Winter 2007

Department of Electrical and Computer Engineering ,
The University of British Columbia,
Vancouver, BC, Canada

Arun Chebium, Pooya Jaferian, Nima Kaviani, Fahimeh Raja
{arunc, pooyaj, nimak, fahimehr}@ece.ubc.ca

[A Usability Analysis of Microsoft Windows Vista's Firewall]

[The usability of personal firewalls has not received a significant amount of attention in the literature. However, it is essential that these firewalls - which are used by the lay end-user to protect his/her computer from malicious programs on the internet - be usable as well as secure, and that one concept lead to the other seamlessly. Here, we report on the results of a usability analysis of Windows Vista's firewall. Our heuristic evaluation of the firewall (based on standard usability guidelines and carefully extracted benchmarks) has thrown up many areas of improvement. In this term project, we propose a medium-fidelity prototype to address some of these issues, perform lab experiments and user studies involving this prototype, and based on the results of our rigorous field work, and suggest final modifications leading to a high-fidelity prototype.]

A Usability Analysis of Microsoft Windows Vista's Firewall

TERM PROJECT – PHASE III

Arun Chebium, Pooya Jaferian, Nima Kaviani, Fahimeh Raja

{arunc, pooyaj, nimak, fahimehr}@ece.ubc.ca

Department of Electrical and Computer Engineering

The University of British Columbia, Vancouver, BC, Canada

CPSC 544, Human Computer Interaction

Fall 2007

CONTENTS

FIGURES

Abstract. The usability of personal firewalls has not received a significant amount of attention in the literature. However, it is essential that these firewalls - which are used by the lay end-user to protect his/her computer from malicious programs on the internet - be usable as well as secure, and that one concept lead to the other seamlessly. Here, we report on the results of a usability analysis of Windows Vista's firewall. Our heuristic evaluation of the firewall (based on standard usability guidelines and carefully extracted benchmarks) has thrown up many areas of improvement. In this term project, we propose a medium-fidelity prototype to address some of these issues, perform lab experiments and user studies involving this prototype, and based on the results of our rigorous field work, suggest final modifications leading to a high-fidelity prototype.

Keywords: **Security, Usability, Heuristic Evaluation, personal firewalls, Windows Vista**

1 INTRODUCTION

Firewalls are amongst the most complex pieces of software that are paid the least attention to, in terms of usability (by designers) and presence (by the end users). Similar to other security applications if the firewall's user interface is not "easy-to-understand" enough for the user to quickly make the correct decision, it could end up with a configuration that might be as dangerous as having no firewall at all. An in-depth analysis and a survey of existing literature of analyzing the usability of personal firewalls have brought to light a number of security and usability issues that make firewalls special and interesting to study.

Microsoft® Windows Vista™ includes a new and enhanced version of Windows' Firewall. It allows/blocks network traffic according to its configuration in order to provide a desired level of protection from malicious users and programs on a network. In contrast to traditional Windows Firewall, Vista's firewall includes enhancements for more advanced protection and configuration. However, Vista is in its initial stages of testing, and Microsoft claims that Vista is far ahead of the competition [4]. This claim will need a reality check. Thus, in this project, we will evaluate Vista's firewall in the light of the performance of popular personal firewalls and against a set of usability benchmarks that we have extracted and defined based on our ideas and the ideas outlined in the literature. Therefore, we would like to conduct a usability study of Vista's firewalls, evaluate it critically against our benchmarks, define some improvements, evaluate them via user studies and lab experiments, and then finalize a set of suggestions that could be incorporated into Vista's firewall in order to improve its usability.

2 FIREWALL DESCRIPTION, RELATED WORK AND USABILITY BENCHMARKS

In this section we first present an overview of Vista's firewall. Then, we present a note on usability studies on personal firewalls that can be found in the literature. Finally, we provide the usability benchmarks that we have extracted and defined based on our brainstorming and on the results of a survey of the literature on usability studies of personal firewalls.

2.1 HIGH-LEVEL DESCRIPTION OF VISTA'S FIREWALL

Windows Vista offers many improvements over its predecessor, Windows XP. A significant portion of these improvements concern the security features provided by the operating system. The firewall is one among these features. In this section, we will describe the firewall currently offered by Vista and highlight the major functionality that can be achieved using this firewall.

Vista's firewall offers the following basic functionality to the end user:

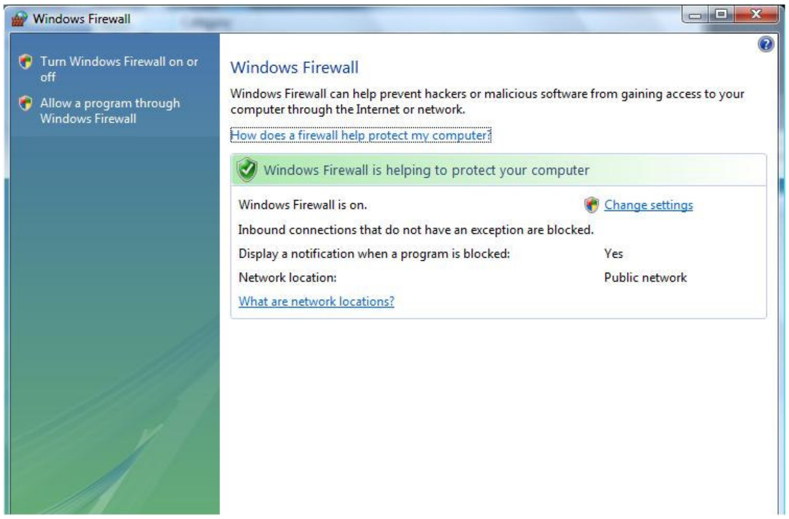
It allows the user to control inbound/outbound connections to/from the computer. By default, the firewall disallows all connections from the external world; for a program to be allowed through the firewall, an 'exception' for the program must be defined in the firewall.

When a program (not already specified as an 'exception') receives an incoming connection, the firewall shows a dialog box and asks the user if he/she is willing to 'unblock' the program and allow it to receive the connection.

In contrast, all outgoing connections are allowed by the firewall unless rules have been configured to explicitly disallow such connections.

In addition, the firewall offers two different interfaces to the user - a "basic" user interface (for 'day-to-day' functionality) and an "advanced" user interface (for customizable functionality). The basic user interface, called “Windows Firewall”, can be accessed through “Control Panel -> Windows Firewall”. (Throughout this report, this user interface will be termed “Basic Firewall”.) The interface is shown in Figure 1. The main window shows the firewall's current status and provides some links that can be used to change the firewall’s settings (Figure 2). The features of the firewall that can be tweaked using the basic user interface are:

1. Turning firewall On/Off
2. Blocking all incoming connections
3. Defining some exceptions in order to allow specific programs/incoming connections on specific ports through the firewall
4. Defining various 'profiles' (i.e., different types of networks to which the computer could belong) on which the firewall settings may be applied.


Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall
How does a firewall help protect my computer?
Change settings
What are network locations?

Windows Firewall

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

Windows Firewall is helping to protect your computer

Windows Firewall is on.

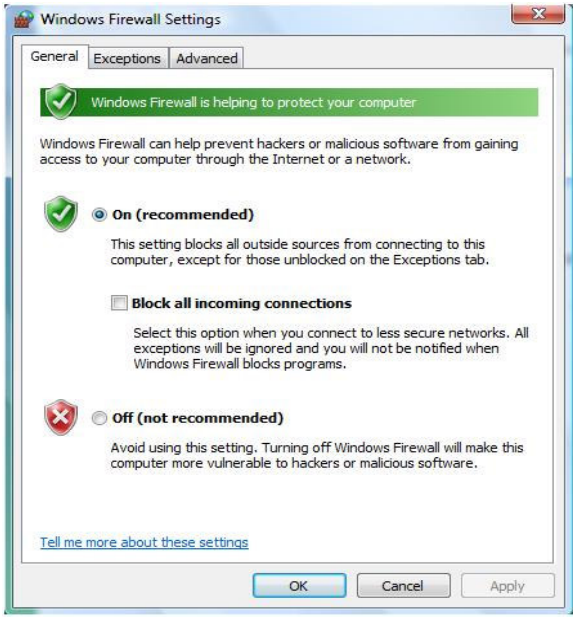
Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked: Yes

Network location: Public network

FIGURE 1: WINDOWS VISTA’S FIREWALL'S BASIC INTERFACE

The "advanced" user interface, termed “Windows Firewall with Advanced Security”, can be accessed through “Control Panel -> Administrative Tools -> Windows Firewall with Advanced Security”. (Throughout this report, we will use the term “Advanced Firewall” to refer to this interface.) The main window of this interface is shown in Figure 3. This interface is used to define fine-grained and fully customizable rules for incoming as well as outgoing connections. These rules can be customized with respect to their program, port, network connection, profiles, users, groups, and scope. The interface also allows the user to export/import firewall rules.



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.

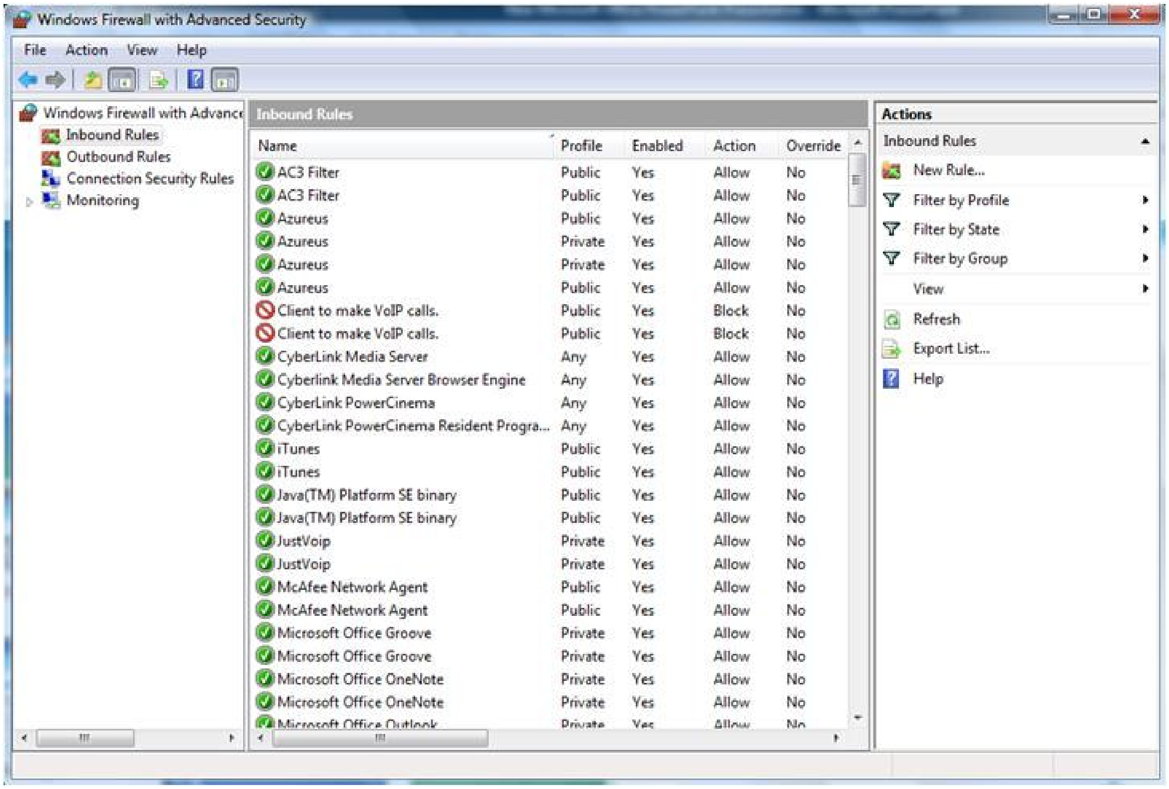
○ Off (not recommended)

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

FIGURE 2: BASIC FIREWALL'S SETTINGS

In both interfaces, there are links to a generalized help menu that is similar to that provided by other Microsoft Windows applications. Thus, in summary, user interaction with Vista's firewall is achieved by means of two interfaces, a set of dialogue-box prompts (when incoming connections arrive), and a standardized help menu.



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 3: WINDOWS FIREWALL'S ADVANCED INTERFACE

2.2 A NOTE ON USABILITY STUDIES OF PERSONAL FIREWALLS IN THE LITERATURE

The first significant work in comparative usability analysis of various personal firewalls can be found in [3]. In [3], the authors begin by defining some important terms: HCI-S as "Human Computer Interaction applied to Computer Security" and an HCI-S interface as “that part of a user interface which is responsible for establishing the common ground between a user and the security features of a system". Then, they specify six criteria that a good HCI-S system must adhere to (these guidelines are variations of the usability guidelines established by Nielsen [9]). Based on the proposed criteria, they perform a heuristic evaluation of Windows XP's Internet Connection Firewall (ICF) and propose some improvements in the form of a medium fidelity prototype (however, they do not evaluate their suggested prototype through lab experiments and/or user studies).

In [8] the author studies the usability of various firewalls that employ direction-based filtering. Wool's work, however, is not based on a well-defined methodology; he merely critiques different characteristics of firewalls in an ad-hoc manner. Also, the study targets enterprise firewalls, and thus the domain of Wool's study domain is rather different from that of the study contained in this report.

In [2], the authors present the results of a study of the usability of 13 different personal firewalls. The methodology used in this work is as follows: the authors define some use-cases (the normal scenarios that a user may face during interaction with a personal firewall) and some 'misuse' cases (i.e., scenarios that attempt to exercise a firewall in erroneous ways; the firewall must respond quickly and efficiently and negate any such activity), and study the behavior of each firewall when subjected to these scenarios. The authors perform heuristic evaluations of the firewalls and, based on the results of their work, provide some general recommendations for a good firewall. This approach differs from the study contained in this report in many respects: the scenarios used for the evaluations are limited, the heuristics are not the standard usability heuristics that are generally employed, and the final suggestions made by the authors are rather general and have not been rigorously evaluated by means of lab experiments or user studies.

Finally, in [10], the authors also present different techniques of presenting help-related content to the users in order to increase the usability of personal firewalls. Though these results do not have any direct bearing on our usability evaluations, the suggested help techniques can be used to further improve the prototypes proposed in this report.

2.3 USABILITY BENCHMARKS

As discussed before, we see that firewalls need to be simultaneously usable and secure. This is a complex requirement that requires good judgment during the design process in order to achieve. We believe that this may be achieved - and user-friendly personal firewalls may be designed and deployed - if designers and developers adhere to some benchmarks, standards and design principles. Here are some benchmarks that we have extracted and defined, based on the research material that we have surveyed:

1. Firewalls must be easy to configure and set-up and must convey their essential security features to users in a meaningful manner.
2. Firewalls must be designed such that similar functionality is located in similar positions on different applications sold by various competitors [1].
3. Firewalls must not display cryptic alert messages. They must teach users about network security by educating them via every alert (but must reveal only minimal security information required to complete the task). They must also provide the users ready access to a comprehensive help menu [2].
4. Firewalls must make themselves more visible. This can be done by [2]:
    a. Displaying the firewall name and logo in every alert.
    b. Indicating presence actively in system tray and having informative pop ups come up periodically.
5. Firewalls must enforce least-privilege and be able to create a finely-grained rule without too much burden on users [2].
6. Firewalls must be designed such that the most natural way to complete a firewall related task is also the most secure [7].

7. Firewalls must allow users to review created rules, understand how they will act and their resultant severity [2].

8. Firewalls must allow users to revise hasty decisions by periodically alerting the user about the current and desired states of configured rules [2].

9. Firewalls must allow users to easily revoke rules/actions that have already been configured [7].

10. Firewalls must not convey to the user the impression that it is possible to do things (with them) that are not possible in practice [1].

3 USABILITY ANALYSIS OF VISTA’S FIREWALL

3.1 HEURISTIC EVALUATION

For the purpose of our heuristic evaluation we looked into a set of tasks that a typical end user is supposed to be able to perform while using the firewall. To do so, two of our experimenters examined the interface and tried to come up with a series of possible actions for the end users. Meanwhile the other two members of our team played the role of observers in the system and logged the behavior of the experimenters. The logged actions were later examined against the usability criteria for usable systems by [9] (see Table 1) and also the principles for designing secure systems which can be counted as follows:

1. The users should be reliably made aware of the security tasks they must perform.

2. The users should be able to figure out how to successfully perform those tasks

3. The interface should be designed in such a way that doesn't lead the users to make dangerous errors

4. The users should be sufficiently comfortable with the interface to continue using it

5. The users should have sufficient feedback to accurately determine the current state of the system

TABLE 1: SUMMARY OF NIELSEN'S USABILITY CRITERIA

NO.	Criteria	Description
1	Visibility of system status	It is important for the user to be able to observe the internal state of the system through the HCI. This can be achieved by the system providing correct feedback within a reasonable time.

2	Match between the system and the world	An HCI which uses real-world metaphors is world easier to learn and understand. This will assist a user in figuring out how to successfully perform tasks.
3	User control and freedom	System functions are often chosen by mistake. The user will then need a clearly marked exit path.
4	Consistency and standards	Words, situations and actions need to be consistent and have the same meaning. A list of reserved words can assist in this area.
5	Error prevention	It is obviously best to prevent errors in the first place through careful design. However, errors do occur and they need to be handled in the best possible way.
6	Recognition rather than recall	The user should not have to remember information from one session to another. Rather, the user should be able to 'recognize' what is happening.
7	Flexibility and efficiency of use	The system should be efficient and flexible to use. Productivity should be increased as a user learns a system. The system should not control the user; rather, the user should dictate which events will occur. The system should be suitable for new and power users.
8	Aesthetic and minimalistic design	Information which is irrelevant should not be displayed. The user should not be bombarded with information and options.
9	Help users recognize, diagnose, and recover from errors	Error messages need to be clear and suggest a solution.
10	Help and documentation	Users tend to turn to help and documentation as a last resort. Help functionality needs to be context-sensitive and easy to search.

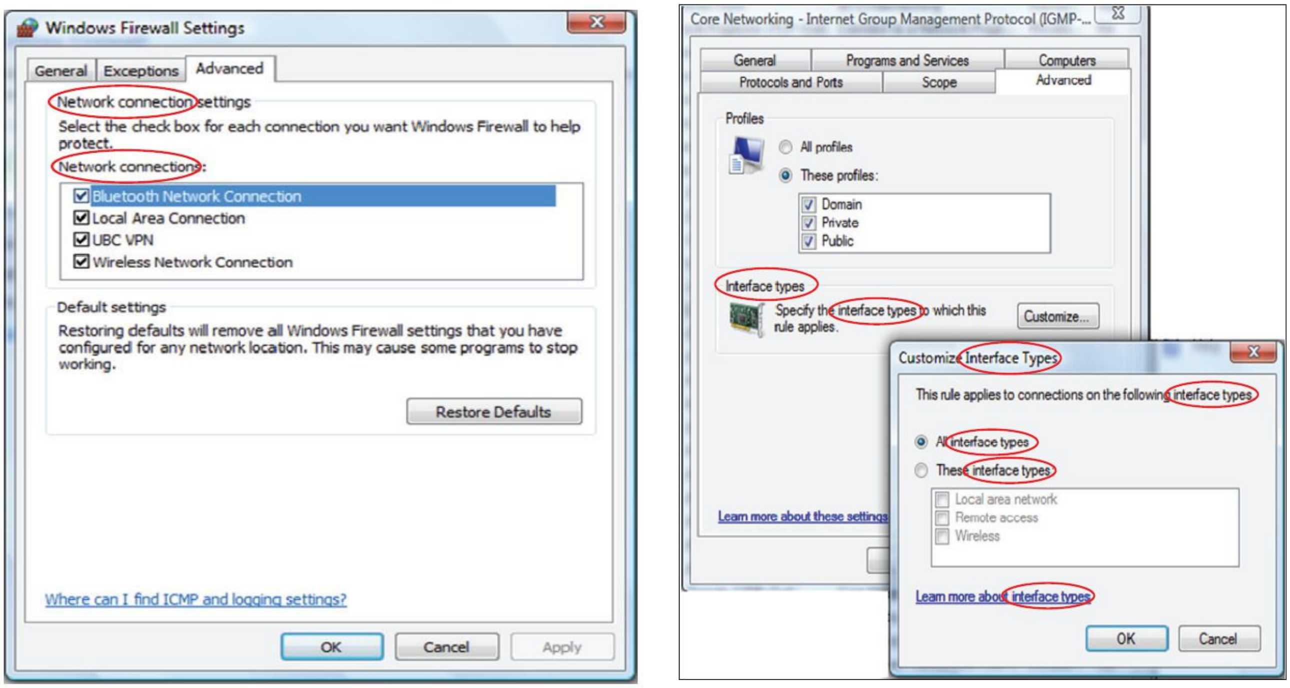
Having all the above criteria in mind, we started a heuristic evaluation of Vista's firewall to examine the interface and possibly identify the points of improvement. Below we bullet point some of our findings which clearly show the contradictions between the interface of Vista's firewall and the criteria in Table 1.

3.1.1 TERMINOLOGY INCONSISTENCY

The first problem that we identified was the terminology inconsistency while referring to the same concepts across different pages on Windows Vista's firewall. The inconsistent terminology obviously contradicts the fourth criteria in our model and would confuse the user with understanding the concepts or clearly using the designed system. Especially in using firewalls contradictory design may lead to wrong interpretation of the behavior for different systems by the user and thus may direct the user to take wrong or dangerous decisions which opposes the third principle in designing secure systems.

INTERCHANGEABLE USE OF THE TERMS NETWORK CONNECTION AND INTERFACE

We realized that in the Change Settings window of the simple firewall interface, and in its Advanced tab, the firewall can be set to manage each of the existing network connections such as local area and wireless connections. However, after switching to the advanced firewall interface, we noticed that this same concept is referred to as “Interface” which can be a source of confusion for the user (Figure 4).



Network connection settings

Select the check box for each connection you want Windows Firewall to help protect.

Network connections:

☑ Bluetooth Network Connection
☑ Local Area Connection
☑ UBC VPN
☑ Wireless Network Connection

Default settings

Restoring defaults will remove all Windows Firewall settings that you have configured for any network location. This may cause some programs to stop working.

Restore Defaults
Where can I find ICMP and logging settings?
OK
Cancel
Apply
Core Networking - Internet Group Management Protocol (IGMP-...
General
Programs and Services
Computers
Protocols and Ports
Scope
Advanced

Profiles

○ All profiles
● These profiles:
☑ Domain
☑ Private
☑ Public

Interface types

Specify the interface types to which this rule applies.

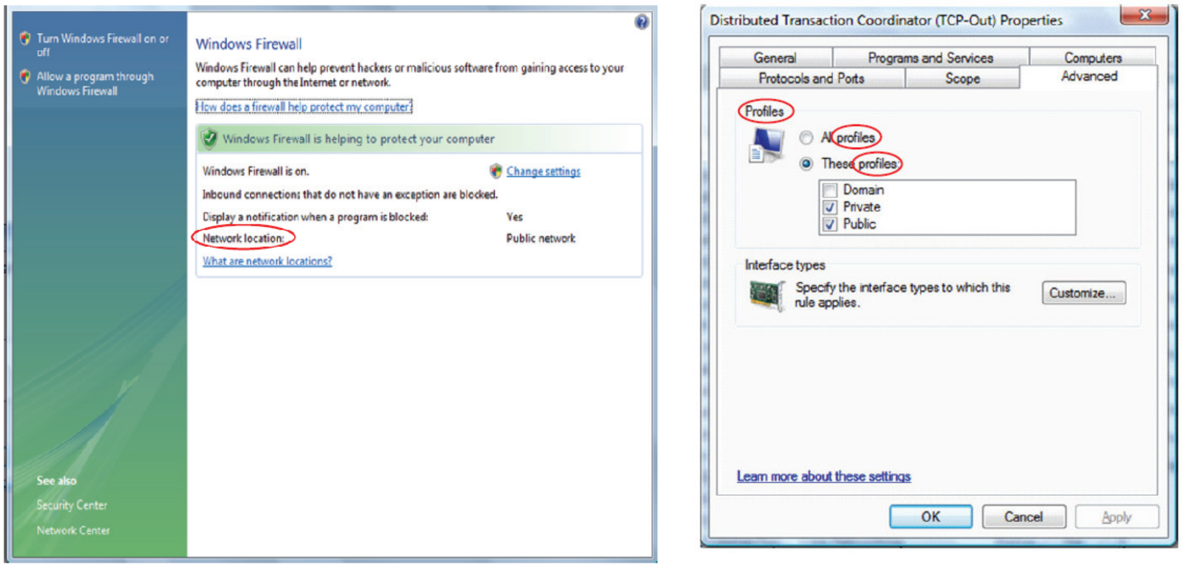
This rule applies to connections on the following interface types.

● All interface types
○ These interface types:
□ Local area network
□ Remote access
□ Wireless

FIGURE 4: ILLUSTRATION OF TERMINOLOGY INCONSISTENCIES IN WINDOWS VISTA'S FIREWALL

INTERCHANGEABLE USE OF PROFILE AND NETWORK LOCATION

In the simple firewall interface the domain of current activities for the user is referred to as Network Location. Looking into the settings of the advanced firewall interface, we realized that this notion is referred to as Profile, classified into Public, Private, and Domain, where domain entails more specific meaning with respect to the area of user's activities. This shows a conflict between the two terms addressing the same concept (Figure 5).



Windows Firewall

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

How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

Windows Firewall is on.	Change settings
Inbound connections that do not have an exception are blocked.	
Display a notification when a program is blocked:	Yes
Network location:	Public network

What are network locations?

Distributed Transaction Coordinator (TCP-Out) Properties

Profiles

○ All profiles

● These profiles

☐ Domain
☑ Private
☑ Public

Interface types

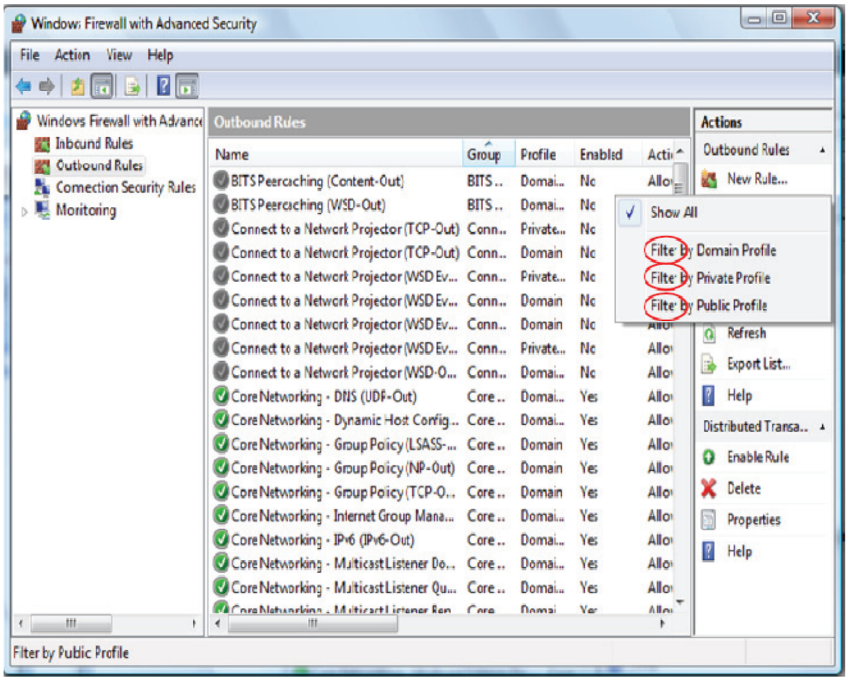
Specify the interface types to which this rule applies.

Learn more about these settings

FIGURE 5: INCONSISTENCY IN REFERRING TO NETWORK LOCATION AND PROFILE

IMPROPER USE OF THE TERM 'FILTER' TO CHANGE THE VIEW FORMAT

The term "Filter" is used on the advanced firewall interface to enable the user to decide about the set of rules (based on the properties that those rules share) to be shown on the screen. For example, the user can filter and display the rules that have been defined on the same profile. However, the term "Filter", once defined on the firewall interface, can diverge users' minds toward filtering out the set of available connections rather than just displaying different rules (Figure 6)



Window: Firewall with Advanced Security

Outbound Rules

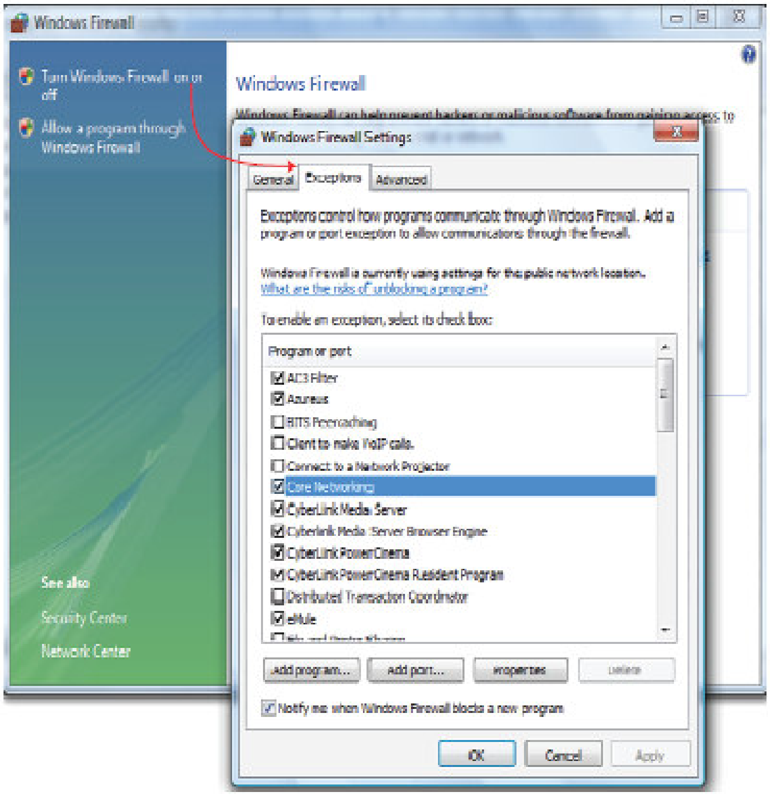
Name	Group	Profile	Enabled	Acti
BITS Peercaching (Content-Out)	BITS ..	Domai...	No	Allo
BITS Peercaching (WSD-Out)	BITS ..	Domai...	No	
Connect to a Network Projector (TCP-Out)	Conn...	Private...	No	
Connect to a Network Projector (TCP-Out)	Conn...	Domain	No	
Connect to a Network Projector (WSD Ev...	Conn...	Private...	No	
Connect to a Network Projector (WSD Ev...	Conn...	Domain	No	
Connect to a Network Projector (WSD Ev...	Conn...	Domain	No	Allo
Connect to a Network Projector (WSD Ev...	Conn...	Private...	No	Allo
Connect to a Network Projector (WSD-O...	Conn...	Domai...	No	Allo
Core Networking - DNS (UDP-Out)	Core...	Domai...	Yes	Allo
Core Networking - Dynamic Host Config...	Core...	Domai...	Yes	Allo
Core Networking - Group Policy (LSASS-...	Core...	Domain	Yes	Allo
Core Networking - Group Policy (NP-Out)	Core...	Domain	Yes	Allo
Core Networking - Group Policy (TCP-O...	Core...	Domain	Yes	Allo
Core Networking - Internet Group Mana...	Core...	Domai...	Yes	Allo
Core Networking - IPv6 (IPv6-Out)	Core...	Domai...	Yes	Allo
Core Networking - Multicast Listener Do...	Core...	Domai...	Yes	Allo
Core Networking - Multicast Listener Qu...	Core...	Domai...	Yes	Allo
Core Networking - Multicast Listener Rep	Core	Domai	Yes	Allo

Filter by Public Profile

FIGURE 6: IMPROPER USE OF THE TERM "FILTER"

3.1.2 THE EASE OF TURNING THE FIREWALL ON/OFF

One of the main tasks that users often need to perform is to easily alter the status of their firewall. That is, it should be possible for the user to recognize the current state of the firewall, whether it is on or off, and how to switch from one mode to another. This issue is inline with the first, the third, and the seventh criteria in using the firewall, i.e. visibility of system status, user control and freedom, and flexibility and efficiency of use. Having not been able to clearly change the status of their system based on the context they are exposed to, the users may feel uncomfortable with performing their desired tasks and may feel uncomfortable with using the interface, leading to a contradiction with the first and the fourth principles of designing secure systems. Through our analysis of how well Windows Vista's interface responds to the needs of the users with altering the status of the firewall from *ON* to *OFF* or vice versa we ran into an interesting problem which we refer to as *Wrong navigation from the sidebar.* Our analysis of the interface showed that in the simple firewall interface, user has two options to turn the firewall on or off. There is a button on the sidebar, named "Turn Windows Firewall on or off" and also there is a link on the main window to change the settings of the firewall. User can navigate to the change setting window of the simple firewall interface by clicking on either of these two options. However, the problem with using the sidebar button is that, if the settings window is already activated, clicking this button doesn't navigate the user to the panel that can be used to turn the firewall on or off (Figure 7).



Windows Firewall can help prevent hackers or malicious software from gaining access to

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

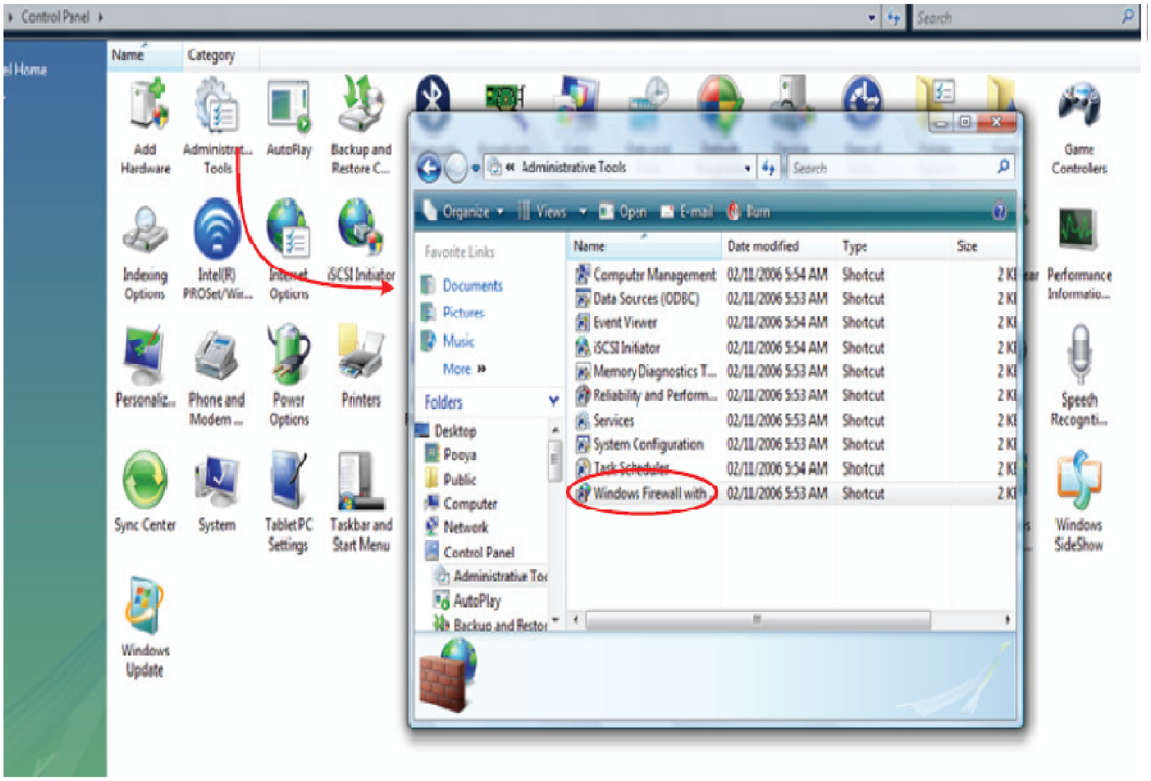
☑ AC3 Filter
☑ Azureus
☐ BITS Peercaching
☐ Client to make VoIP calls.
☐ Connect to a Network Projector
☑ Core Networking
☑ CyberLink Media Server
☑ Cyberlink Media Server Browser Engine
☑ CyberLink PowerCinema
☑ CyberLink PowerCinema Resident Program
☐ Distributed Transaction Coordinator
☑ eMule

☑ Notify me when Windows Firewall blocks a new program

FIGURE 7: THE EASE OF TURNING THE FIREWALL OFF

3.1.3 ACCESSING THE FIREWALL

Similar to the needs on easily changing the status of the firewall, it should be possible for the users to easily access it to control the behavior of the system which brings user control and freedom to the users once dealing with the firewall. Our initial investigations of the simple firewall interface, demonstrated that there is no way for the user to navigate from the simple firewall interface to the advanced firewall interface. It gets even worse once we realized that there is hardly any help or indication about the existence of such an advanced firewall interface for the user. This is while the user may need to interact with the advanced firewall interface in order to be able to define, change, or modify the firewall rules (Figure 3). The advanced firewall interface is placed under the Administrative Tools category under Windows Vista's control panel. It is thus very difficult for the user to find the correct location for this advanced firewall interface without previously being aware of its existence (Figure 8).

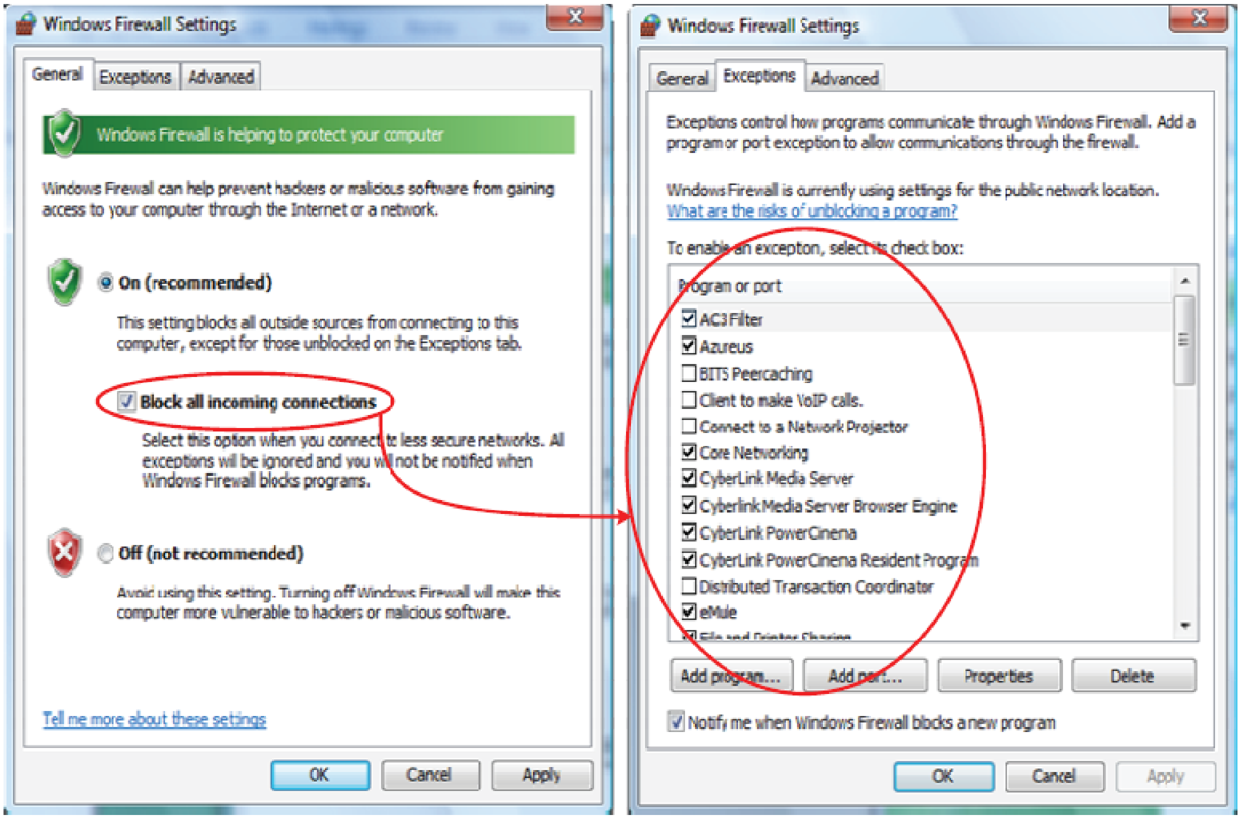


Name	Date modified	Type	Size
Computer Management	02/11/2006 5:54 AM	Shortcut	2 K
Data Sources (ODBC)	02/11/2006 5:53 AM	Shortcut	2 K
Event Viewer	02/11/2006 5:54 AM	Shortcut	2 K
iSCSI Initiator	02/11/2006 5:54 AM	Shortcut	2 K
Memory Diagnostics T...	02/11/2006 5:53 AM	Shortcut	2 K
Reliability and Perform...	02/11/2006 5:53 AM	Shortcut	2 K
Services	02/11/2006 5:53 AM	Shortcut	2 K
System Configuration	02/11/2006 5:53 AM	Shortcut	2 K
Task Scheduler	02/11/2006 5:54 AM	Shortcut	2 K
Windows Firewall with ...	02/11/2006 5:53 AM	Shortcut	2 K

FIGURE 8: THE EASE OF TURNING THE FIREWALL ON/OFF

3.1.4 BLOCKING ALL THE INCOMING CONNECTIONS

The check box for blocking all the incoming connections in the simple firewall interface has been placed in the same tab where the firewall can be turned on or off. This has made this option invisible to the user such that it is hard for the user to block or unblock all the incoming connections from the simple firewall interface (Figure 9). A second problem is inter-related between the General tab of the simple firewall interface and its Exceptions tab. Even in a situation where the check box for “Blocking all the incoming connections” is selected, the user can still modifies the list of exceptions for different programs/ports. Nevertheless, this change to the exception list will have no effect on the behavior of the system, as checking the "Block all incoming connections" box will automatically drop all the incoming requests (Figure 9).



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

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

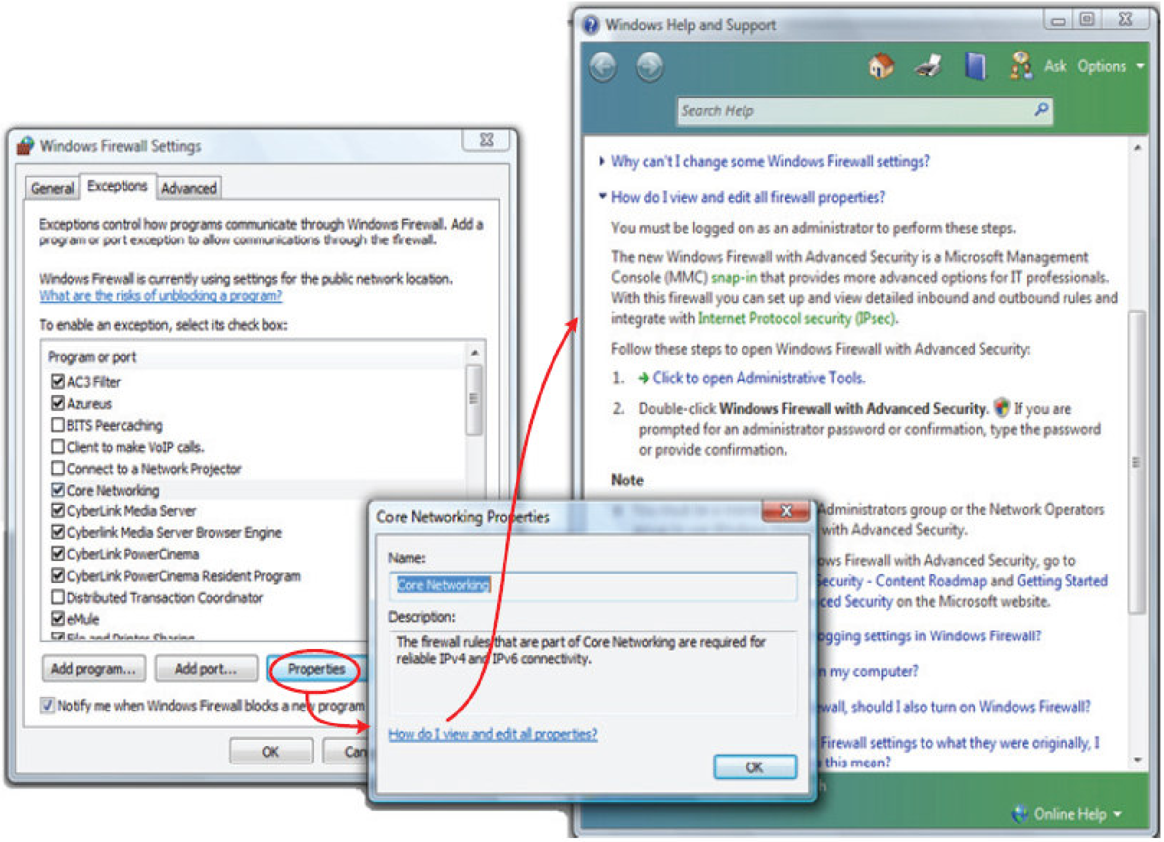
Program or port
- ☑ AC3Filter
- ☑ Azureus
- □ BITS Peercaching
- □ Client to make VoIP calls.
- □ Connect to a Network Projector
- ☑ Core Networking
- ☑ CyberLink Media Server
- ☑ CyberlinkMedia Server Browser Engine
- ☑ CyberLink PowerCinema
- ☑ CyberLink PowerCinema Resident Program
- □ Distributed Transaction Coordinator
- ☑ eMule
- ☑ File and Printer Sharing

☑ Notify me when Windows Firewall blocks a new program

FIGURE 9: BLOCKING ALL INCOMING CONNECTIONS

3.1.5 CONFUSING FUNCTIONALITY OF THE PROPERTIES BUTTON

In the Exceptions tab of firewall settings window, there is a "properties" button which, at the first glance, seems to contain the properties of the tab. However, it just relates to the programs and ports listed in the exception list. This inherent ambiguity in the functionality of this button can be confusing to the end user. Once the property button on the Exceptions tab is clicked, it shows the basic properties defined for the selected program from the list of exceptions. To edit the properties, the user has to have administrative privileges; however, there is no way for the user to execute this task with administrative privileges from this point. Moreover, even with administrative privileges, the user still needs to go to the advanced firewall interface to view and edit the properties, and there is no way to help the user navigate to the advanced firewall interface from this location. Consequently, the task of the button is totally misleading for the user (Figure 10).



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port
☑ AC3 Filter
☑ Azureus
□ BITS Peercaching
□ Client to make VoIP calls.
□ Connect to a Network Projector
☑ Core Networking
☑ CyberLink Media Server
☑ Cyberlink Media Server Browser Engine
☑ CyberLink PowerCinema
☑ CyberLink PowerCinema Resident Program
□ Distributed Transaction Coordinator
☑ eMule
☑ File and Printer Sharing

☑ Notify me when Windows Firewall blocks a new program

Name: Core Networking

Description: The firewall rules that are part of Core Networking are required for reliable IPv4 and IPv6 connectivity.

How do I view and edit all properties?

▸ Why can't I change some Windows Firewall settings?

▾ How do I view and edit all firewall properties?

You must be logged on as an administrator to perform these steps.

The new Windows Firewall with Advanced Security is a Microsoft Management Console (MMC) snap-in that provides more advanced options for IT professionals. With this firewall you can set up and view detailed inbound and outbound rules and integrate with Internet Protocol security (IPsec).

Follow these steps to open Windows Firewall with Advanced Security:

1. ➔ Click to open Administrative Tools.
2. Double-click **Windows Firewall with Advanced Security.** If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

Note

Administrators group or the Network Operators with Advanced Security.

ws Firewall with Advanced Security, go to ecurity - Content Roadmap and Getting Started ced Security on the Microsoft website.

gging settings in Windows Firewall?

n my computer?

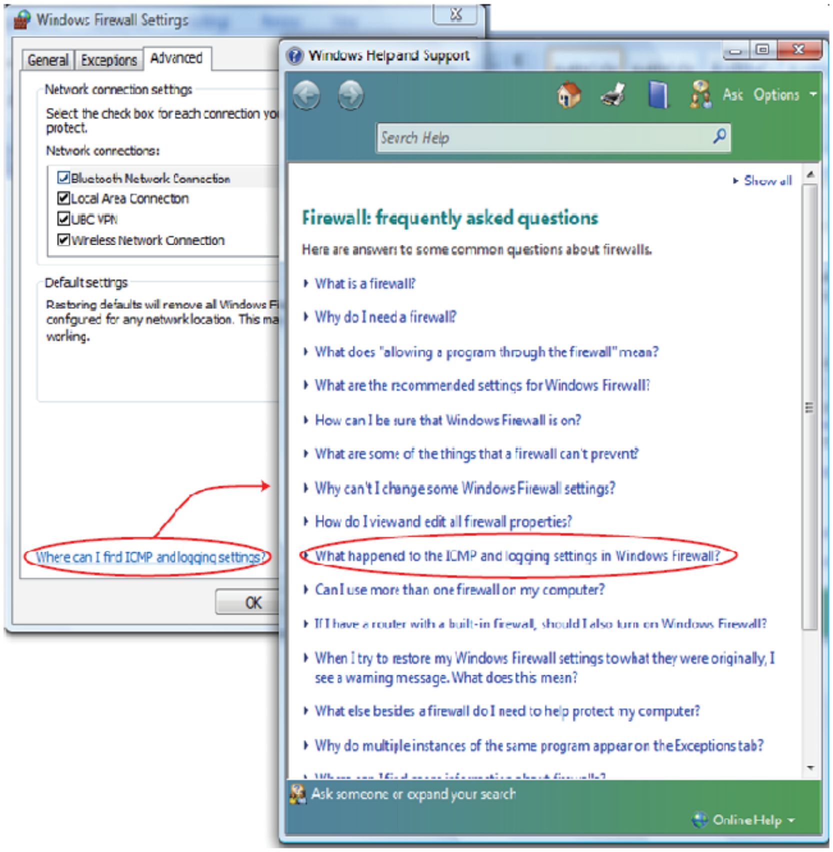
wall, should I also turn on Windows Firewall?

Firewall settings to what they were originally, I this mean?

FIGURE 10: CONFUSING FUNCTIONALITY OF PROPERTIES BUTTON

3.1.6 INSUFFICIENT HELP CONTENT

Not having enough help material to shine some light on the current status of a user can be considered as a clear usability problem in a system, contradicting the ninth and tenth Nielsen's criteria (see Table 1) which is asking for help and documentation that can assist users with recognizing, diagnosing, and recovering from errors. Our initial and heuristic evaluation of the system showed that Windows Vistas firewall lacks enough help material to solve users' confusion. It appeared that in multiple situations, the current help for Windows Vista's firewall either is completely missing or does not directly take the user to the desired help material. One of the main issues with respect to the firewall help is that, most of the help links are directed to one static page of Frequently Asked Questions. This is then left up to the user to search among the existing questions and find the answer for the question that s/he is looking for. Also, it turned out that some pages of the firewall had irrelevant link or no link to any help page at all (Figure 11). Another issue with respect to the help in Windows Vista's firewall is that there is no lightweight help for the simple firewall interface. It basically means that there is no way for the user to find the usage of a button or to understand the meaning of a concept by hovering the mouse on it.



Network connection settings

Select the check box for each connection yo
protect.

Network connections:

☑ Bluetooth Network Connection
☑ Local Area Connecton
☑ UBC VPN
☑ Wireless Network Connection

Default settings

Restoring defaults will remove all Windows Fi
configured for any network location. This ma
working.

Where can I find ICMP and logging settings?

Firewall: frequently asked questions

Here are answers to some common questions about firewalls.

- What is a firewall?
- Why do I need a firewall?
- What does "allowing a program through the firewall" mean?
- What are the recommended settings for Windows Firewall?
- How can I be sure that Windows Firewall is on?
- What are some of the things that a firewall can't prevent?
- Why can't I change some Windows Firewall settings?
- How do I view and edit all firewall properties?
- What happened to the ICMP and logging settings in Windows Firewall?
- Can I use more than one firewall on my computer?
- If I have a router with a built-in firewall, should I also turn on Windows Firewall?
- When I try to restore my Windows Firewall settings to what they were originally, I see a warning message. What does this mean?
- What else besides a firewall do I need to help protect my computer?
- Why do multiple instances of the same program appear on the Exceptions tab?

FIGURE 11: IMPROPER USE OF HELP

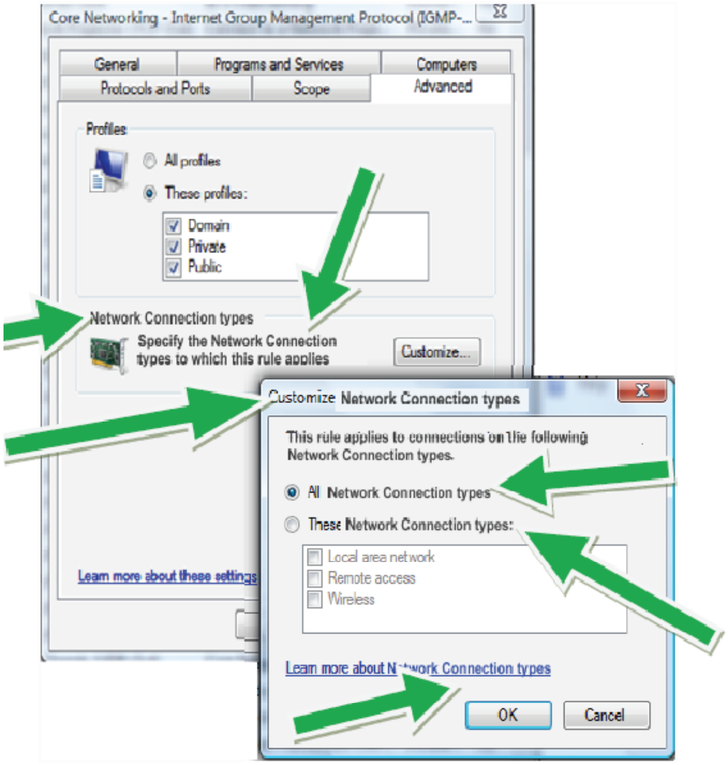
3.2 MEDIUM FIDELITY PROTOTYPE

Having the requirements collected from the heuristic phase, the next step would be to design a prototype that can be compliant with the requirements of the user on one hand, and can address the set of Nielsen's usability criteria [9] as well as the principles for designing security systems that we pointed out in the previous section. In this section we go over the identified problems from Section 3.1 and we represent the alternative prototype that we came up with, in order to address and possibly solve those problems. At each point we also justify why we believe the new prototype would be a good alternative to be taken into consideration while designing the interface.

3.2.1 TERMINOLOGY INCONSISTENCIES

In Section 3.1.1, we mentioned some of the inconsistencies that we detected while analyzing the interface of Windows Vista's firewall. In our rectification of these inconsistencies we try to refer to the mental model of the users and also the backgrounds that they may have obtained as a consequence of working with other environments and technologies that use similar concepts. This conceptual analysis of users' mental models formed the basis for our manipulation and correction of the terminologies in Windows Vista's firewall interface.

Interchangeable use of the terms Network Connection and Interface. Having the two terms compared, we realized that the term "Network Connection" carries a better conceptual meaning, as older versions of MS Windows (including Windows XP) use the same term to refer to different network access points handled by different network adaptors. The term "Interface" seems to be a new concept emerging from the advanced security interface for Windows Vista's firewall with a much broader meaning than what is intended for the conceptual model of a network connection and its adaptor. Consequently, for our prototype, we suggested the term "Network Connection" to be used across the whole GUIs for both simple and advanced firewall interfaces (see Figure 12).



Profiles

○ All profiles

● These profiles:

☑ Domain
☑ Private
☑ Public

Network Connection types

Specify the Network Connection types to which this rule applies

Learn more about these settings

Customize Network Connection types

This rule applies to connections on the following Network Connection types.

● All Network Connection types

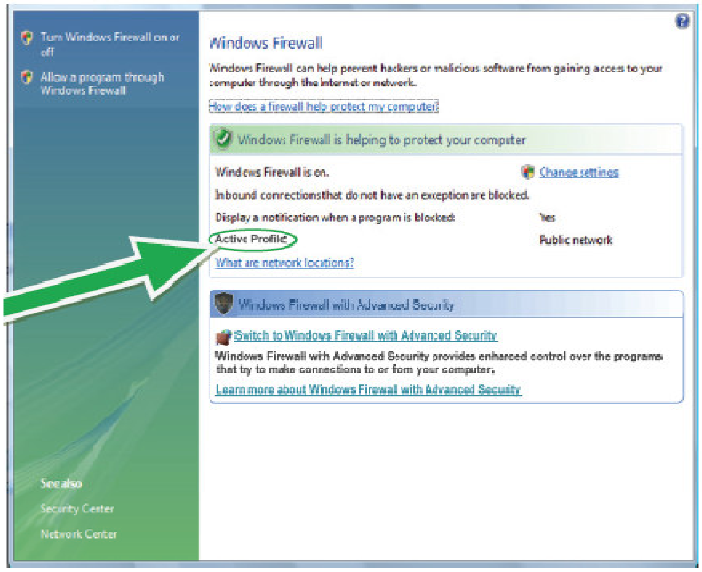
○ These Network Connection types:

□ Local area network
□ Remote access
□ Wireless

Learn more about Network Connection types

FIGURE 12: RESOLVING THE TERMINOLOGY IN OUR SUGGESTED INTERFACE

Interchangeable use of Profile and Network Location. Another point of inconsistency appeared between the terms "Profile" and "Network Location" with both referring to the context in which the user of the system has been situated. The idea behind this term is to give the users (possibly with mobile computers) the flexibility to switch from one location to another and at the same time be able to rapidly reconfigure their system settings to adjust the firewall with the required controls that they expect over their resources. To choose the optimal solution, we referred to the mental model of users' minds. It turned that most of mobile phones also use the term "Profile" to refer to the current context in which a user is located, a motivating enough reason for us to prefer "Profile" over "Network Location" (Figure 13).



Turn Windows Firewall on or off
Allow a program through Windows Firewall
See also
Security Center
Network Center

Windows Firewall

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

How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

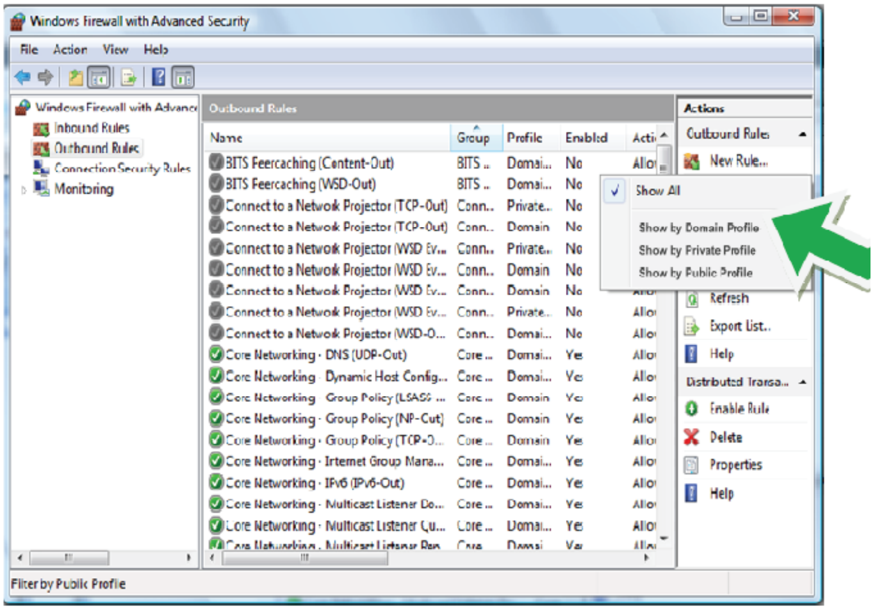
Windows Firewall is on.	Change settings
Inbound connections that do not have an exception are blocked.	
Display a notification when a program is blocked:	Yes
Active Profile:	Public network

Windows Firewall with Advanced Security

Windows Firewall with Advanced Security provides enhanced control over the programs that try to make connections to or from your computer.

FIGURE 13: SUGGESTED MODIFICATION TO THE SIMPLE INTERFACE IN ORDER TO RESOLVE THE INCONSISTENCIES FOR THE TERMS NETWORK LOCATION AND PROFILE

Improper use of the term 'filter' to change the view format. Having thought from users' perspective, we realized that the term "Filter" in the context of a firewall application conveys a meaning closer to filtering out some information, programs, or ports, whereas, according to Section 3.2.1, this term is used in the current version of the advanced interface for Windows Vista's firewall to filter out some of the information presented on the screen and to change the view of the information. We believe such a misuse for the word "Filter" will become confusing for the users with their expectations. The term "Show" appeared to be a more acceptable and a self-contained term to be chosen for the purpose of changing the view of the shown information. Consequently our team decided to replace "Filter" with "Show" to be tested in our alternative prototype (Figure 14).



Name	Group	Profile	Enabled	Acti
BITS Peercaching (Content-Out)	BITS ..	Domai...	No	Allo
BITS Peercaching (WSD-Out)	BITS ..	Domai...	No	
Connect to a Network Projector (TCP-Out)	Conn..	Private...	No	
Connect to a Network Projector (TCP-Out)	Conn..	Domain	No	
Connect to a Network Projector (WSD Ev...	Conn..	Private...	No	
Connect to a Network Projector (WSD Ev...	Conn..	Domain	No	
Connect to a Network Projector (WSD Ev...	Conn..	Domain	No	
Connect to a Network Projector (WSD Ev...	Conn..	Private...	No	Allo
Connect to a Network Projector (WSD-O...	Conn..	Domai...	No	Allo
Core Networking - DNS (UDP-Out)	Core ...	Domai...	Yes	Allo
Core Networking - Dynamic Host Config...	Core ...	Domai...	Yes	Allo
Core Networking - Group Policy (LSASS ...	Core ...	Domain	Yes	Allo
Core Networking - Group Policy (NP-Out)	Core ...	Domain	Yes	Allo
Core Networking - Group Policy (TCP-O...	Core ...	Domain	Yes	Allo
Core Networking - Internet Group Mana...	Core ...	Domai...	Yes	Allo
Core Networking - IPv6 (IPv6-Out)	Core ...	Domai...	Yes	Allo
Core Networking - Multicast Listener Do...	Core ...	Domai...	Yes	Allo
Core Networking - Multicast Listener Qu...	Core ...	Domai...	Yes	Allo

Filter by Public Profile

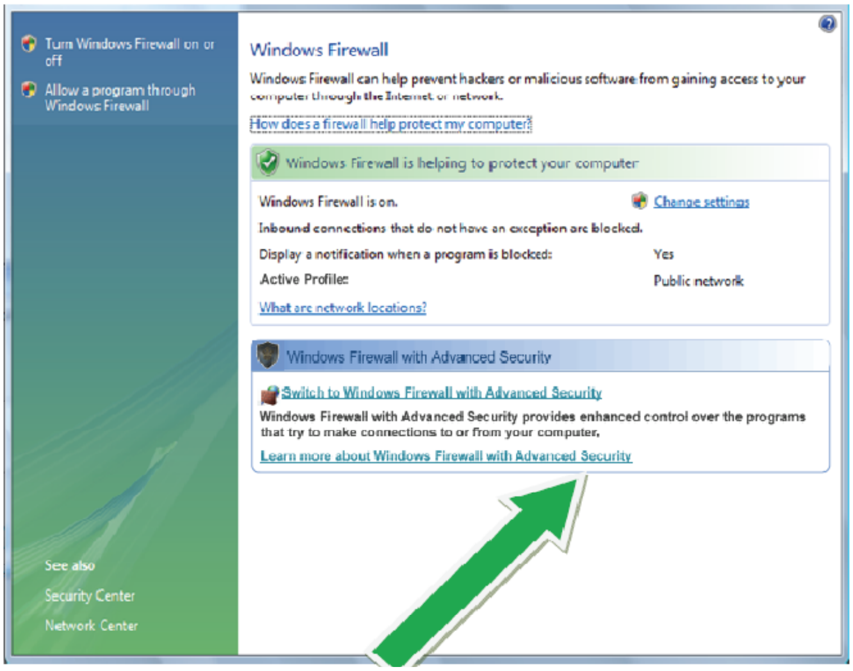
FIGURE 14: REPLACEMENT OF THE TERM "FILTER" WITH "SHOW"

3.2.2 THE EASE OF TURNING THE FIREWALL ON/OFF

In Section 3.1.2, we identified a problem of malfunction with Windows Vista's firewall interface. The solution to this problem would be to modify the functionality of this button such that it can directly navigate the user to the desired tab. In our prototype, however, we didn't try to address this feature due to its simplicity.

3.2.3 ACCESSING THE FIREWALL

One of the most challenging problems with the current implementation of Windows Vista's firewall is how to access the firewall. As mentioned in Section 3.1.3, it was so hard, even for our experimenters of the system, to figure out how to access the advanced interface for Windows Vista's firewall. It seems to be a big hurdle for novice users to find it without being already familiar with its existence. For the purpose of our prototype we decided to have a direct access to the advanced firewall from the simple firewall interface, something that seems to be currently missing in the simple interface for Windows Vista's firewall. This also helps the user to become aware of the existence of another interface with more advanced functionalities for Windows Vista. This might motivate some of the users to later on learn how to use this interface for their own goods (Figure 15).


Turn Windows Firewall on or off
Allow a program through Windows Firewall
See also
Security Center
Network Center

Windows Firewall

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

How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

Windows Firewall is on. Change settings

Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked: Yes

Active Profile: Public network

What are network locations?

Windows Firewall with Advanced Security

Switch to Windows Firewall with Advanced Security

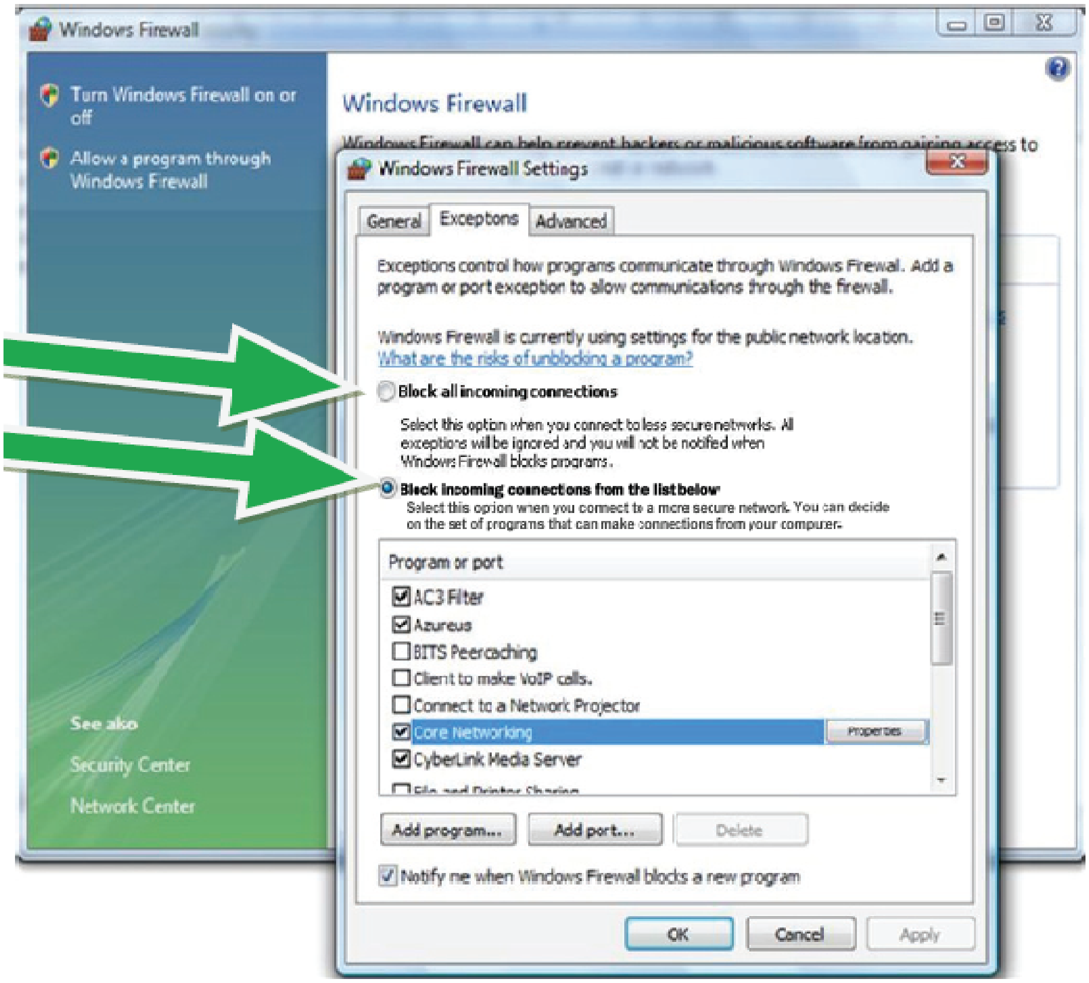
Windows Firewall with Advanced Security provides enhanced control over the programs that try to make connections to or from your computer.

Learn more about Windows Firewall with Advanced Security

FIGURE 15: PLACING A LINK TO THE ADVANCED INTERFACE IN THE SIMPLE INTERFACE

3.2.4 BLOCKING ALL THE INCOMING CONNECTIONS

Basically the "Exceptions" tab in the simple interface for Vista's firewall takes care of managing different programs and ports by either letting them through the firewall or blocking their access to the internet. We modified this tab such that it also has the check box for blocking or unblocking all the incoming connections. In this case the name of the tab can be changed to "Program/Port Access Control". Also in our prototype we suggested a change in the design of the Exceptions tab so that checking the box for "Block all the incoming connections" will not prevent us from manipulating other programs. This decision was made to enable the users in critical situations (i.e. where a threat is perceived by the user) to first block all the incoming connections and then disable the programs or ports that are causing the problem. Thereafter, the user will possibly be able to unblock the other connections and get back to her regular tasks (Figure 16).



Windows Firewall can help prevent hackers or malicious software from gaining access to

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

○ **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.

● **Block incoming connections from the list below**
Select this option when you connect to a more secure network. You can decide on the set of programs that can make connections from your computer.

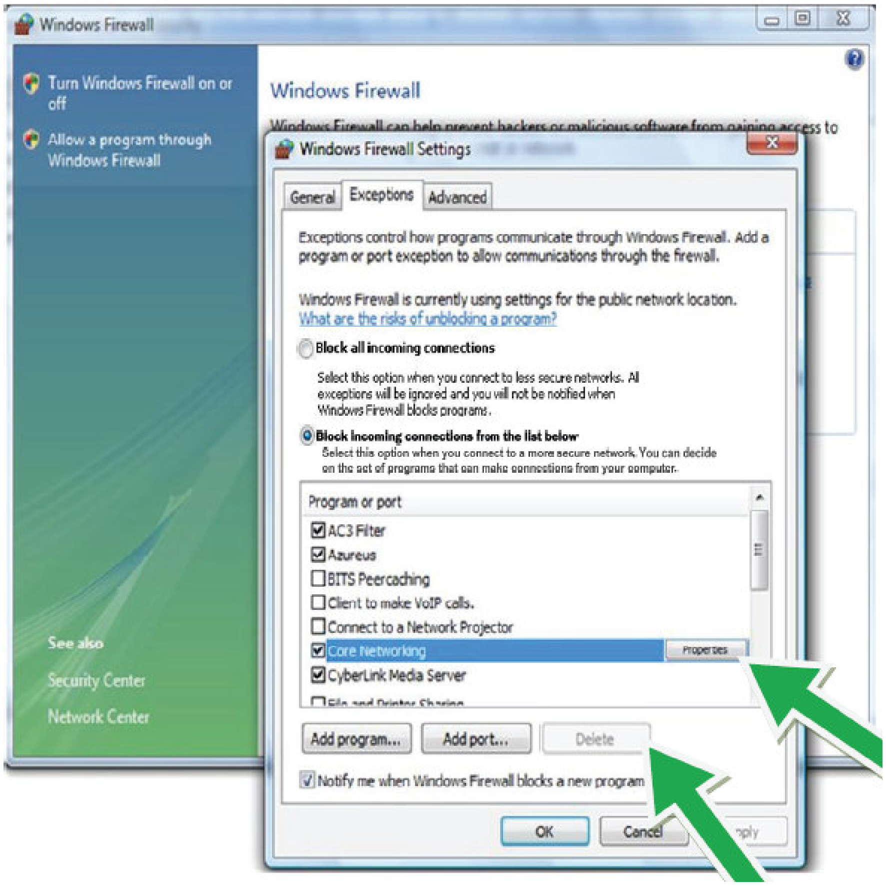
Program or port
☑ AC3 Filter
☑ Azureus
□ BITS Peercaching
□ Client to make VoIP calls.
□ Connect to a Network Projector
☑ Core Networking Properties
☑ CyberLink Media Server
□ File and Printer Sharing

☑ Notify me when Windows Firewall blocks a new program

FIGURE 16: OUR PROTOTYPE FOR HANDLING EXCEPTIONS AND BLOCKING CONNECTIONS

3.2.5 CONFUSING FUNCTIONALITY OF THE PROPERTIES BUTTON

The confusing presence of the "properties" button in the advanced tab was another point of change in our new prototype. We got to an agreement that having the properties button placed right in front of each program or would make more sense with helping the user to understand which program the properties button is related to. As a result, in our prototype we shifted the properties button in front of each selected program resulting in having an interface which is much closer to the user’s mental model in terms of understanding the functionality of the “properties” button (Figure 17).



Windows Firewall can help prevent hackers or malicious software from gaining access to

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

○ **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.

● **Block incoming connections from the list below**

Select this option when you connect to a more secure network. You can decide on the set of programs that can make connections from your computer.

Program or port
☑ AC3 Filter
☑ Azureus
□ BITS Peercaching
□ Client to make VoIP calls.
□ Connect to a Network Projector
☑ Core Networking Properties
☑ CyberLink Media Server
□ File and Printer Sharing

☑ Notify me when Windows Firewall blocks a new program

FIGURE 17: OUR PROTOTYPE TO HANDLE PROPERTIES FOR EACH OF THE EXCEPTIONS IN THE FIREWALL

3.2.6 INSUFFICIENT HELP CONTENT

The problem with insufficient help content can be addressed by making the references to the target help materials more direct and accurate such that the end users can better find the help contents they are looking for. In our new prototype however, we didn’t try to address this issue as there seems to be a straight forward solution for this problem.

3.3 BACKGROUND WORK ON ANALYSIS OF THE BASIC VISTA’S FIREWALL

We conducted an independent user study to confirm the reality and validity of the problems we found in our heuristic evaluation (See Appendices A and B). In this study, we conducted surveys, interviews and lab experiments in order to evaluate the usability of Microsoft Windows Vista's Firewall in its current format. It is worth mentioning that the studied samples of lab experiment, survey, and interviews are different.

In our previous study we used the same questionnaire as the one in this study. The participants of the survey were very diverse, but most of them were undergraduate students of UBC from different majors. Also, we had a number of Masters and PhD students. The goal of the survey was to gain an understanding of the general knowledge of the university's population about firewalls and their preferences. The result of our survey can be found in Appendix B.

After the survey, we tried to analyze Vista's firewall's usability by interviewing users. To study user judgments about Vista's firewall, we first asked users to do some pre-defined tasks. The goal of this step was to make users familiar with Vista's firewall (since the results of our survey showed that most of the users are not familiar with Vista and especially with its firewall). After users performed the tasks, we had an interview with them. By asking some pre-defined questions, we tried to understand participant experiences with Vista's firewall. Our interview was semi-structured and the questions were open-ended and varied depending on responses we got from the participants. We have shown the result of the interviews in Appendix B.

In parallel with sample survey and interviews, a laboratory experiment was conducted with twelve participants. In this study the users were asked to perform some typical tasks with firewall (See Appendix A). The results of this study validated our findings in our heuristic evaluation.

As can be seen in Figure 18, most of our participants looked for a shortcut to access the simple firewall interface and about 83% of them had difficulty accessing the firewall with advanced security (Figure 19). These results show the need for improvements in accessing the firewall.

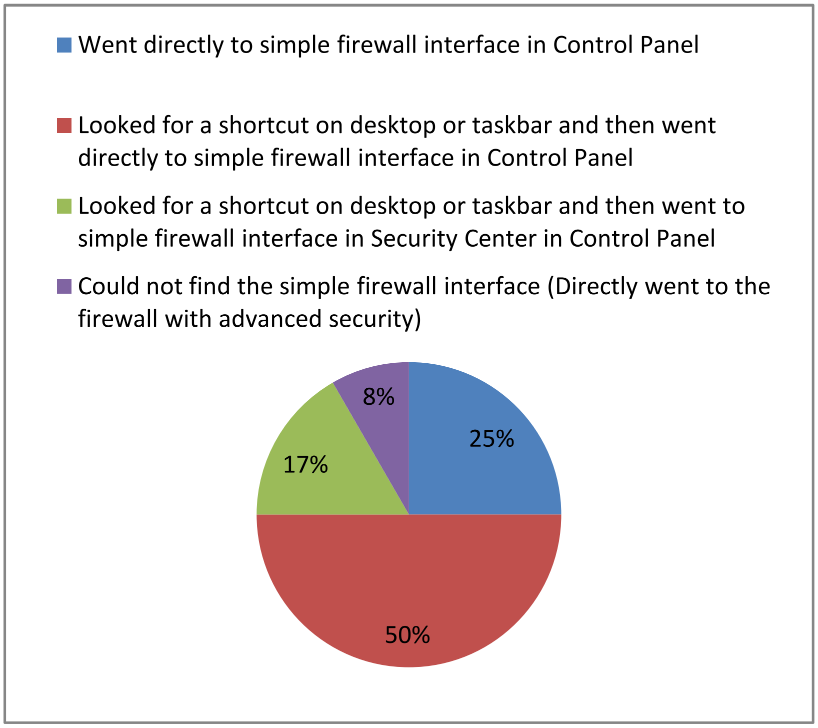


FIGURE 18: ACCESSING THE SIMPLE FIREWALL INTERFACE

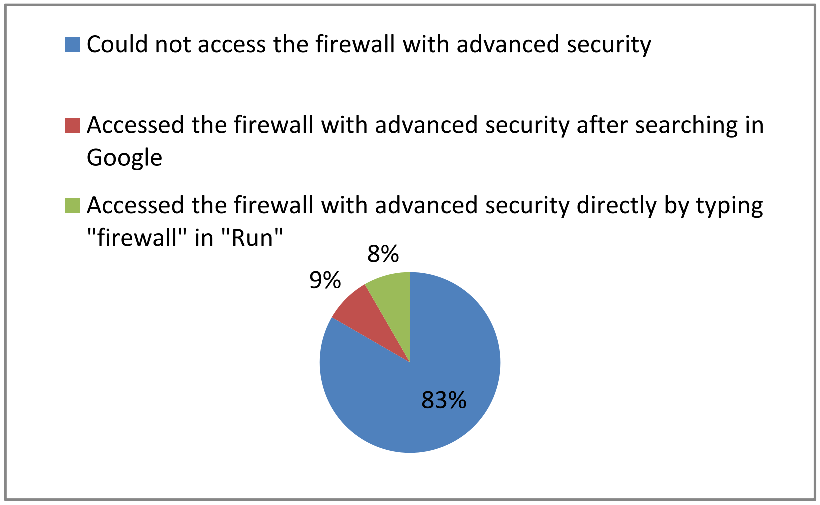


FIGURE 19: ACCESSIN THE FIREWALL WITH ADVANCED SECURITY

Most of our participants had problems in finding out exactly where to block all incoming connections (Figure 20). This was due to the fact that the check box for this purpose was in a window where there were two prominent options for turning the firewall on/off and this check box was not obvious at all. Therefore the participants went to the Exceptions tab where they could change the settings for programs and ports. This result validates the problem with the placement of this option in the firewall interface.

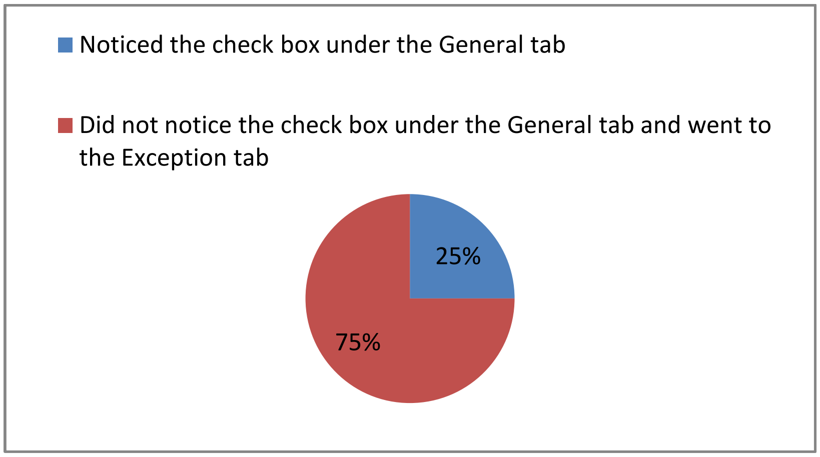


FIGURE 20: BLOCK ALL INCOMING CONNECTIONS

All participants thought that 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?

Finally as depicted in Figure 21, only 42% of the participants could correctly guess the functionality of the button "Properties". Only 33% of our participants could correctly identify that the link "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 (Figure 22). They thought that this link is somehow related to some functionality of the firewall instead of just displaying some specific categories of the rules.

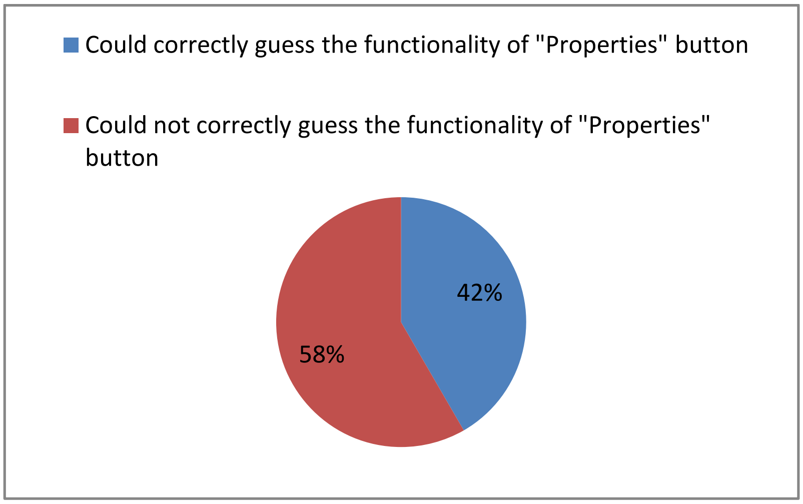


FIGURE 21: COMMNET ON THE FUNCTIONALITY OF PROPERTIES BUTTON

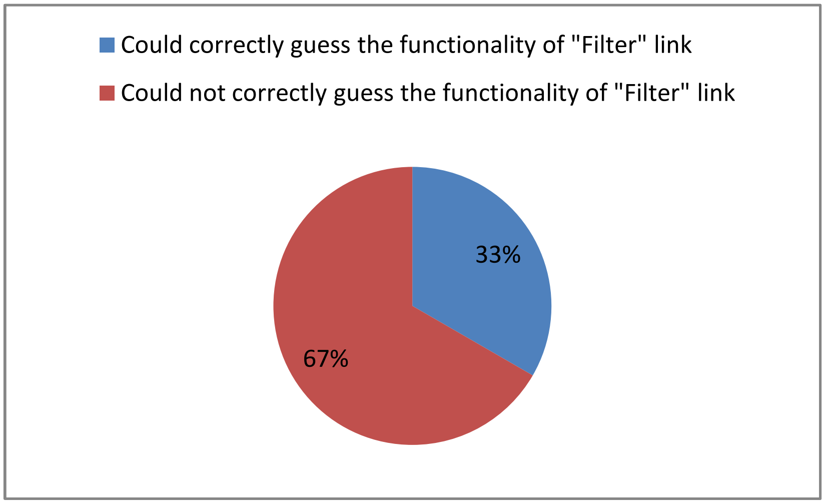


FIGURE 22: COMMENT ON THE FUNCTIONALITY OF FILTER LINK

All the above results from this 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 visibility of system status, user control and freedom, error prevention, and sufficient help and documentation. Consequently, we have made some suggestions for improvement and continued our analysis based on these suggestions.

3.4 USER STUDY

We conducted a user study in order to evaluate the usability of our prototype for Vista's Firewall. Each participant completed a one-hour session in our study. In this session, first s/he was introduced to the theme of our project. Then upon the completion of appropriate consent form (Appendix D) and the questionnaire, the user was asked to perform specific tasks on the test computer. The details of our user study are presented in the following sections.

3.4.1 QUESTIONNAIRE

Before starting the user study of the prototype, our participants completed a questionnaire comprising 15 questions. The content and questions in this questionnaire have been obtained from the report contained in appendix B. By means of the questionnaire, we wanted to obtain general demographic information about our participants and information about the expectations of the users of a good personal firewall. (We have attached the questionnaire in Appendix C of this report.) In this section, we provide an overview of the results from the questionnaire. It is worth mentioning that the participants of this survey are the same as those who participated in our user study.

Our survey had 9 participants. Our participants were all university students (2 Computer Science PhD students, 4 Electrical and Computer Engineering PhD students, 2 Interactive Arts Master students, and 1 Interactive Arts Bachelor student). Most of our participants displayed good knowledge about computers in general; a couple of them even had a strong background in Human-Computer Interaction.

The first few questions in our questionnaire were about the operating systems and the security related software used by the participants. As shown in figure 23, 89% of our participants had Windows XP on their computers; only one participant had Windows Vista installed.

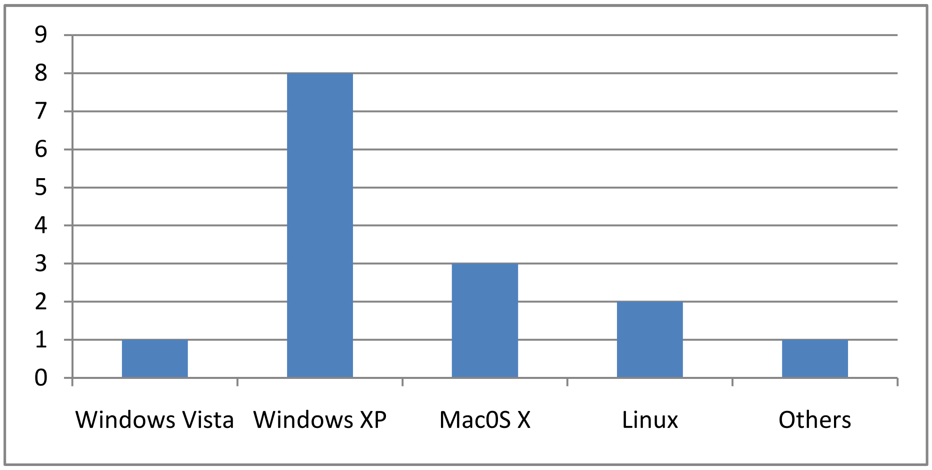


FIGURE 23: THE OPERATING SYSTEM INSTALLED ON THE PARTICIPANTS' COMPUTER

Also, the results of the questionnaire show that the firewall is one amongst the important security software programs used by the participants. Information about the security software programs installed on the participants' computers is shown in figure 24.

.

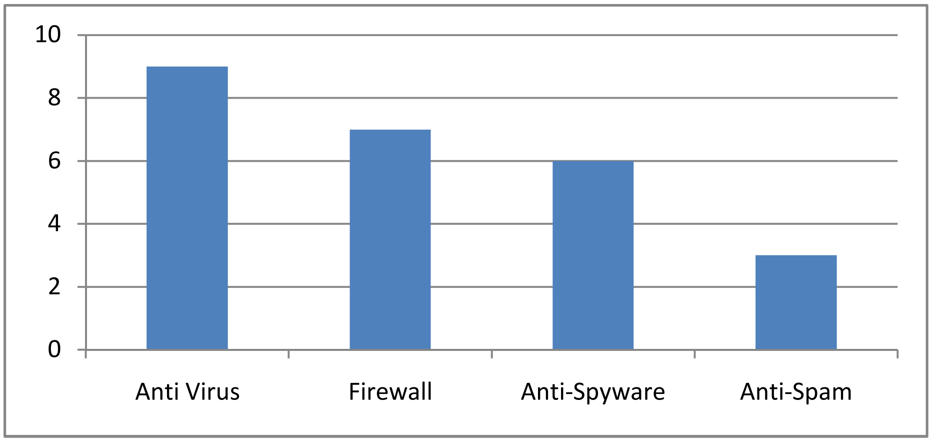


FIGURE 24: SECURITY SOFTWARE INSTALLED ON THE PARTICIPANTS' COMPUTER

In the next set of questions, we sought some information about participants' knowledge of firewalls, Windows Vista, and Vista's firewall (in that order). As shown in figure 25, about 56% of the participants have had experience with some kind of personal firewall and have explored its different capabilities; only one participant had no experience with any kind of firewall.

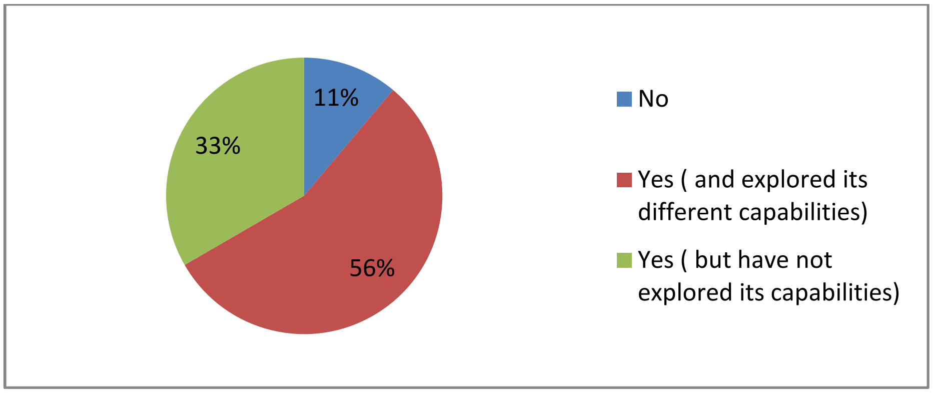


FIGURE 25: PREVIOUS EXPERIENCE OF PARTICIPANTS WITH A PERSONAL FIREWALL

Also, when our participants were asked about the reasons for using firewalls on their computers, about 56% said that they had installed firewalls on their computers in order to "control network connections" (see figure 26). This shows that our participants possessed adequate knowledge about the goal of installing and using a firewall.

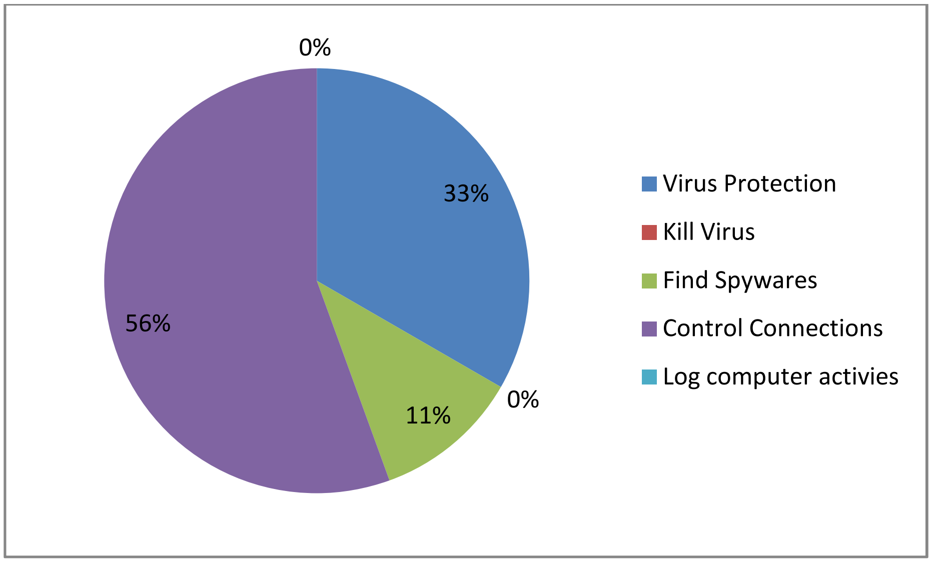


FIGURE 26: THE REASON FOR INSTALLING A FIREWALL FROM PARTICIPANTS' POINT OF VIEW

The participants also expressed awareness of the fact that most operating systems have firewalls built into them (89%, from figure 27); however, some thought that MacOS and Linux operating systems do not have built-in firewalls. (We hypothesize that this may be due to MacOS's idea of making security invisible (for the most part) to the end user.)

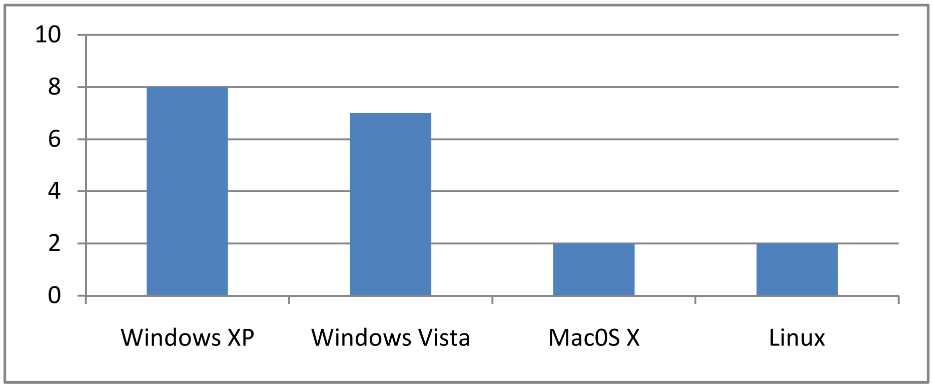


FIGURE 27: THE OPERATING SYSTEMS WITH A BUILT-IN FIREWALL FROM PARTICIPANTS' POINT OF VIEW

When participants were asked about their experience with Windows Vista, as shown in Figure 28, 67% of the participants responded saying that they had not had previous experience with Vista; only 11% had more than 3 months experience with using Vista .

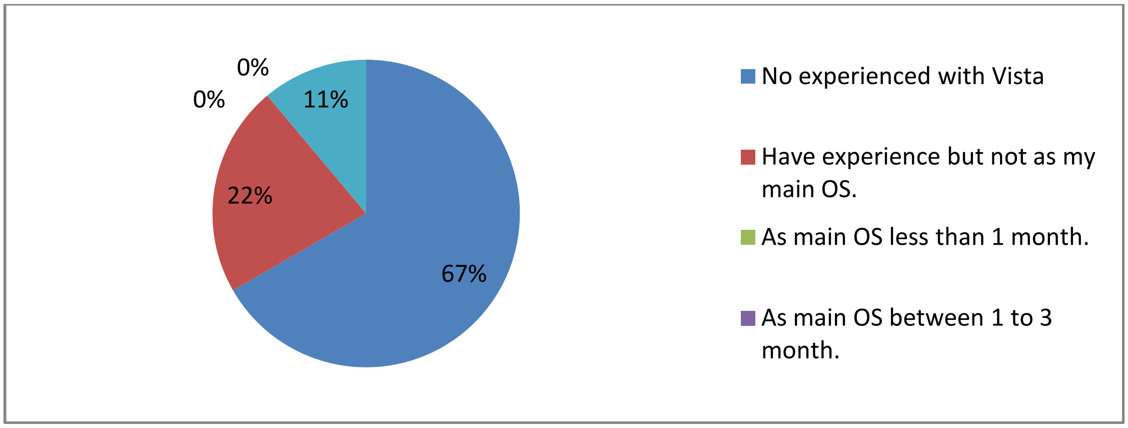


FIGURE 28: PARTICIPANTS' EXPERIENCE WITH WINDOWS VISTA

After questions about participants' general knowledge, we asked some questions about the preference of the participants when they work with a firewall. In this part of the questionnaire, we avoided asking questions specific to Windows Vista, because we predicted that the participants usually wouldn't have had significant experience with Windows Vista.

In this part, we first asked participants about a good interface for a firewall. As we shown in Figure 29, 78% of the participants prefer a firewall with one advanced and one simple user interface which shows that Vista's approach is good.

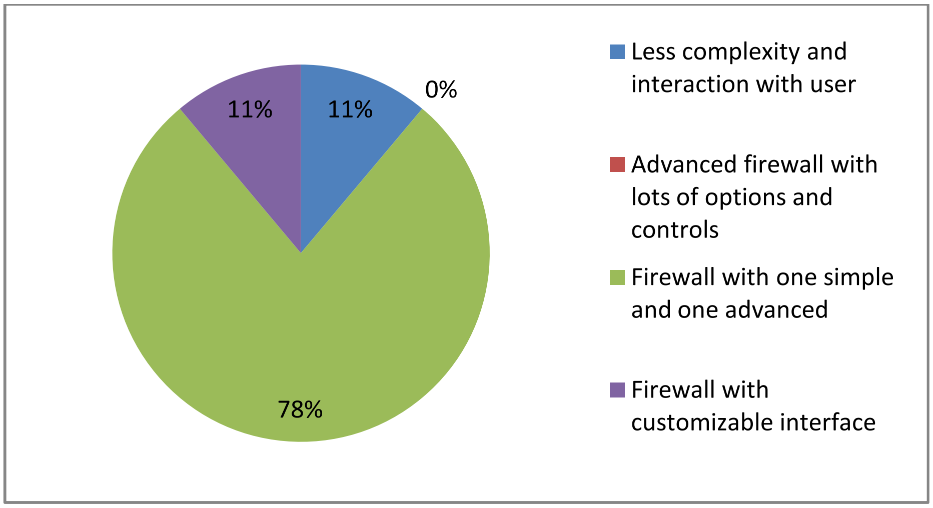


FIGURE 29: PARTICIPANTS PREFERENCE ABOUT FIREWALL'S USER INTERFACE

The participants also expressed the opinion (67%, see figure 30) that they would like to make most of the firewall-related decisions themselves and would prefer the firewall to merely help them in the process by giving some recommendations that would be helpful.

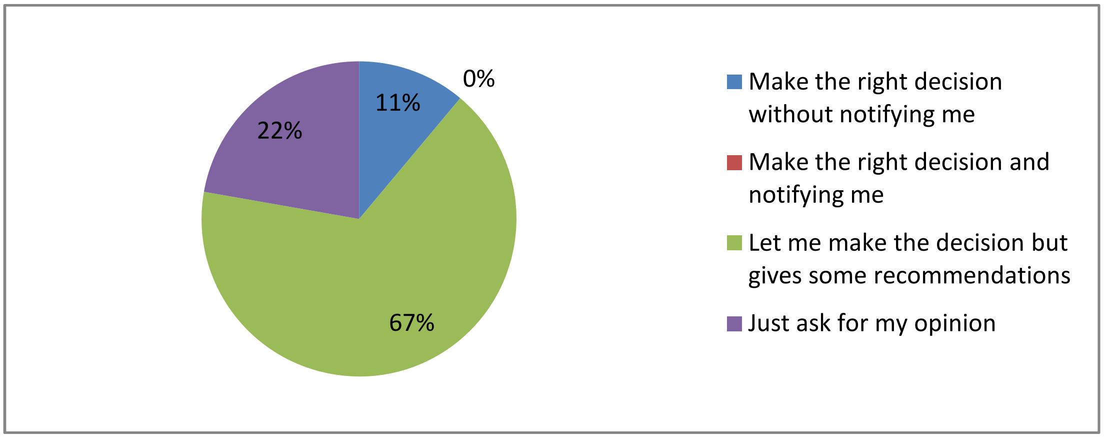


FIGURE 30: PARTICIPANTS' PREFERENCE FOR DECISION MAKING PROCESS

To gain understanding about participants' preference when they need some help or information about the firewall, we asked them if they prefer using firewall's built-in help or use search engines to find a solution. The result of the questionnaire shows that 6 out of 9 participants (67%) prefer using Google or other search engines to find an answer to their problems. The rest prefer using built-in help.

Finally, we asked participants about the features that they may use frequently within a month. The goal of this question is to have an understanding about which features are suitable for basic interface and which are suitable for advance interface. We show the result of this question in Figure 31.

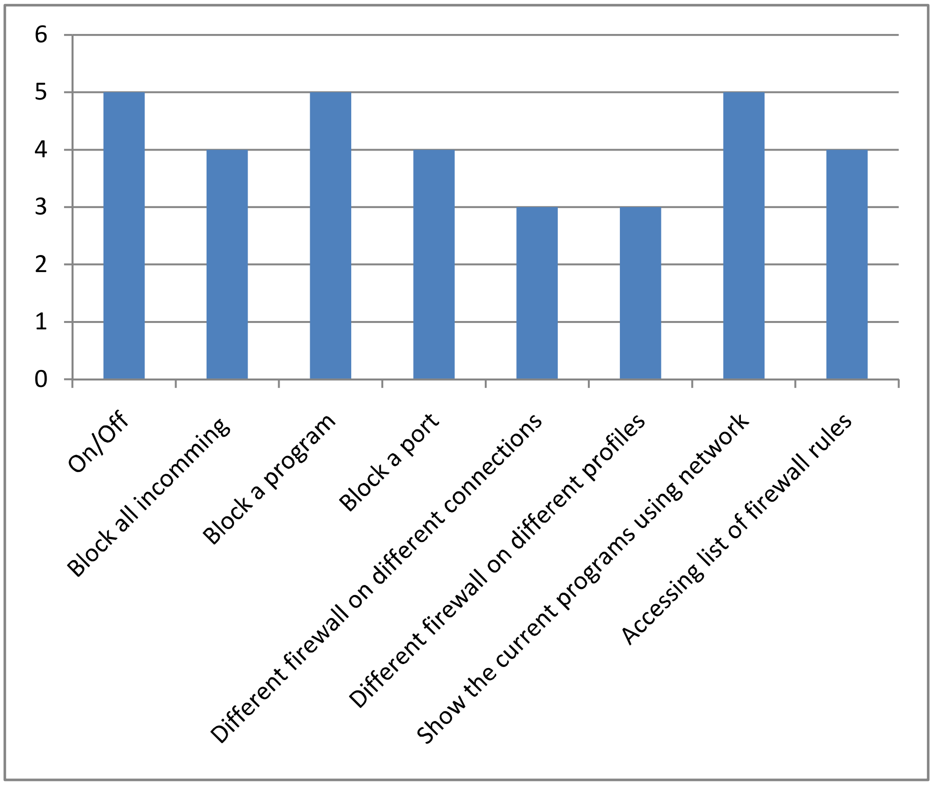


FIGURE 31: FEATURES THAT USED BY PARTICIPANTS FREQUENTLY

3.4.2 LABORATORY EXPERIMENT

In our laboratory experiment, we used a "*.pdf*" file in which we had a list of our proposed interfaces (each interface in one page). The user was told which page to go when s/he clicked on a link or button in an interface. We asked each participant to perform the following tasks on our prototype for Vista's firewall. These tasks were the typical tasks that one can perform on firewalls and covers some of our solutions we suggested in our prototype (the same tasks as in the study in Appendix A).

1. <u>Accessing the Simple Firewall Interface and the Firewall with Advanced Security:</u> the user could navigate through "Control Panel > Windows Firewall" in order to gain access to the simple firewall interface. Then s/he could click on a link there, in the main window (Figure 15), in order to access the Firewall with Advanced Security which gives her/him more detailed view of the firewall. It is important to have quick access to the firewall because the user may suddenly want to change some settings of the firewall when s/he encounters with a malicious logic.

2. <u>Determining the Current State of the Firewall:</u> The participants were asked to comment on the present status of the firewall. We were interested in knowing how they determined the current state and if there is enough hints for them for this purpose or not. 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 her/his computer is in a secure state (or not).

3. <u>Turning the Firewall On / Off:</u> There are two options available on the simple firewall interface to turn the firewall on/off, namely the "Turn Windows Firewall on or off" link in the sidebar of main window and the "Change Settings" link in the middle of that window (Figure 1). These links result in popping up the same window where the user can turn the firewall on / off (under the "General" tab). There is also a "Windows Firewall Properties" link in the firewall with advanced security (Figure 3) to perform this task. The user could click on this link in order to navigate to the appropriate window to turn the firewall on/off.

4. <u>Blocking all Incoming Connections:</u> In order to block all incoming connections, the user should click on the "Change Settings" link in the main window of the simple firewall interface, click on the "Exception" tab, and check the available radio button for this purpose (Figure 16). There is also a "Windows Firewall Properties" link in the firewall with advanced security to perform this task. The user could click on this link in order to navigate to the appropriate window to block all incoming connections. 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 not frequently 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 Vista's 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 main window and the "Change Settings" link in the middle of the same window. The first option directly navigates to the window in which the user could perform the task, but the second option navigates to a window in which the user should click on Exception tab to go to the appropriate window. In this window, the user could click on the "Add Program" button to add a program to the list of allowed programs (Figure 16). 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. Opening a specific Port on the Firewall: The user may decide to host a server program that needs to accept requests and replay 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" button. This is also a task that is frequently done and highly important. An exposed port could be a major source of system vulnerability. Thus, the decision needs to be made with care and be carefully managed.

7. 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 (Figure 2). This task enables the user to create highly granular rules that filter traffic based on specified conditions. Once created, these rules can be either enabled or disabled depending on the requirements of the network.

8. Using Firewall's Help: In this step, the user was asked to click on some of the help links offered within the Vista's Firewall interface to observe their thoughts about the help function in Windows Vista Firewall.

9. Commenting on the names of one button and one link in the firewall interface before clicking on them – specifically the "Properties" button under the "Exception" tab in the simple firewall interface and "Show" link in the firewall with advanced security: The purpose of this task was to see if the chosen features are open to misleading interpretations and whether the user can determine the expected functionality of these features. It is important because from the usability perspective the terms and features of the interface should enable users to instantly grasp the details of the conceptual model.

3.4.3 DATA COLLECTION

Both quantitative and qualitative data were collected during our study. The Quick Screen Recorder software was installed and used to capture the computer screen in order to record all user activities. Participants' responses to the questionnaires were also collected. Additionally, two experimenters sat with each participant throughout the sessions. The experimenters recorded every comment made by the participants regarding usability problems, as well as their general observations. If participants chose to talk during an experiment, they were not discouraged from doing so.

3.4 EVALUATION AND RESULTS

After conducting laboratory experiment, we analyzed the results of the experiment. We categorized the result of our analysis based on the tasks in Section 3.1:

1. Accessing the Simple Firewall Interface and the Firewall with Advanced Security: All of our participants first searched for a shortcut on desktop, taskbar, or tray and then went to the Control Panel in order to access Vista's firewall. That shows the need for a shortcut to access the firewall quickly. Five participants (56% of the population) went directly to the simple firewall interface in the Control Panel and the remaining found it in the Security Center of Windows Vista (Figure 32). The reason for this indirect access was that the items in control panel were sorted alphabetically and when the user was looking for the firewall, s/he noticed the Security Center before Windows Firewall. In general, none of our participants had problem with accessing the simple firewall.

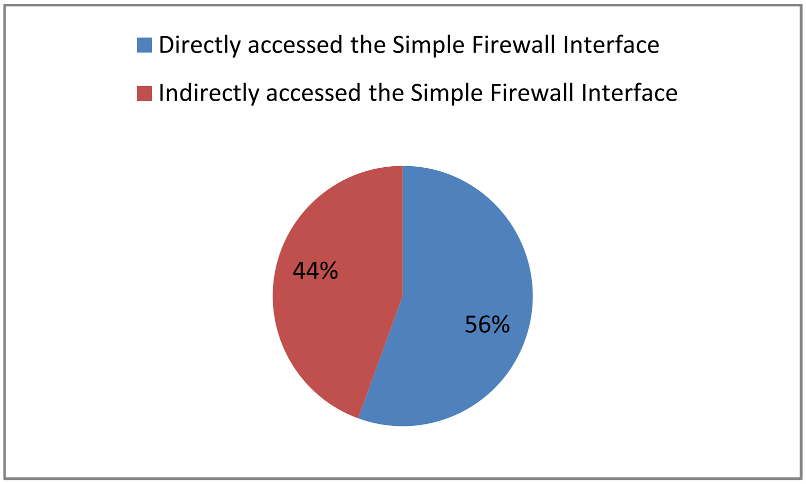


FIGURE 32: ACCESSING THE SIMPLE FIREWALL INTERFACE IN OUR PROTOTYPE

As shown inFigure 33, only one of our participants could not access the firewall with advanced security. However, the main problem regarding the access to this interface is that in the simple firewall interface, there is a tab called "Advanced" and 44% of our participants navigated this tab before noticing the link to the advanced firewall. These results show that the name of the "Advanced" tab should be changed to avoid users' confusion. Also another suggestion to improve our prototype is to put a firewall icon in the tray, so that users can access it quickly. The reason for placing the icon in tray is to first let user do other frequent interactions with the firewall through this icon more efficiently, and second to put firewall icon in a place consistent with users' mental-model (most of the other personal firewalls have an icon in the tray)

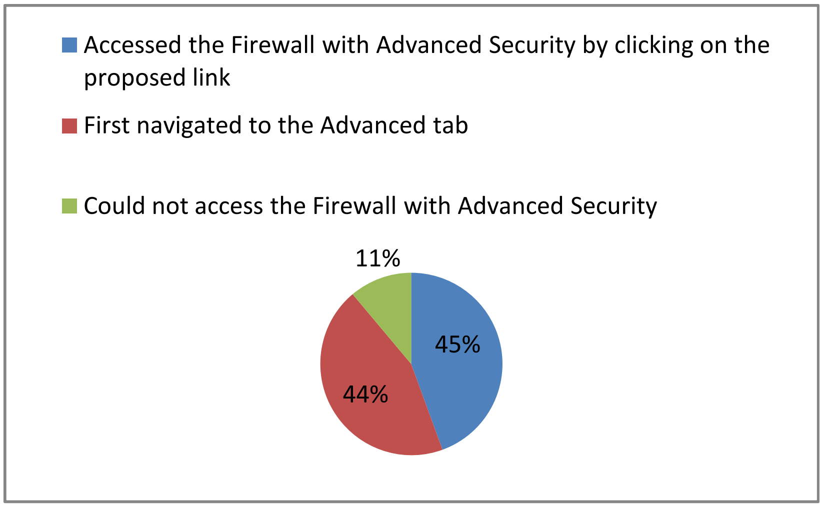


FIGURE 33: ACCESSING THE FIREWALL WITH ADVANCED SECURITY IN OUR PROTOTYPE

2. <u>Determining the Current State of the Firewall</u>: Every participant could correctly identify the current state of the firewall since it is explicitly shown in the main Window of both interfaces with two different clues. 44% (4 out of 9) of our participants noticed the green ribbon and the tick sign in it to identify secure state and the rest used the text description (Figure 34). Therefore, the user interface could successfully inform the user about the current state of the firewall.

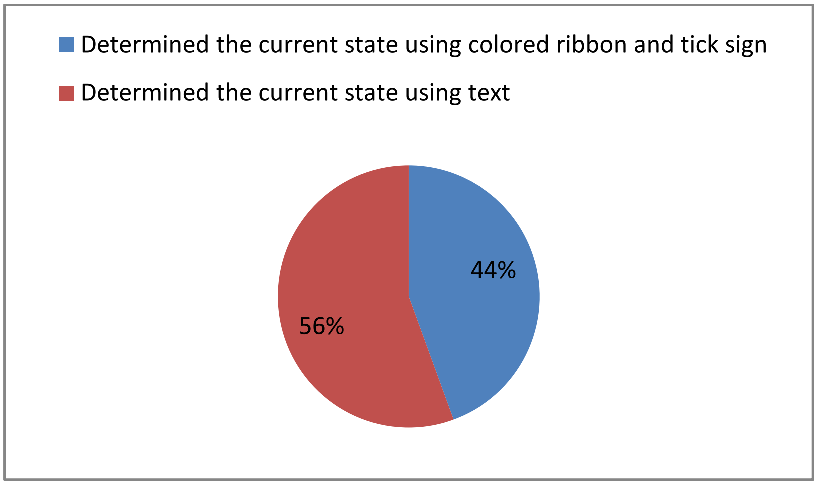


FIGURE 34: DETERMINING THE CURRENT STATE OF THE FIREWALLIN OUR PROTOTYPE

Another finding observed during this part of the study is that, the design of the link to advanced firewall in our prototype is somehow misleading. As it confused one of the participants in determining the state of the firewall (The participant said "The basic firewall is active because it is green and there is a tick mark on it but the advanced firewall is off because it is blue and there is a black icon on it").

Therefore, the design of the link to the advanced firewall should be changed, so that it does not convey information about the state of the firewall by its misleading color and icon. Also, as we suggest having a firewall icon in the tray, we can change that icon's color as well.

3. Turning the Firewall On / Off: Every participant turned the firewall off successfully. However, we noticed that 89% 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 (Figure 35). 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. Also another participant said that it looks like a link to help about turning firewall on/off.

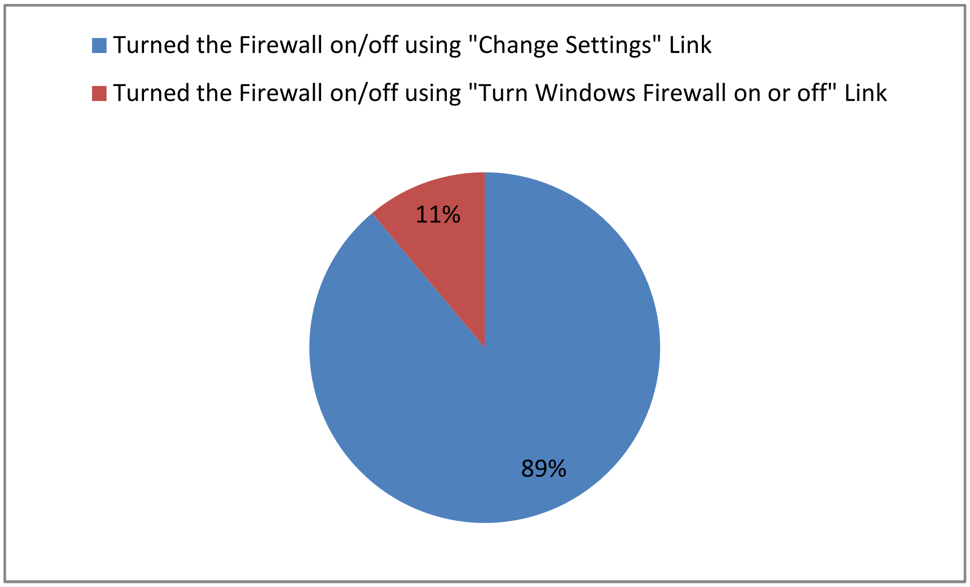


FIGURE 35: TURNING THE FIREWALL ON/OFF ON OUR PROTOTYPE

Based on the findings from this part of the study, we suggest removing the “Turn Windows Firewall on or off” link from the side bar in the firewall window to make the interface design minimal and less confusing. Also, as the result of our questionnaire shows, turning firewall on/off is the most frequent task by the users. Therefore, we suggest allowing user to turn the firewall on/off from the firewall icon in the tray without need to going through multiple steps to reach the radio-button.

4. Blocking all Incoming Connections: only 44% of the participants navigated directly to the “Exception” tab to block all incoming connections and the rest first went to the “Advanced” tab (Figure 36). The main reason behind this misunderstanding is that the users do not have a clear understanding that inbound connections that do not have an exception are blocked by default. Also, two participants mentioned that the “Exception” resembles Errors (As it indicates errors in many programming languages). Therefore we suggest changing the name of the Exception tab to more expressive term.

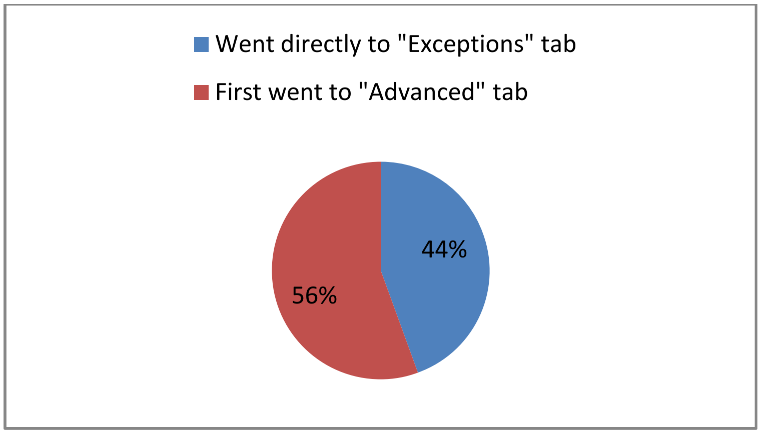


FIGURE 36: BLOCK ALL INCOMING CONNECTIONS ON OUR PROTOTYPE

5. Allowing a Specific Program through the Firewall: All of users went to Change Settings, and then Exceptions tab to allow a specific program through the firewall (The reason that users found the list of programs in exception tab is that they performed the previous task, and saw the list of programs).

6. 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 open specific port because it is in the same tab as where they unblock programs.

7. <u>Configuring an Inbound/Outbound Firewall Rule</u>: Thanks to the link to the advanced firewall in our prototype, all of our participants could successfully add a rule to the firewall. However, 44% of the participants first went to the advanced tab of the basic firewall, and 33% of them used properties button of a specific program in the Exception tab of basic interface (Figure 37). After some trial and error they went to the advanced interface and performed the task. Another interesting observation in this part of the study is that, 55% of the users try clicking on the green and red icons in the main window of the advanced interface. These icons looks like clickable buttons, therefore we suggest using some other clues to avoid misleading of the user.

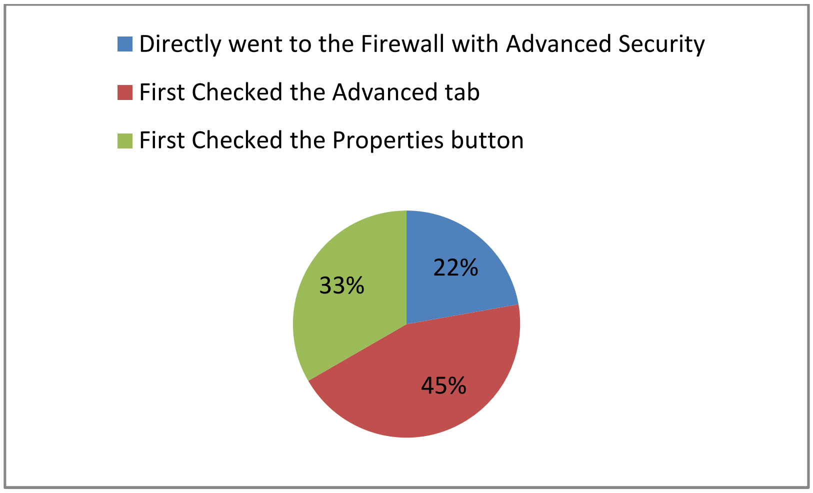


FIGURE 37: CONFIGURING AN INBOUND/OUTBOUND RULE ON OUR PROTOTYPE

8. Using Firewall's Help: Help links in our prototype leads users directly to the topic that the link name states. Therefore, our changes to the original user interface seem successful, focused on the users' task, and lead user to a parsimonious help.

9. Commenting on the names of one button and one link in the firewall interface before clicking on them – specifically the "Properties" button under the "Exception" tab in the simple firewall interface and "Show" link in the firewall with advanced security : All of our participants could correctly guess that the "Properties" button relates to a specific program. But the problem with this button is that there is no mean to change the properties of the program when this button is clicked. We suggest giving user flexibility to change some properties of the selected program.

   About changing the term "Filter" to "Show" in our prototype, 89% of the users could guess the functionality of the "Show" link. Also we showed users the original Filter link, and 67% of the users said that the filter conveys the same meaning as well. An interesting problem with our prototype is mentioned by one of the participants. The participant told us that the icon close to "Show" link is the standard icon for filter. Therefore there is an inconsistency in the prototype. For improving this problem, we suggest removing the filter icon, or even omit this change and use original "Filter" link.

4 DISCUSSIONS ON THE FINAL PROTOTYPE

Based on our results of our lab experiments and user studies, here are our summarized suggestions for the final prototype:

- Fix further terminology/icon inconsistency: Refine terms/icons so that they consistently convey accurate meanings. Many examples of these problems in the existing firewall have been listed in the preceding pages. Further, some of the changes that we proposed have had terminology problems as well: for instance, one participant thought that "Switch to Windows Vista Firewall with Advanced Security" was an ad of some sort! A careful review of all terms used in the various screens is thus necessary.

- Reduce redundant tabs in the basic firewall: The 'Advanced' tab in the basic firewall interface is usually left unused by users executing simple firewall operations; we suggest that this be made a part of the advanced interface.

- Make the advanced interface look like an extension of the basic interface: The fact that the advanced interface looks completely different from the basic interface has caused some participants to shy away from using the advanced interface. We recommend that the advanced interface be modeled to resemble the basic interface so that the user has a feeling of continuity. This may be achieved by presenting the advanced interface as a series of extended 'grayed out' tabs on the basic interface and explicitly ask the user for permission before 'un-graying' them and making them accessible to the user.

- Add a firewall icon in the system tray: This will serve as visual reminders to the user about the firewall. Further, allowing the user to turn the firewall on/off from the system tray icon, and alerting the user by blinking this icon when the firewall is turned off (this can be done upon system re-start), will be added features.

- Provide ability to change multiple rules in the advanced interface: This will help users customize their firewall quicker.

- Provide a more extensive help menu and ability to access it at various points during interaction with firewall: Providing helpful 'help balloons' at various stages and guiding users to a comprehensive help menu will increase the firewall's usability.

- Allow users to view list of programs currently using network connections: This is a feature present in Windows defender; this could be moved to the basic firewall interface as an additional tab so that users can better understand the current state of their computer.

5 CONCLUSIONS, LIMITATIONS, AND FUTURE WORK

The interface of a program is an important front end for the users to transfer their intentions to the processing engines. The interface becomes more important once the decisions made by the user may seriously change the status of the system and possibly cause dangers or threats to the confidentiality, integrity, or availability of the information stored on a machine. Windows firewalls as the gateways to the outside world are among the master pieces of applications to help users protect and secure their systems. In this paper we examined the firewall interface for Windows Vista, the most recent version of Microsoft Windows, which is still in its beta version and is undergoing changes and improvements to eventually become compliant with the needs and the requirements of the end users.

Our research basically aimed at identifying the existing problems with the interface of Windows Vista's firewall by examining the interface against globally accepted benchmarks from a Human-Computer-Interaction perspective. The suggested ideas were accompanied by a set of solutions that also were evaluated by conducting lab experiments. Our overall results show considerable improvements over the current interfaces for Windows Vista's firewall. Our results showed that a considerable amount of users were easily able to navigate to the advanced interface for Windows Vista's firewall, were less confused with the terminologies, concepts and purposes, and were more willing to interact with the firewall. However, there are some possible points of improvements in our system. For example, most of our users were able to successfully add or delete a port or a program to the firewall. This was mainly because in one of our earlier tasks we had asked the users to try and block all the incoming connections which was resided in the same tab of the simple interface as the possibility for adding or deleting a program or a port. Thus our subjects would get to realize how to perform the other task and so we had almost a 100% success rate for this task, while our earlier work had proven it somehow confusing for the users to find this without having a previous background about where those functionalities are located.

Another possible improvement to the system could be extending our model to a high fidelity prototype which appeared to be difficult to develop within our time frame for this project. A high fidelity prototype will possibly be a more realistic approach to expose the users to an interactive situation for the firewall leading to more accurate final results.

It should be taken into the consideration that Windows Vista is a product design for the public. Consequently, the final product should be accessible and usable for a diverse set of users. Our preliminary research clearly identified some of the current flaws in designing Windows Vista's firewall, and through this work we hope that we can take a step towards having a user friendly interface for the end users of Windows Vista's firewall.

REFERENCES

[1] Garfinkel, S. "Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable". PhD thesis, Massachusetts Institute of Technology, May 2005.

[2] Herzogl, A. and Shahmehri, N., "Usability and security of personal firewalls". In IFIP Security Conference, 2007.

[3] Johnston, J., Harm J., Eloff, P., and Labuschagne, L.,. "Security and human computer interfaces". Computers & Security, 22(8): 675–684, December 2003.

[4] Jones J., "Windows Vista - 90 Day Vulnerability Report". [Online] Available: http://blogs.csoonline.com/node/218

[5] McGrath, J. Methodology matters: Doing research in the behavioral and social sciences. BGBG, 152-169, 1994.

[6] The New Windows Firewall in Windows Vista and Windows Server 2008. [Online] Available: http://www.microsoft.com/technet/community/columns/cableguy/cg0106.

[7] Yee, K. "User interaction design for secure systems". In Proceedings of the International Conference on Information and Communications Security (ICICS'02), 278–290. Springer-Verlag, December 2002.

[8] Wool A., "A Quantitative Study of Firewall Configuration Errors". Computer, 37(6): 62-67, June 2004.

[9] Nielsen, J. and Molich, R., 1990. Heuristic Evaluation of User Interfaces, Proc. ACM CHI'90 Conf. (Seattle, WA, USA, 1–5 April), pp. 249–256.

[10] Herzog, A. and Shahmehri, N. 2007. User help techniques for usable security. In Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology (Cambridge, Massachusetts, March 30 - 31, 2007). CHIMIT '07. ACM, New York, NY, 11.

APPENDIX A

USABILITY OF WINDOWS VISTA FIREWALL: A LABORATORY USER STUDY

Fahimeh Raja, Robi Boeck, Pouyan Arjmandi, and Ganapathy Viswanathan

***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.**

***Index Terms*— Microsoft Windows Vista, Personal Firewall, Usability Analysis, User Study.**

INTRODUCTION

A 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.

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].

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.

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.

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).

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.

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.

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.

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.

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.

RESULTS

LABORATORY STUDY

The results obtained for each of the tasks mentioned in Section VI.B 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 blocking all incoming connections (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.

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.

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	3.5	3.5

software.		
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

TABLE 2: **SUMMARY OF USER EXPERIENCE**

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.

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.

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.

USABILITY STUDY OF VISTA'S FIREWALL USING RESPONDENT METH 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.**

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.

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.

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.

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.

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.

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.

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 38-44.

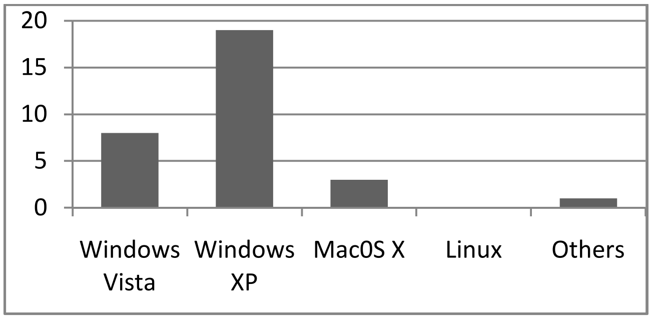


FIGURE 38: THE USAGE OF EACH OPERATING SYSTEM

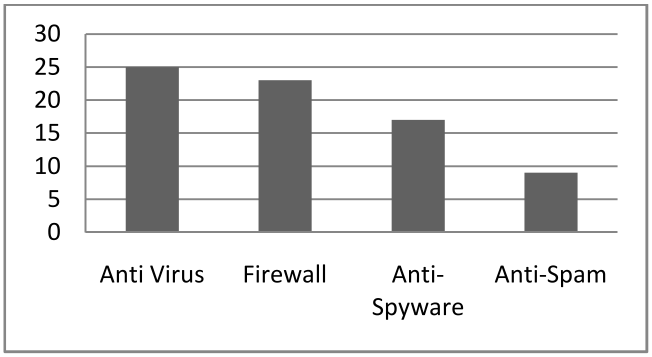


FIGURE 39: TYPE OF SECURITY SOFTWARE USED BY THE USERS

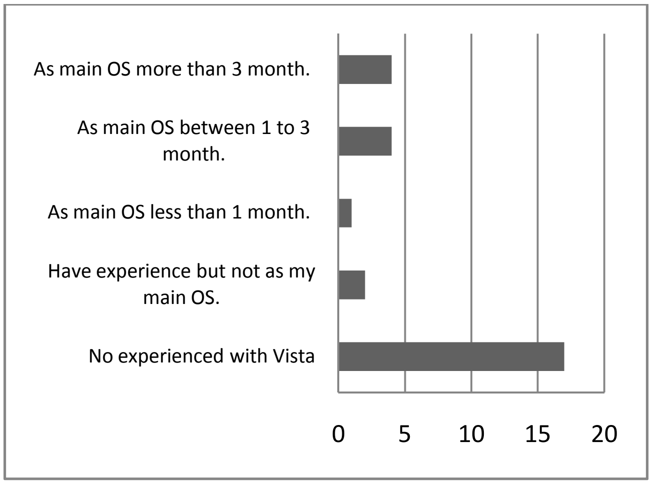


FIGURE 40: THE EXPERIENCE OF USERS WITH WINDOWS VISTA

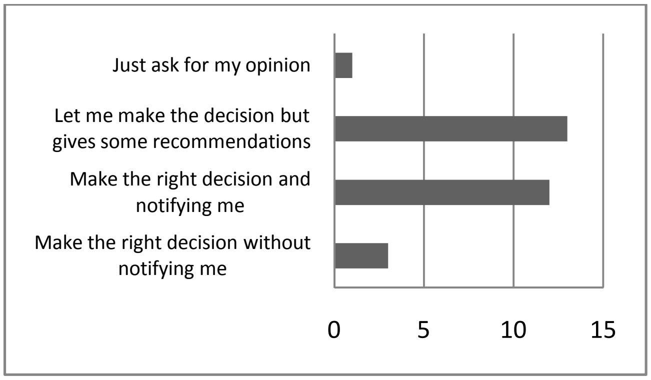


FIGURE 41: THE GENERAL PREFERENCE OF USERS ABOUT A FIREWALL'S INTERFACE

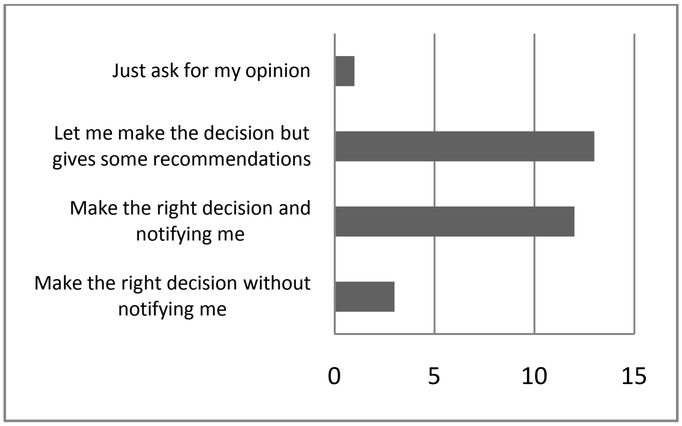


FIGURE 42: USERS PREFERENCE FOR FIREWALL NOTIFICATIONS

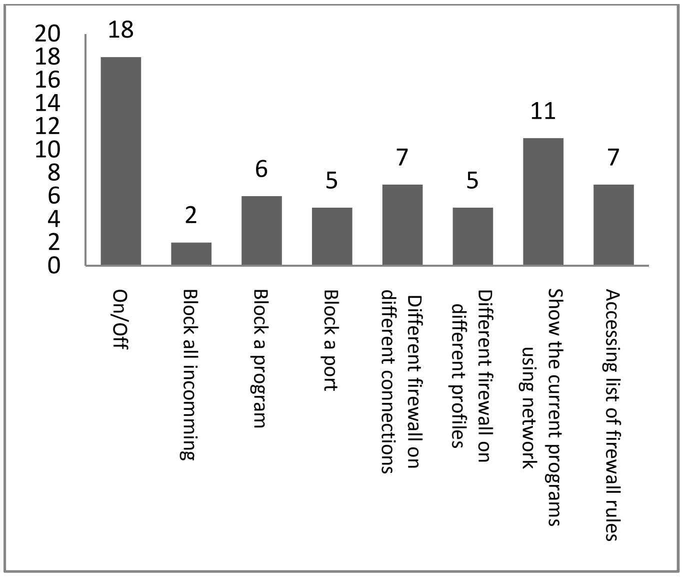


FIGURE 43: THE FUNCTIONS THAT USERS PREDICT THEY WILL USE AT LEAST ONCE IN A MONTH

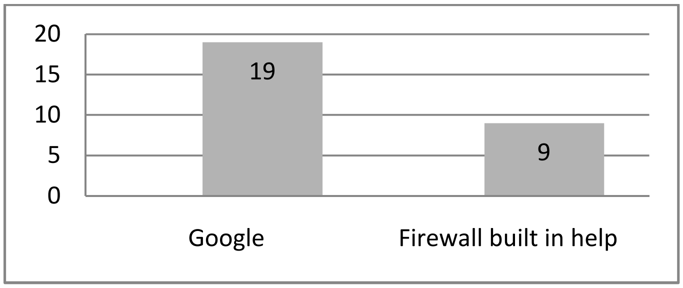


FIGURE 44: THE PREFERENCE OF USERS TO GET HELP

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.

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.

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".

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".

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.

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.

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.

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.

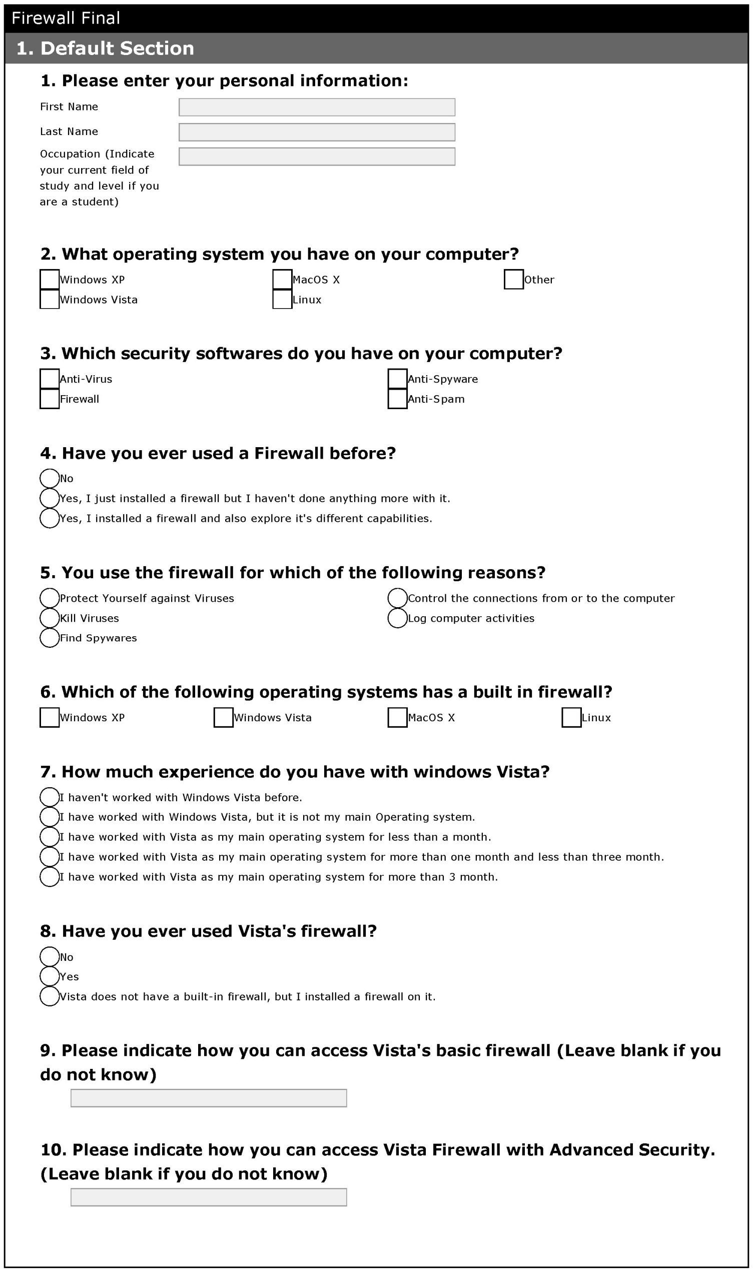
[4] N. Shahmehri, "Usability and Security of Personal Firewalls.", presented at the 22nd International Information Security Conference (IFIP TC-11), Sandton, South Africa, May 14-16, 2007.

[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.

APPENDIX C: QUESTIONNAIRE



Firewall Final

1. Default Section

1. Please enter your personal information:

First Name

Last Name

Occupation (Indicate your current field of study and level if you are a student)

2. What operating system you have on your computer?

□ Windows XP
□ Windows Vista
□ MacOS X
□ Linux
□ Other

3. Which security softwares do you have on your computer?

□ Anti-Virus
□ Firewall
□ Anti-Spyware
□ Anti-Spam

4. Have you ever used a Firewall before?

○ No
○ Yes, I just installed a firewall but I haven't done anything more with it.
○ Yes, I installed a firewall and also explore it's different capabilities.

5. You use the firewall for which of the following reasons?

○ Protect Yourself against Viruses
○ Kill Viruses
○ Find Spywares
○ Control the connections from or to the computer
○ Log computer activities

6. Which of the following operating systems has a built in firewall?

□ Windows XP
□ Windows Vista
□ MacOS X
□ Linux

7. How much experience do you have with windows Vista?

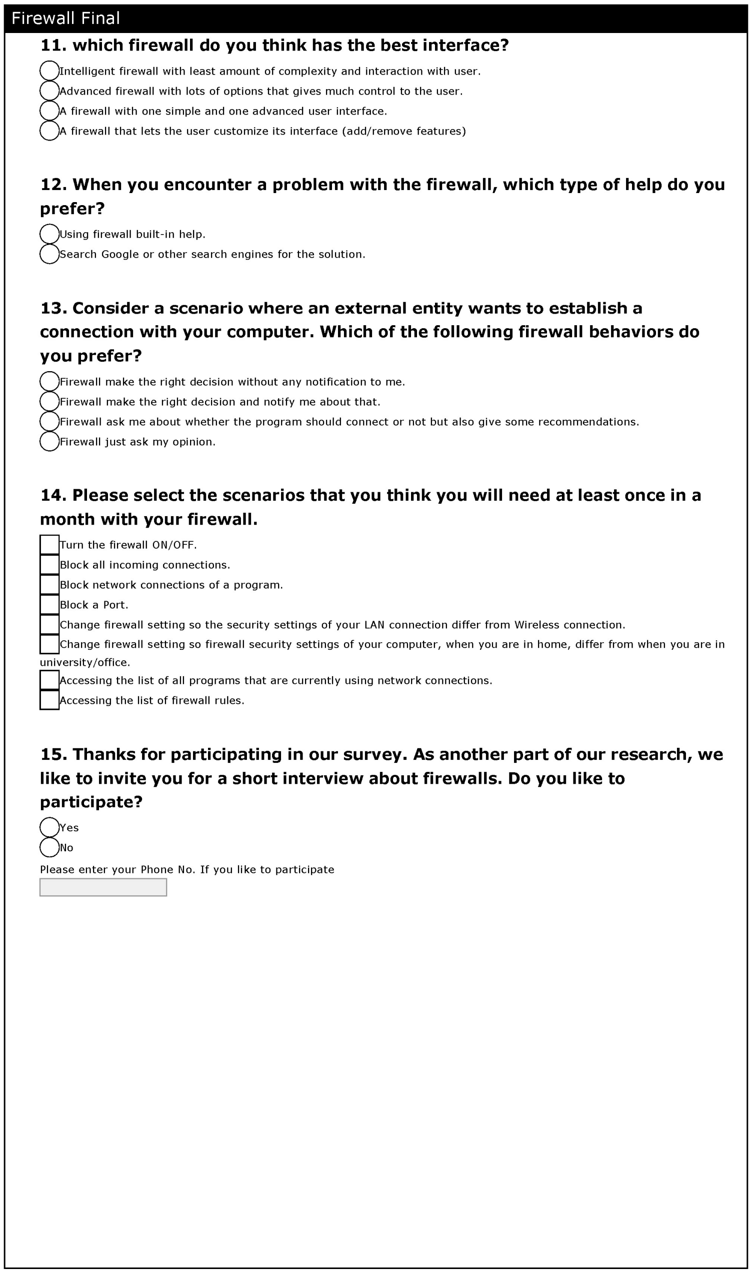
○ I haven't worked with Windows Vista before.
○ I have worked with Windows Vista, but it is not my main Operating system.
○ I have worked with Vista as my main operating system for less than a month.
○ I have worked with Vista as my main operating system for more than one month and less than three month.
○ I have worked with Vista as my main operating system for more than 3 month.

8. Have you ever used Vista's firewall?

○ No
○ Yes
○ Vista does not have a built-in firewall, but I installed a firewall on it.

9. Please indicate how you can access Vista's basic firewall (Leave blank if you do not know)

10. Please indicate how you can access Vista Firewall with Advanced Security. (Leave blank if you do not know)



Firewall Final

11. which firewall do you think has the best interface?

○ Intelligent firewall with least amount of complexity and interaction with user.
○ Advanced firewall with lots of options that gives much control to the user.
○ A firewall with one simple and one advanced user interface.
○ A firewall that lets the user customize its interface (add/remove features)

12. When you encounter a problem with the firewall, which type of help do you prefer?

○ Using firewall built-in help.
○ Search Google or other search engines for the solution.

13. Consider a scenario where an external entity wants to establish a connection with your computer. Which of the following firewall behaviors do you prefer?

○ Firewall make the right decision without any notification to me.
○ Firewall make the right decision and notify me about that.
○ Firewall ask me about whether the program should connect or not but also give some recommendations.
○ Firewall just ask my opinion.

14. Please select the scenarios that you think you will need at least once in a month with your firewall.

□ Turn the firewall ON/OFF.
□ Block all incoming connections.
□ Block network connections of a program.
□ Block a Port.
□ Change firewall setting so the security settings of your LAN connection differ from Wireless connection.
□ Change firewall setting so firewall security settings of your computer, when you are in home, differ from when you are in university/office.
□ Accessing the list of all programs that are currently using network connections.
□ Accessing the list of firewall rules.

15. Thanks for participating in our survey. As another part of our research, we like to invite you for a short interview about firewalls. Do you like to participate?

○ Yes
○ No

Please enter your Phone No. If you like to participate

APPENDIX D: CONSENT FORM

(See next page)

THE UNIVERSITY OF BRITISH COLUMBIA

Electrical and Computer Engineering
2332 Main Mall Vancouver, B.C.,
V6T 1Z4

Consent Form
Human Computer Interaction (Course Project)

Student Investigators

Arun Chebium, Pooya Jaferian, Nima Kaviani, Fahimeh Raja

Project Purpose and Procedures

This course project is designed to investigate how people interact with certain types of interactive technology. Interactive technology includes applications that run on a standard desktop or laptop computer, such as a word processor, web browser, and firewall, as well as applications on handheld technology, such as the datebook on the Pocket PC, and also applications on more novel platforms such a SmartBoard (electronic whiteboard) or a Diamond Touch tabletop display.

The purpose of this course project is to gather information that can help improve the design of interactive technology. You will be asked to use one or more forms of interactive technology to perform a number of tasks. We will observe you performing those tasks and analyze how the technology is used. You may be asked to complete a number of questionnaires and we may ask to interview you to find out your impressions of the technology. You will be asked to participate in at most 3 sessions, each lasting no more than 1 hour. The sessions may also be videotaped. Videotapes will be used for analysis and may also be used for class project presentations and other research presentations in the Department of Electrical and Computer Engineering at the University of British Columbia. You have the option not to be videotaped.

Although only a course project in its current form, this project may, at a later date, be extended by one or more of the student investigators to form the basis of his/her thesis research.

Confidentiality

The identities of all people who participate will remain anonymous and will be kept confidential. The one exception is that excerpts from the videotape may be presented as described above, and your identity may be revealed through those video excerpts. Identifiable data and videotapes will be stored securely in a locked metal filing cabinet or in a password protected computer account. All data from individual participants will be coded so that their anonymity will be protected in any reports, research papers, thesis documents, and presentations that result from this work.

Remuneration/Compensation

We are very grateful for your participation. However, you will not receive compensation of any kind for participating in this project.

Contact Information about the Project

If you have any questions or require further information about the project you may contact Professor Kellogg Booth – ksbooth@cs.ubc.ca

Contact for information about the rights of research subjects

If you have any concerns about your treatment or rights as a research subject, you may contact the Research Subject Information Line in the UBC Office of Research Services at 6048228598.

Consent

We intend for your participation in this project to be pleasant and stressfree. Your participation is entirely voluntary and you may refuse to participate or withdraw from the study at any time.

Your signature below indicates that you have received a copy of this consent form for your own records. Your signature indicates that you consent to participate in this project. You do not waive any legal rights by signing this consent form.

I, ________________________________, agree to participate in the project as outlined above. My participation in this project is voluntary and I understand that I may withdraw at any time.

Participant's Signature Date

Student Investigator's Signature Date