Usability study of Vista's firewall using respondent methods

Steven Yu, Pooya Jaferian, Gaurav Agashe, Faraaz Shamji

***Abstract*— a firewall is one of the most important security tools against network attacks. Microsoft, in its new version of the Windows, Vista, offered a new firewall with plethora of advance features that if used correctly, can protect a personal computer from most of security threats. The unfortunate truth is that many end-users of Microsoft Vista have little or no security knowledge and are easily confused by the advanced features contained within the firewall. Subsequently, it is easy to see why users are a primary contribution to the majority of computer security errors. The purpose of this work is to analyze the usability of the Vista firewall and to relate ease of use, intuitive controls and interface to effective firewall protection. This was achieved by gathering a large amount of survey sample data along with conducting interactive demonstrations where users tried to perform common firewall operations. These users were then individually interviewed to gather user data on the effectiveness of the Vista firewall's GUI and organization. Data gathered from our surveys and interviews, suggests that the majority of the users did not see a clear purpose for a firewall and hence were not aware of the different settings that need to be tuned for complete protection. Overall, users preferred not to muddle with firewall settings and would rather have the operating system make intelligent security decisions on their behalf.**

***Index Terms*—Usability Analysis, Firewall, HCISec.**

I. Introduction

SECURITY mechanisms and tools are only effective when used correctly and in a reasonable time. When a security mechanism or tool is used in a wrong way, it gives user a false sense of safety; therefore it will be more dangerous than absence of such mechanism or tool. The goal of the security usability research area is to use security effectively. Security software is usable if the people who are expected to use it first are reliably made aware of the security tasks they need to perform. Second, are able to figure out how to successfully perform those tasks; Third, don't make dangerous errors; and finally are sufficiently comfortable with the interface to continue using it[1].

Microsoft Windows Vista, as a new and groundbreaking Microsoft's operating system, ships with an improved user interface, and lots of other features for security, data management, etc. One of new improvements in Vista, in comparison to Microsoft Windows XP (SP2), is a new personal firewall. As Microsoft focuses a lot on the security boost of the Vista in comparison to XP, users will trust Vista's firewall as a part of Vista's security solution. Therefore, in order to be successful, the firewall should be usable. In our work, we studied usability of Microsoft Windows Vista's firewall. The problem of usability study of Vista's firewall is important from different points of view. First, Vista is a new operating system, so there is no prior usability study on its built-in firewall. Also, as a new operating system, there are still some chances to improve its flaws by Microsoft in its future updates. Second, users gradually switch their windows XP to Vista. Therefore in the future Vista will become most popular operating system in the world, and consequently its internal firewall. Third, as many users upgrade their operating system to Vista for its security features, users should not disappoint with its firewall, as second mostly used security software (according to our survey).

The rest of this report is organized as follows. In section 2, we overviewed related works. In section 3, we will give a brief overview on Vista's firewall and its features. In section 4, we show our methodology for evaluation of the Vista's firewall usability and consequently show the results we got from our survey and interviews. In section 5, we discuss about our results, and how Vista's firewall can be improved with respect to the results from our study. The paper is concluded with section 6, in which we discuss limitation of our work, and future directions.

II. Related Works

We can classify related works into two categories. First category is general usability guidelines for security that can help building usable secure system. We can evaluate a secure systems usability from viewpoint of these guidelines by checking which guidelines are used in the system and how effective they are. Second category is works in the area of usability analysis of firewalls.

A. General Usability Guidelines

In [2], Nielsen proposed 10 usability heuristics. These heuristics can be employed to perform a "Heuristic Usability Analysis" on software systems. In our work, before designing our interviews, we performed an informal heuristic evaluation of Vista's firewall, and identified its major problem. Then we designed our questionnaire and interview to study the founded problems more in detail. In this paper, we will focus on respondent techniques we used; therefore we will not give further details about our heuristic evaluation.

In [3] authors reviewed available user help techniques for achieving usable security, and identify strengths and weaknesses of each. During our interviews, we asked some questions to check which user help techniques, Vista's firewall users prefer.

B. *Usability study of firewalls*

In [4] the authors compare 13 firewalls for respecting to their alert when a program wants to make an outbound connection and also when it wants to accept incoming connections. The weakness of the [4] is that the evaluation is not based on a user study. Therefore, the recommendations for usable alerts for personal firewalls are not validated.

In [5] authors defined the term "HCI-Sec" and proposed 6 guidelines, based on Nilsen's 10 usability guidelines, for a successful user interface for a secure system. Consequently they proposed some improvements for Windows XP's firewall and compared the new improved prototype with current firewall based on HCI-Sec criteria. Again, in this work, authors didn't perform a user study to find the weaknesses of XP's firewall from real user's point of view, and also analyze the usability of the new prototype. In our interview's, we asked questions about Vista's firewall, to see how users like the application of 6 HCI-Sec criteria on Vista's firewall.

In [6], wool studied the usability of direction based filtering rules in several major firewalls. The difference of this analysis with our work is that first, Wool studied enterprise firewalls that their main users are security practitioners not normal users. Second, he does not perform a user study to analyze the usability of current firewalls and also to validate his new prototype from actual users' point of view. Furthermore, the domain of the Wool's work is limited to usability of rules not other facets of firewalls.

III. Microsoft Windows Vista's Firewall

Based on [7], Vista's firewall is classified as application proxy firewalls. Also it is considered a personal firewall at it targets the home users. So it differs from enterprise firewalls which can be installed on a network computers and accept central policies.

The Vista's firewall functionality is simple. In its default setting, firewall allows all outgoing connections and blocks all incoming connections. When a new program is installed, and requests accepting incoming connections, firewall asks user to build an exception (a rule) for the program that allows it to accept incoming connections.

The new Vista's firewall has two different user interfaces. The first interface, which called "Windows firewall", is placed in Control Panel and for conciseness we will all it "Basic Interface". It gives user the ability to Turn the firewall On/Off, block all the incoming connections, define exception for some programs in accepting incoming connections, define exception for some ports to accept incoming connections, and enable/disable firewall on a particular network interface. The second interface, which is called "Windows firewall with Advanced Security", is placed in the "Control Panel/Administrative Tools" and for conciseness we will call it Advanced Interface. It gives user ability to define some rules for unblock Incoming connections, and block outbound connections. Also in contrast with the previous interface, it gives full-control over each rule (e.g. setting protocol, local port, remote port, network address, etc.). Also another feature in the advance firewall is that the user can set different rules for different network profiles (e.g. have different rules in home network and public networks). Generally, the advanced interface covers all the functionality delivered in the basic interface.

IV. Evaluation Methodology

There are different approaches available to do research in the social and behavioral sciences. McGrath classified these approaches into 8 different categories [McGrath]. Each category has some advantages and disadvantages based on degree of generalizability, precision, and realism it can achieve. We chose two different approaches to study Vista's firewall. First, sample survey, in which we will conduct a survey based on a questionnaire to obtain a general understanding about usability of Vista's firewall. Second, judgment study, in which we study users' opinion about Vista's firewall after they performed some tasks with it. For the second part we conducted semi-structured interviews to ask about user's experiences with the firewall. The advantage of the first approach we used is obtaining generalizable results about the firewall, and the advantage of second approach is obtaining more precise and specific results.

A. *Collecting data using Sample Survey*

To survey users about Vista's firewall, we built a short questionnaire with general questions about a good firewall. The questions of our survey are shown in Table I.

TABLE I
The questions used in the study

#	Question
1	Personal Information
2	Current Operating System
3	Security software they have
4	Degree of experience with firewall in general.
5	General knowledge of the user about the concept of firewall.
6	Awareness of user about availability of buil-in firewall
7	Previous experience of user with Windows Vista
8	Previous experience of user with Vista's firewall
9	Ask about how they can access Vista's firewall
10	Ask about how they can access Vista's advanced firewall
11	Ask about user's preference for a firewall's interface
12	Ask about user's preference when they need help
13	Ask about user's preference when firewall shows a message
14	Ask about scenarios that user needs at least once in a month
15	Ask if they like to participate in our survey

We made our survey available on the web, so we can collect as many as possible answers. The participants of our survey were 23 Undergraduate students from different majors, three computer sciences and computer engineering master students, two electrical and computer engineering PhD students, and two PhDs in computer science. The result of our survey is shown in figures 1-7.

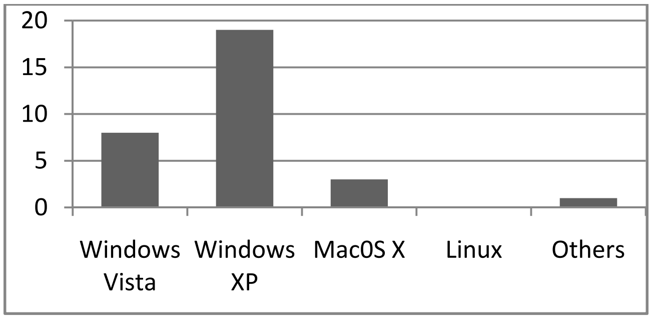

Figure 1 – The usage of each operating system

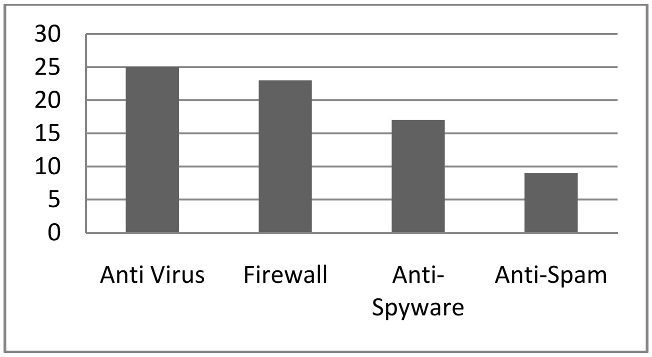

Figure 2 – Type of security software used by the users

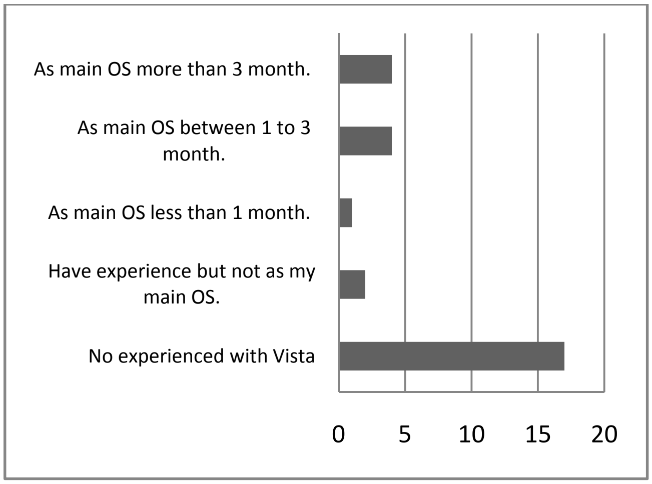

Figure 3 – The experience of users with Windows Vista

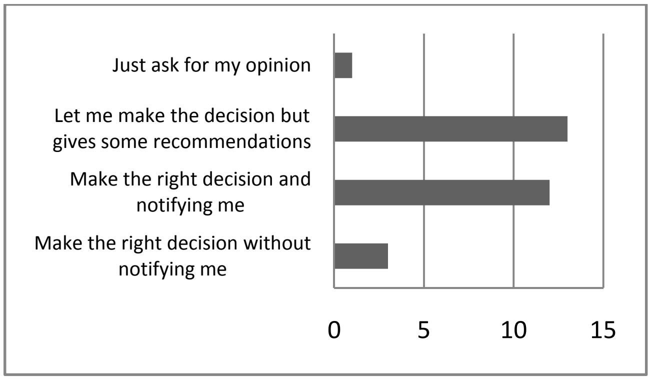

Figure 4 - The general preference of users about a firewall's interface

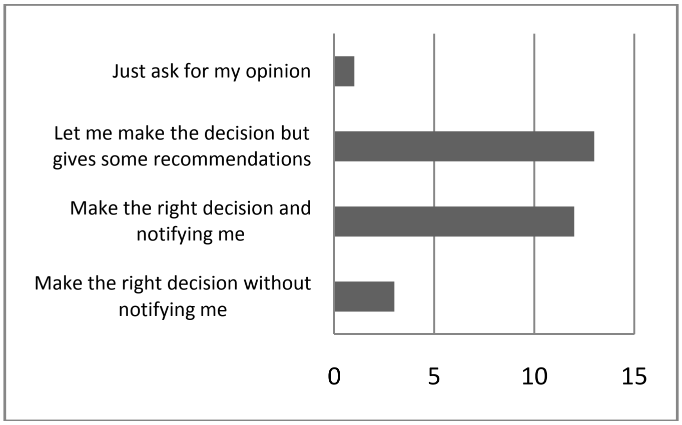

Figure 5 Users preference for firewall notifications

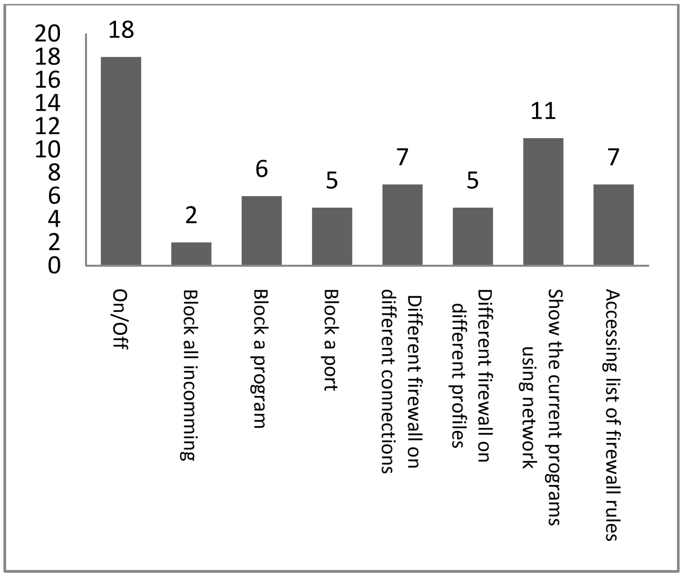

Figure 6 – The functions that users predict they will use at least once in a month

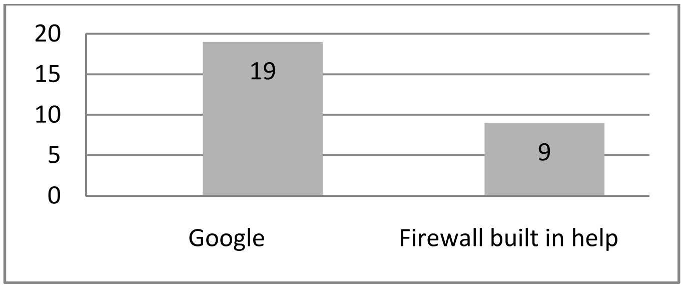

Figure 7 – The preference of users to get help

B. Collecting Information using Interviews

The result of our survey showed that only less than 30 percent of the people installed Vista on their computer. Therefore, we decided to interview our participants after they go through 6 predefined tasks so they have a good mental model about Vista's firewall.

We design 7 general tasks for users (Find firewall, Turn firewall On/Off, Block all incoming connections, Unblock a program/Port, disable firewall on LAN connection, and find firewall with advanced security and Add a new rule for blocking Yahoo Messenger to the firewall for public network profile). The tasks are performed on a Windows Vista Premium Home Edition, using an account with administrative rights (from the viewpoint of principles of designing secure systems, it should be supposed that the users normally work with an account with limited privileges, but it is not followed by users in real-life). The time for performing tasks is 15~25 minutes. We will help users in doing the task, if it takes more than 3 minutes for them to find out how they can do that. After the user finished all the tasks, we started the interviews.

We designed a semi-structured interview, with 18 questions, and we ask additional questions, if the user mentions an important point that needs more clarification. The participants of our study was 2nd to 4th year undergraduate students from different majors (electrical and computer engineering, mechanical engineering, mining, law, etc.). In the following we present the result of the interviews.

1) General information about participants

Four participants have windows Vista on their computer, five have XP, two have OS X Leopard and one has OS X Tiger. Three participants, who have not Vista on their computer, also don't have any previous experience with Vista. From 12 participants, 8 stated that they have not installed a third party personal firewall on their computer. The Mac users believe that there is no need to install firewall because Mac is secure (They don't mention that Mac has a built-in firewall, but one of them mentions if he want to install a firewall, he will install Unix-based standard firewall). The rest prefer relying on Built-in firewall of their OS. From the users who installed a third party personal firewall, one has Zone-Alarm pro, two have Norton Internet Security, and one has a Korean firewall. Also one of the users was installed Norton, but because it slows down the computer, the program was removed.

2) General impression of Vista's firewall

After doing tasks with Vista's firewall, none of the participants like to switch to Vista, for its new built-in firewall. Mac users believe that Vista is inferior to OS X in sense of security as one of them stated: "*I don't even have to know what a firewall is. Leopard takes care of all my security needs.*" Also, none of the current Vista's users like the Vista more after the experiment as one of them stated: "*I didn't like it before, I don't like it now*".

About what they like about the firewall, four participants stated that they like Vista's firewall because it is free and integrated with OS. Five stated that it is easy to use, simple and has separated advanced settings: "Keeping the advanced security separate is a good plan as I am less likely to screw up the settings". Two users stated that having advanced firewall give user more options for security. And one user has no reason to like Vista's firewall.

About what they don't like about the firewall, seven participants stated that having no access to advanced interface is no appropriate. One participant doesn't like the fact that Microsoft assumes the average users are novice and the advance interface should be hide from them. One participant stated that: "it has too many options with no feed-back".

3) Firewall accessibility and Visibility

About the placement of the firewall in the control panel, all the participants like it to be in the current place. About the availability of firewall in the tray, two users believe that it is waste of resources. Also, one user believe that: "if there is a direct link from tray or desktop to the firewall, someone may access it and screw things up in my firewall".

4) Use of available features

When users asked for a scenario for using "block all incoming connections" option in firewall, four of them mention that is could be useful in case of an attack from Trojan or Virus. Also two users mentioned that it could be useful when they are not using the internet. One user mentions that it could be useful when doing online banking. The rest of the users don't find this feature useful. Two users prefer to unplug their network cable, as one of them stated: "I could just unplug the cable".

For blocking and unblocking programs, four participants faced real-life scenarios during their work with computer. Three users blocked the outbound connection of different non-malicious programs (programs that want to connect to internet for registration, etc), also one of them was unblocked eMule to accept incoming connections. Rest of the participants mentioned that blocking programs could be useful to avoid Trojans and Viruses.

For blocking and unblocking ports, eight participants have no knowledge about ports, one user opened a port for his P2P application and one other participant mentioned that he blocked ports randomly when using "bitcomet" to prevent the upload speed from getting too high.

For enabling and disabling firewall on a specific connection, 8 participants believe that there they need same level of security on their different connections. 4 participants stated that they wireless is less secure so the firewall should be always available on the wireless connection.

For different rules on different network profiles, 7 participants stated that they prefer more security on public networks such as Starbucks and campus. 5 participants mention that they need same level of security in all networks.

5) User help techniques

When participants are asked about which kind of help they prefer to use, 9 participants stated that they prefer searching google instead of Vista's built-in help. One participant stated that: "*On Google, you are able to sift through hundreds of problems and their solutions and find help pertaining most to your issue.*" Another participant also mentioned online forums: "*I will google it, user forums are a gold mine of troubleshooting tips and tricks.*" And about windows help they mentioned that: "*It is very selective in the help topics and does not cover all the possibilities.*" Two other people mention that they will use windows help and one mention that: "*I first turn to windows help but usually end up asking a friend or google.*" Another user also mentioned that, it could be useful if there is a brief help about each item on the firewall. Also another user mentioned that small-links to help under each item could be useful.

We asked users if they like something like office-assistant that can give them directions. None of the user like such a feature as stated by one of the users: “Hate it! Waste of resources and annoying.” We also asked users if they like availability of a tutorial about Vista’s firewall (An animation or film, like one available for software in Mac). Again none of participants said that they will go through such a tutorial.

Finally, we asked users to choose between single interface, two different interfaces, a customizable interface, and an adaptive interface. Four participants preferred just one interface. One of them stated that: “My Mac just works and I’ve never had to mess around with its settings. A simple ON/OFF button is good enough for me.” Eight participants preferred having two interfaces while one of them mentioned: “*I also like the customizable interface.*” None of the participants liked the adaptive interface.

V. Discussion

The result of our survey shows that, Firewall is the second most traditional security product on users’ computers. Also, it shows that users are not willing to change the configuration of their firewall frequently. Also the result of our survey and study demonstrated that users prefer a firewall with one simple and one advanced interface more than other designs. It shows that the general design of the Vista firewall is very appropriate. But, we found some flaws in the interface that could be improved in order to improve the general usability of Vista’s firewall:

1- The biggest problem which mentioned by most of the users is that the advanced firewall is inaccessible from the simple interface.

2- Placing “block all incoming connections” option in the main window of basic interface seems not appropriate. As the result of our survey shows, it could be the least used feature in a firewall. Also during interviews, users can not give a real-life scenario for using this option.

3- Enable/Disabling firewall on a specific connection is not much useful to be placed in the basic user interface.

4- Ability to block out-going connections can be very useful for users, even more than blocking incoming connections; therefore it could be useful to provide that feature in the basic interface.

5- Vista’s built in help is weak. Searching the help would not give users appropriate results. Also the context sensitive help does not direct users to right place. As a result, users prefer searching google. It could be useful to provide online help feature (like office 2007) to be able to provide more appropriate search results for the user.

6- The placement of firewall in the control panel is good. But it could be useful if there is an indication of firewall, and its current state in the tray.

7- The users like to have an overview about the programs that currently using the network connection. It could be useful that the firewall provide such a feature in its simple interface. It is also in harmony with Nielsen’s “Visibility of system status” heuristic.

VI. Conclusion

In this paper we studied usability of Windows Vista’s built-in personal firewall using two different methods, Questionnaire and Interviews. We found some weaknesses and strengths for the Vista’s firewall and recommend some improvements for the firewall.

But, our work has some limitations. First, in our recommendations we tried to eliminate the weaknesses of Vista’s firewall we found in our study. But our recommendations should be tested and validated using another user study. Second, the participants of our interviews are novice users. We could strengthen our findings by extending our interview sample to some more experienced users from security point of view.

For feature works, it could be useful to build a prototype with our recommended improvements, and conduct a user study based on the new prototype.

References

[1] A. Whitten, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.", presented at the 8th USENIX Security Symposium, Washington, D.C., Aug. 23-36, 1999, Pp 169-184.

[2] J. Nielson. (2005, Feb 2). *Ten Usability Heuristics*. [Online]. Accessed: 2007, Nov 18. Available: <http://www.useit.com/papers/heuristic/heuristic_list.html>.

[3] A. Herzog, N. Shahmehri, "User Help Techniques for Usable Security.", presented at the Conference on Human Factors in Computing Systems, Cambridge, Massachusetts, 2007, Article No. 11.

[4] N. Shahmehri, "Usability and Security of Personal Firewalls.", presented at the 22nd International Information Security Conference (IFIP TC-11), Sandton, South Africa, May 14-16, 2007.

[5] J. Johnston, “Security and Human Computer Interfaces.” *Computers and Security*. Volume 22, 675 – 684, 2003.

[6] A. Wool, “The Use and Usability of Direction-Based Filtering in Firewalls.” *Computers & Security*. Volume 23, 459 – 468, 2004.

[7] M. Stamp, Information Security: Principles and Practice. Wiley-Interscience, 2005.