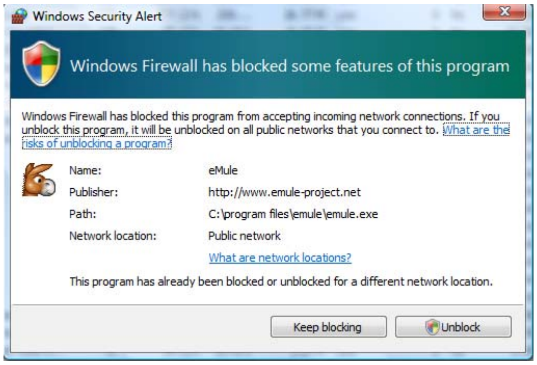


Figure 3 – Managing outbound connections



Windows Firewall has blocked some features of this program

Windows Firewall has blocked this program from accepting incoming network connections. If you unblock this program, it will be unblocked on all public networks that you connect to. What are the risks of unblocking a program?

Name: eMule
Publisher: http://www.emule-project.net
Path: C:\program files\emule\emule.exe
Network location: Public network
What are network locations?

This program has already been blocked or unblocked for a different network location.

Figure 4 – Firewall message for unblocking a program

The result of this analysis shows that there exist two critical tasks that can result insecure system state: 1- Removing a rule using the simple interface while there exist a same rule in the firewall but for a different profile. 2- Blocking an outgoing connection for a program. To improve the firewall's user interface, we design a prototype based on ESS method to support two mentioned tasks. To design interface using interface methods, the tasks that should be supported in the interface should be analyzed using HTA method. We show the result of HTA for two critical tasks in Figure 5 and Figure 6.

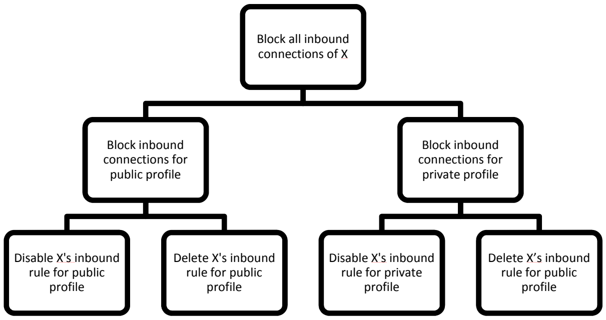

Block all inbound connections of X
Block inbound connections for public profile
Block inbound connections for private profile
Disable X's inbound rule for public profile
Delete X's inbound rule for public profile
Disable X's inbound rule for private profile
Delete X's inbound rule for public profile

Figure 5 – HTA for blocking all inbound connections of X

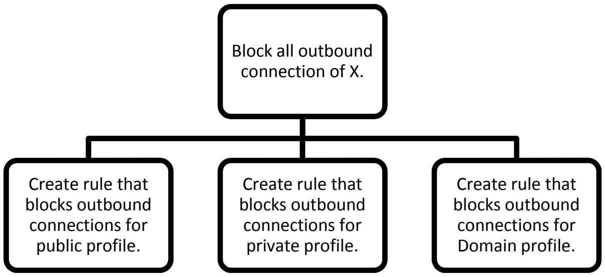

Block all outbound connection of X.
Create rule that blocks outbound connections for public profile.
Create rule that blocks outbound connections for private profile.
Create rule that blocks outbound connections for Domain profile.

Figure 6 – HTA for blocking outgoing connections of X

5.2 Prototype Design

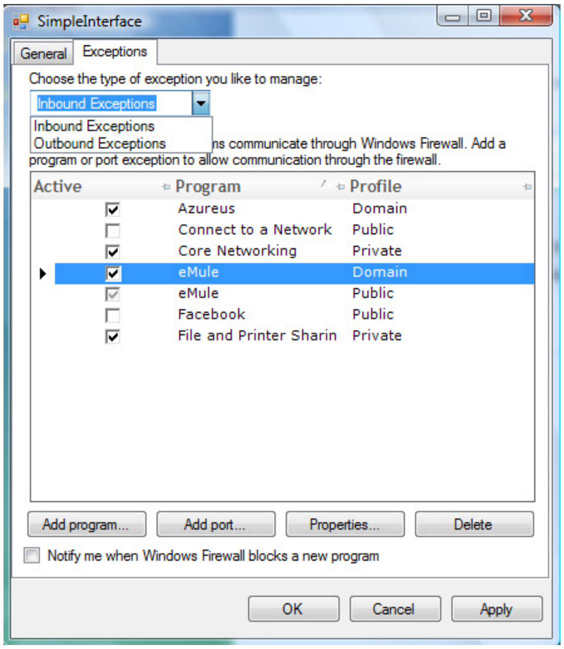
In this step, we use ESS method [9] to build a high fidelity prototype that can help users perform the two critical tasks with fewer errors and in less time.

Based on [9], ESS follows a two phase approach. In the first phase the information that user requires to complete a task successfully is found. In this phase, first the task hierarchy is traversed and for each goal, the information required to determine goal completion as well as information to find sub goals is identified. Then for the leaf nodes in the tree, the information for execution of the particular action is identified. In the second phase, the user interfaced is designed by providing the required information found in the previous phase clearly.

First Phase of ESS for Task 1: For the first task which is presented in Figure 5, the information required to determine two sub-goals successfully, is list of two rules that should be disabled as well as profile for which the rule is defined for and state of the rule (enabled/disabled). In addition, to perform the leaf actions for the Task 1, user requires a mean for disabling or removing rules. To determine completion of each sub-goal, the previously shown rules should be removed from the list or their state should be changed.

First Phase of ESS for Task 2: For the second task, the user needs the following information to determine the leaf tasks she should perform. First, the user should be made aware that all outbound connections are allowed except those that have an outbound rule. Second, the user should be able to see the available rules for outbound connections as well as the profile and state of each. To determine the goal completion, the rules for each profile should be added to the interface and be shown to the user.

User Interface Design Phase: Based on the analysis of information required to complete each task successfully, we tried to show the information explicitly in the firewall's interface. We changed the design of the Exceptions tab of Vista's firewall as shown in Figure 7.



...ns communicate through Windows Firewall. Add a program or port exception to allow communication through the firewall.

Active	Program	Profile
☑	Azureus	Domain
☐	Connect to a Network	Public
☑	Core Networking	Private
☑	eMule	Domain
☑	eMule	Public
☐	Facebook	Public
☑	File and Printer Sharin	Private

Figure 7 – Prototype designed based on ESS method

As shown in this figure, all the information about inbound and outbound connections, their activation status, their profile, and the description about the behavior of firewall for inbound and outbound connections is shown.

To provide the same experience as working with real Vista's firewall for the user, we make all the buttons in the interface functional. Therefore, a user can add, or delete programs or ports as well as changing properties of each rule. Also we simulate other tabs of Vista's simple interface to provide consistency with Vista's firewall. It is also worth mentioning that the prototype is developed with C# language using Visual Studio 2008 and .NET framework 3.5.

5.3. User Study

After development of the prototype, we conducted a user study to compare the performance of our prototype and Vista's firewall.

We recruited 8 participants for our study. Four participants are IT graduate students from SFU's school of interactive arts. Two participants are computer science graduate students of SFU. One Participant is computer science undergraduate student of SFU, and one participant is engineering graduate student of SFU. All the participants are aged between 23 and 27. We collected information about participants experience with windows Vista, Vista's firewall, and firewall's in general in a pre-user study questionnaire. The demographic information collected from the questionnaire is shown in Figure 8, Figure 9, and Figure 10.

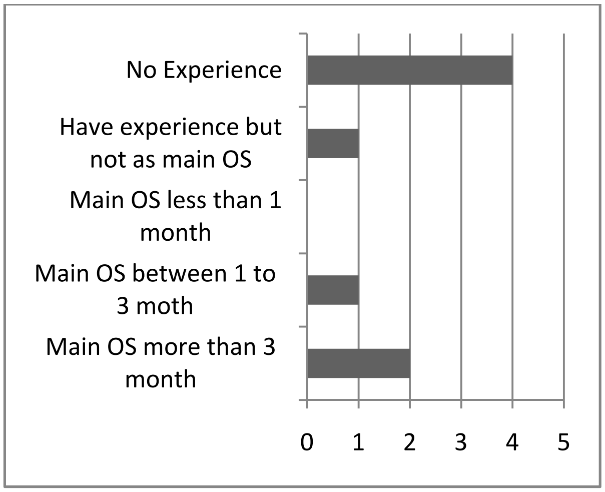


Figure 8 – Participant's experience with Vista

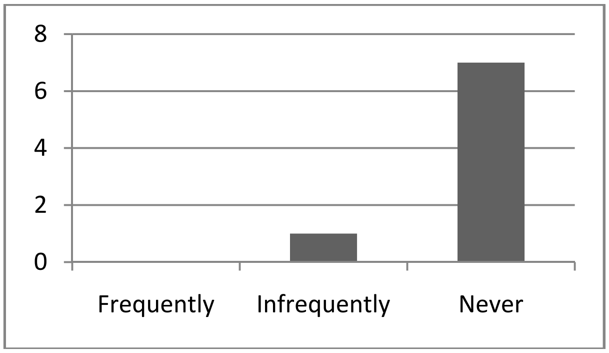


Figure 9 – Frequency of Vista's firewall usage by participants

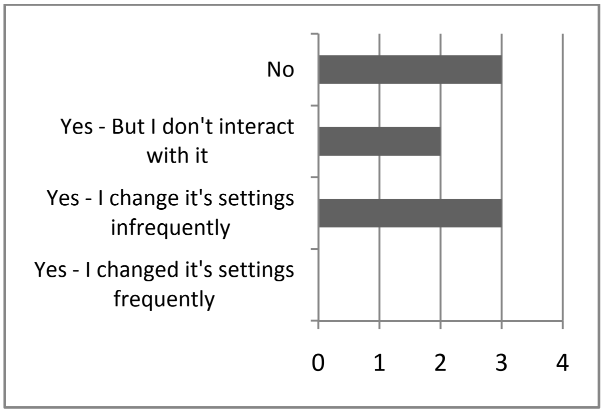


Figure 10 – Experience of users with firewalls in general

After collecting the demographic information about participants using the questionnaire, we presented the users with the basic information about Vista's firewall. We used a 6~7 minute PowerPoint presentation in which we talked about the goal of the firewall, the default behavior of firewall with respect to inbound and outbound connections, and the concept of profiles.

After the presentation, we give users list of tasks that they should perform on Vista's firewall. The list of the tasks is as follows:

- Turn firewall On/Off.
- Allow the program "eMule" to establish outbound and inbound connections.
- You unblocked program "eMule" while you were in home as well as university, when firewall shows a message about unblocking program. Now you know that it is a harmful program. Block "eMule" again to disallow inbound connections by this program.
- You become aware that the program "eMule" establishes connection to an unknown host to send your private information. As you like to continue using it, block the outgoing connections created by "eMule".

The first two tasks are given to the users for two reasons. The first reason is to let users become familiar with the interface by performing simple tasks. The second reason is to analyze the performance of two groups on tasks that do not require using new features of the improved interface. If the performance of two groups does not differ significantly, it shows that the two groups are statistically similar.

The last two tasks are the tasks for which we improve the usability of the interface using ESS method.

As performing tasks 3, and 4 with Vista's interface, requiring users to deal with advanced interface of the firewall, and as we see that users can't perform these tasks successfully using Vista's interface, we let them to perform these tasks again by giving them knowledge about existence of advanced interface. We will show the redoing of tasks 4 and 3 by tasks 5 and 6 respectively.

6. Results

We will analyze the result of user study from two different angels. First we will show average time to completion for each task by each group. Second we show the number of goal errors each group committed for each task.

The average time to completion for each task is presented in Table 1 and Table 2.

Table 1 – Average time to completion

	Vista Group	ESS Group
Task 1	50.5	40
Task 2	141.5	137.75
Task 3	62.25	54.75
Task 4	89	77
Task 5	289.25	X
Task 6	254	X

Table 2 – Number of goal errors

	Vista Group	ESS Group
Task 1	0	0
Task 2	0	1
Task 3	4	0
Task 4	4	0
Task 5	1	X
Task 6	1	X

As shown in Table 1, in average ESS group performed better than the Vista group. Also, for tasks 4 and 5, all the Vista users committed goal errors and couldn't perform the task successfully. After we let them know about that they performed the task unsuccessfully and show them advanced interface of the firewall, 3 of the users performed the tasks successfully. One user couldn't determine how she can perform the task. Also in task two, one of the ESS users committed a goal error by adding a rule for outbound connection as well as a rule for allowing inbound connections. This goal error doesn't prevent user from allowing inbound connections but he also blocked outbound connections. As a result this goal error does not result in user doing the task unsuccessfully.

To compare the performance of the two interfaces to show if the ESS interface improved the usability significantly we performed T-test to compare the result. Using SPSS, Independent Samples t-Tests (utilizing a p value of <0.05) were carried out to study the significance of any difference between the mean completion time for each task in our prototype and Vista's interface. First, we compared the times for task 1. As can be seen from Table 3, the *t* test failed to reveal a statistically reliable difference between the mean completion times of the ESS (M = 40 ms) and the Vista's interface (M = 50.5 ms), *t*(6) =1.282, *p* = .247, α = .05. For the second task, by the aim of the T-Test it was proven that no considerable difference between the mean times can be demonstrated (*t*(6) =.383, *p* = .715, α = .05). However, in the case of the third task, as the results of the applied t-Test indicate, we cannot reject our null hypotheses stating that there is no significant difference between the mean times

(t(6) =5.166, p = .011, α = .05). Similarly, based on the performed t-Test, the null hypothesis underlying the effectiveness of our proposed design for the fourth task cannot be rejected (t(6) =5.348, p = .012, α = .05).

The result of the t-Test shows that, two groups' performance on the similar interfaces (Task 1, 2) does not differ significantly, but their performance for the tasks that supported in ESS interface (Tasks 3, 4) differs significantly.

7. Limitations and Future work

The main limitation of our work is the number of our participants. Eight participants are not enough number to perform the comparison. As a future work we suggest performing the user study on at least 8 more participants. In addition, our participants are all computer science, engineering, or IT students. Our result will be more generalizable if we can perform user study on more divers samples.

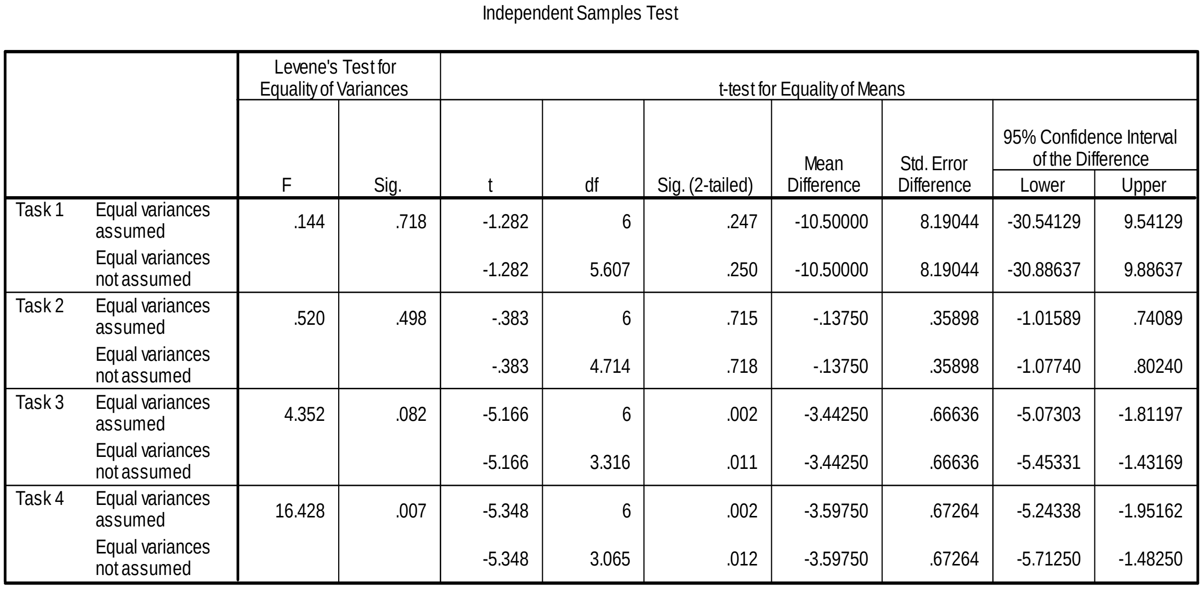
Another limitation of our work is that we compared the result of Task 3 and 4 in the ESS interface with the result of Task 5 and 6 in the Vista's interface. Vista users in Task 5 and 6 deal with the firewall's advanced interface for the first time while ESS users performed the task on the same interface on which they performed task 1 and 2. Therefore they are familiar with the interface on which they should perform their task.

Finally, our prototype improved few aspects of the Vista's interface. By performing thorough analysis of the tasks that results in dangerous errors, Vista's interface can be improved more extensively.

8. Conclusion

In this paper we improved Vista's firewall's user interface to prevent users commit dangerous errors. We developed a high fidelity prototype that of the improvements and compared the prototype with Vista's firewall interface by performing a user study. The result of our user study shows that, our design is effective and can improve the time to completion of the tasks significantly. Also, our result shows that users commit fewer goal errors using our interface in comparison to Vista's interface.

Table 3 Result of the t-Test



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Task 1	Equal variances assumed	.144	.718	-1.282	6	.247	-10.50000	8.19044	-30.54129	9.54129
	Equal variances not assumed			-1.282	5.607	.250	-10.50000	8.19044	-30.88637	9.88637
Task 2	Equal variances assumed	.520	.498	-.383	6	.715	-.13750	.35898	-1.01589	.74089
	Equal variances not assumed			-.383	4.714	.718	-.13750	.35898	-1.07740	.80240
Task 3	Equal variances assumed	4.352	.082	-5.166	6	.002	-3.44250	.66636	-5.07303	-1.81197
	Equal variances not assumed			-5.166	3.316	.011	-3.44250	.66636	-5.45331	-1.43169
Task 4	Equal variances assumed	16.428	.007	-5.348	6	.002	-3.59750	.67264	-5.24338	-1.95162
	Equal variances not assumed			-5.348	3.065	.012	-3.59750	.67264	-5.71250	-1.48250

9. References

[1] S. Yu, P. Jaferian, G. Agashe, and F. Shamji, "Usability study of Vista's firewall using respondent METH methods", *EECE 412 Term Paper*, The University of British Columbia, Vancouver, BC, December 2007.

[2] P. Arjmandi, R. Boeck, F. Raja, and G. Viswanathan, "Usability of Windows Vista Firewall: A Laboratory User Study", *EECE 412 Term Paper*, The University of British Columbia, Vancouver, BC, December 2007.

[3] A. Chebium, P. Jaferian, N. Kaviani, F. Raja, "A Usability Analysis of Microsoft Windows Vista's Firewall", *CPSC 544 Term Report*, The University of British Columbia, Vancouver, BC, December 2007.

[4] A. Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *in Proceedings of the 8th USENIX Security Symposium*, August 1999.

[5] S. Chiasson, P. C. Oorschot, and R. Biddle, "A usability study and critique of two password managers." *In Proceedings of the 15th Conference on USENIX Security Symposium*, August 2006.

[6] A. Herzog, and N. Shahmehri, "User help techniques for usable security." *In Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology*, March 2007.

[7] J. McGrath, "Methodology matters: Doing research in the behavioral and social sciences." *In Human-Computer interaction: Toward the Year 2000*, 152-169, 1995.

[8] J. M. Carroll, and C. Carrithers, "Blocking learner error states in a training wheels system," *Human Factors, Vol 26, Issue 4,* 1984, pp. 377-389.

[9] R. A. Maxion, and R. W. Reeder, "Improving user-interface dependability through mitigation of human error." *Int. J. Hum.-Comput. Stud*. 63, 1-2 (Jul. 2005), 25-50.

[10] B. Kirwan, *A Guide to Practical Human Reliability Assessment,* Taylor and Francis, London, UK, 2004.

[11] S. Pocock, M. Harrison, P. Wright, P. Johnson, "Thea: a technique for human error assessment early in design." *In Proceedings of Eighth IFIP TC.13 Conference on Human-computer Interaction (INTERACT'01)*, Tokyo, Japan, 2001, pp. 247-254.