Towards Improving the Usability of Personal Firewalls

by

Fahimeh Raja

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

in

The Faculty of Graduate Studies

(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

January, 2011

Abstract

Even though personal firewalls are an important aspect of security for the users of personal computers, little attention has been given to their usability. An initial series of usability studies on the Windows Vista firewall that we performed revealed that the participants' lack of an accurate mental model about the firewall's system model significantly contributed to their errors when configuring the firewall. The goal of this thesis research was to build upon these findings and improve the usability of personal firewalls. To do so, we redesigned the user interface of the Vista firewall to more accurately reflect its system model. The results of a laboratory study showed that the modified interface design helped participants to develop more effective mental models of the firewall and improve their understanding of the firewall's configuration, resulted in fewer potentially dangerous errors. However, participants' comments about personal firewalls revealed that it was important to better understand the users' knowledge, expectations, perceptions, and misconceptions of personal firewalls in order to successfully manage design tradeoffs.

We performed a follow-up study, where we conducted semi-structured interviews with a diverse set of participants. Through a qualitative analysis of the data, we found that most of the participants were unaware of the functionality of firewalls and their role in protecting computers. More interestingly, we found that the interaction of most participants with firewalls was limited to responding to warnings, which ask them to allow or block a connection. Therefore, it is crucial to design firewall warnings that are understandable for users, which should result in fewer errors in allowing unwanted connections.

We proposed a novel firewall warning design in which the functionality of a personal firewall is visualized based on a physical security mental model. The results of a laboratory study showed that the new warnings facilitated the comprehension of warning information, better communicated the risk, and increased the likelihood of safe behavior compared to warnings based on those from a popular personal firewall. Moreover, the new warnings provided participants with a better understanding of both the functionality of a personal firewall and the consequences of their actions.

Preface

Versions of chapters 2, 3, and 4 of this thesis have been either published or submitted for publication. The author of this thesis performed all the users studies presented in these chapters. She also analyzed the data from those studies. She authored the corresponding papers, under the supervision of Dr. Konstantin Beznosov, Dr. Kirstie Hawkey, and Dr. Kellogg S. Booth, who provided feedback and guidance throughout the research process.

Below are the details of each chapter:

- Chapter 2: A preliminary and a full version of this chapter have been published. The author of this thesis wrote all the sections of this chapter with great help from Dr. Kirstie Hawkey.

  Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. 2009. Towards improving mental models of personal firewall users. In *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems* (CHI '09). ACM, New York, NY, USA, 4633-4638.

  Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. 2009. Revealing hidden context: improving mental models of personal firewall users. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (SOUPS '09). ACM, New York, NY, USA, 1-12.

- Chapter 3: The qualitative analysis was performed with Pooya Jaferian. A preliminary and a full version of this chapter have been published. The author of this thesis wrote all the sections of this chapter.

  Fahimeh Raja, Kirstie Hawkey, Konstantin Beznosov, and Kellogg S. Booth. 2010. Investigating an appropriate design for personal firewalls. In *Proceedings of the 28th International Conference Extended Abstracts on Human Factors in Computing Systems* (CHI EA '10). ACM, New York, NY, USA, 4123-4128.

Fahimeh Raja, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, and Kellogg S. Booth. 2010. It's too complicated, so I turned it off!: expectations, perceptions, and misconceptions of personal firewalls. In *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration* (SafeConfig '10). ACM, New York, NY, USA, 53-62.

- Chapter 4: Steven Hsu and Clement Wang helped the author to perform the study and analyze the data. A short version of this chapter has been submitted for publication. The author of this thesis wrote all the sections of this chapter.

  Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Clement Wang, and Konstantin Beznosov. 2011. Promoting A Physical Security Mental Model for Personal Firewall Warnings. Submitted for publication.

The research presented in this thesis was approved by the Behavioral Research Ethics Board of the University of British Columbia and its certificate number is H08-01150.

Contents

Appendices

List of Tables

List of Figures

Acknowledgements

First, I offer my gratitude to my supervisor, Dr. Konstantin Beznosov, who has supported me throughout my research.

Special thanks to Dr. Kellogg Booth for his support and helpful insights on my research, and to Dr. Kirstie Hawkey for her mentorship since the initial stages of my research.

Thanks to Dr. Robert Schober who kindly accepted to be on my committee.

I would like to thank my friends at the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who provided me with constructive feedback in all phases of my research.

I would also like to send my thanks to my dear family in Iran; my dad who always supported me and encouraged me to work harder; my mom whose love is unique and my greatest wish is to see her healthy again; Nafiseh, my kind sister; Farzad, my older brother, and his family. I've been away from them for a long time, but they always have had a special place in my heart for their unconditional love.

Last, but certainly not least, my perfect husband, who endured me throughout my research. He encouraged me in an extraordinary way with his passion for perfection. He is one of a kind, and I am super lucky to have him as my husband forever.

To Zahra Kardanpour and Ali Raja, my dear parents,

and

Pooya Mohseni, love of my life.

Chapter 1

Introduction

The term *firewall* has been in use since 1764. It was first used to refer to fireproof walls that "separate the parts of a building most likely to have a fire from the rest of a structure" (Ingham and Forrest, 2002, p. 2). Later uses refer to iron-walls in steam locomotives that separate the engine compartment from the other parts of the locomotive. The purpose of these walls was to prevent the spread of fire (Ingham and Forrest, 2002). In the world of computers, firewalls provide a similar functionality. A computer firewall is a piece of hardware or software that is designed to block the spread of unwanted network traffic; as defined by Oppliger (Oppliger, 1997):

> *A firewall builds a blockade between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted. The general reasoning behind firewall usage is that without a firewall, a network's systems are more exposed to inherently insecure Internet protocols and corresponding services, as well as probes and attacks from hosts elsewhere on the Internet.* (Oppliger, 1997, p. 94).

Computer firewall technology was first introduced in the late 1980s (Avolio, 1999). Before that the Internet was used by a small community who thought that the openness of the Internet was advantageous for sharing and collaboration. However, what happened on November 2, 1988, changed the Internet forever. On that day, Peter Yee at the NASA Ames Research Center sent a message to the TCP/IP Internet mailing list and reported that, "We are currently under attack from an Internet VIRUS! It has hit Berkeley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames" (Avolio, 1999, p. 25). This message was the first documentation of what infected around 6,000 major computers and later called the Morris Worm (Eichin and Rochlis, 1989). This incident and similar incidents after that signaled "the end of an open and benign Internet," and were the beginning of the rapid evolution of firewall technology (Ingham and Forrest, 2002; Avolio, 1999).

The first generation of firewalls[1] was used in the early 1990s (Avolio, 1999). Since then firewalls have matured substantially and now *personal firewalls* are a built-in part of mainstream operating systems. A personal firewall is a software firewall that checks the traffic flowing between a *personal computer* and the network(s). Based on its configuration, the firewall allows or blocks elements of traffic.

With the increasingly growing use of pervasive, persistent, and high-bandwidth connections to the Internet, personal firewalls are becoming commonplace and are recognized as "the first line of defense" for personal computers (McDermott, 2000; Johnston et al., 2003; Xia and Brustoloni, 2004; Stoll et al., 2008). With these always-on Internet connections, personal computers become a target for malicious applications and hackers who not only can steal users' confidential and private information, but also can use their computer resources for denial of service or spam attacks (Goecks et al., 2009; Hole et al., 2005; Xia and Brustoloni, 2004). Therefore, personal firewalls can play an important role in defense against these threats by controlling the traffic flowing between personal computers and the network(s). However, the protection provided by them depends strongly on their correct configuration (Herzog and Shahmehri, 2007; Ecclestone, 2001; Bishop, 2003).

Personal firewalls are intended to be used by home users of computers. They should make decisions about which applications are allowed to connect to, and send and receive data from the network. However, these users are not necessarily security experts (Cranor, 2005). These users are typically computer security illiterate. Therefore, usability of personal firewalls is key to their correct configuration, and thus, their effective protection. However, there has been little work on the usability of personal firewalls; the improvements to firewall technology have been mostly about effectiveness and efficiency rather than usability. The goal of this thesis research is to mitigate this gap. We focus on the *usability* of personal firewalls.

In the rest of this chapter, we provide an overview of our research on the usability of personal firewalls in Section 1.1, followed by a summary of our contributions in Section 1.2. Section 1.3 presents related work on the usability of firewalls. Finally, Section 1.4 outlines the structure of this thesis.

[1] The first generation of firewalls were called packet filters. These firewalls functioned by inspecting each individual packet to see whether it matched the firewall's set of rules. Unlike today's firewalls, packet filters did not store any information about the connection; they did not check if a packet was part of an existing traffic flow, and therefore, they were slower than current firewalls.

1.1 Overview

We began our usability studies of personal firewalls by evaluating the Microsoft Windows Vista firewall. In Windows Vista, the first time a user connects to a network, he must classify it as Home, Work, or Public. The Vista firewall defines three "Network Locations" that correspond to three configuration profiles: Private (applied to Home and Work networks), Public (applied to Public networks), and Domain (applied if the network administrator has specified domain settings). Which profile is automatically applied depends on which network location was selected for the detected network. Such active context-aware computing may help calm the technology by shifting complexity and actions to the system (Chen and Kotz, 2000). However, concealing the impact of network context on the security state of the firewall may result in users developing an incorrect mental model of the protection provided by the firewall. To investigate this issue, we performed a user study with a diverse set of 60 participants.

We examined participants' mental models of firewalls, as well as how the Vista firewall's user interface and our prototype interface support those mental models and participants' understandings of the firewall configuration. Our prototype was designed to more accurately project the firewall's system model through a more explicit representation of the network context and its impact on the firewall's security state.The results of a laboratory study showed that participants produced richer mental models of the firewall after using the prototype than when working with the Vista firewall interface; they were also significantly more accurate in their understanding of the configuration of the firewall. Interestingly, 65% of the participants did not see the benefits of maintaining multiple profiles for different contexts of use. We realized that it was important to gain a deep understanding of users' knowledge, requirements, perceptions, and misconceptions of personal firewalls. Therefore, we performed a followup study.

We conducted semi-structured interviews with a diverse set of 30 participants. Our qualitative analysis of the data revealed that participants with different levels of security knowledge have different understandings about the functionality of a personal firewall. Most participants were not aware of the benefits of the protection provided by a personal firewall; they were not even aware of the existence of a personal firewall on their computers. Our results also showed that context was important for several participants when making security decisions. We found different contextual factors that were important to those participants; however, we also found that they may not have the necessary knowledge to determine the required level of security based on the contextual factors.

One important finding of our interviews was that the interaction of most of our participants with personal firewalls was limited to responding to warnings that ask them about allowing or blocking a connection. However, many of the participants had problems understanding and making informed decisions about these warnings. As a result, they tended to ignore the warnings or even turn their personal firewall off or completely uninstall it. Based on the findings of our first user study, we understood that the design of firewall warnings plays a crucial role in the users' correct response to them. Therefore, we focused on firewall warnings, and proposed a novel interface design for them.

We used an iterative process in the design of firewall warnings in which the functionality of a personal firewall is visualized based on a physical security mental model and the metaphor of a firewall. We performed a study to determine the degree to which our proposed warnings are understandable for our participants, and the degree to which they convey the risks and encourage safe behavior. We compared our warnings with warnings based on those from a popular personal firewall. Our results showed that our proposed warnings facilitated the comprehension of warning information; they helped participants develop a better mental model of the functionality of a personal firewall. They also better communicated the risk; with our warnings, participants had a better estimation of the level of hazard, likelihood of damage or loss, and the severity of potential damage or loss. They could also better describe the potential consequences of their intended actions. More importantly, our warnings increased the likelihood of their safe behavior in response to the warnings. They were also preferred by the majority of our participants.

1.2 Contributions

Here we provide a summary of our contributions for each of the three user studies we performed.

- **Usability Studies of Windows Vista Personal Firewall**: Our usability studies of the Vista firewall makes an important contribution as it highlights the dangers of hidden complexities in security software. Our results showed that a root cause of users' errors in their firewall configuration is the lack of an accurate mental model about the firewall's system model. Another contribution of this part of our research is the design and evaluation of a new interface for the Vista firewall, which more accurately reflects its system model. The results of our evaluation revealed that good interface design plays a crucial role in providing users with an effective mental model of their security applications, resulting in fewer potentially dangerous errors in their security configuration.

- **Expectations, Perceptions, and Misconceptions of Personal Firewalls**: The first contribution of this study is our analysis, which provides an understanding of users' knowledge, expectations, perceptions, and misconceptions of personal firewalls. The second contribution is the examination of the implications of our findings for the design of personal firewalls. We also provide recommendations for designing more usable and effective personal firewalls, warnings and notices.

- **A Physical Security Mental Model For Personal Firewall Warnings**: The most important contribution of this part of our research is the proposal of a novel design for personal firewall warnings. This design is based on the users' mental model of firewalls, i.e., physical security. Another contribution is the evaluation of our proposed warnings, which reveals that our warnings facilitate the comprehension of warning information, better communicate the risk, and increase the likelihood of safe behavior. These findings support that our approach is promising for improving the design of security warnings.

It should be noted that the variability of our participants with respect to age, gender, educational level, background, and security knowledge and expertise is a major strength of all of our three user studies.

1.3 Related Work[2]

Prior research has considered the usability of personal firewalls. Johnston et al. (Johnston et al., 2003) performed a heuristic evaluation of the Windows XP personal firewall and proposed improvements for its interface, such as the visibility of the firewall features and status, and the learnability of the interface. They believed that their recommendations increase the users' trust to their firewalls.

Berson (Berson, 2005) described design principles used by ZoneAlarm labs to create personal firewalls that are usable for consumers. He emphasized the human-centered design of security products, and provided guidelines to increase the usability of security products, including personal firewalls. He recommended that the designers of security products know the audience of their products and speak their language, think like the audience, eliminate clutter, eliminate complexity, create just enough feedback, and be a customer advocate.

[2] Prior work related to each of the three user studies that we performed is presented in the corresponding chapters.

Herzog and Shahmehri (Herzog and Shahmehri, 2007) performed a usability study of 13 personal firewalls that were the most popular personal firewalls for Microsoft Windows XP[3]. They compared the granularity of rules and the usability of rule setup for these firewalls. They defined use and misuse cases and performed a cognitive walk through to examine the behavior of the firewalls for these scenarios. Their results highlighted the need to convey the firewall design model and default settings to users.

Another body of work has investigated the usability of firewalls for administrators and organizations. Geng et al. (Geng et al., 2005) considered the difficulty of defining firewall rules to enforce an expected security policy correctly, and of understanding these rules to make necessary changes. They proposed an interactive interface that combines simulation, visualization, and interaction to help system administrators understand and update firewall configurations. Wool (Wool, 2004) critiqued usability problems of enterprise firewalls that stemmed from a mismatch between the users' natural definition of network traffic *direction* and that of a firewall's. A firewall treats the traffic from the computer to the network as outbound, whereas most users would consider it as inbound.

Although the above-mentioned studies informed our usability studies of personal firewalls, all of them are based on evaluation by experts; they lack studies with target users of those firewalls to validate their findings. Hazari (Hazari, 2005) performed an exploratory study to investigate users' perceptions of factors that could affect the selection of a personal firewall in an organization. His Q-sort[4] analysis showed that ease-of-use is of high priority for users, but he did not describe what users meant by ease-of-use. Moreover, the study was performed with students from a graduate business management security course who all had a hands-on firewall assignment including installation, configuration, and use of a commercial personal firewall. This would not be a good sample for getting end-users' perceptions of personal firewalls because average users of computers rarely have this much security training.

Stoll et al. (Stoll et al., 2008) used a spatial extension of the desktop metaphor to visually show system-level information for a personal firewall-like tool. Their goal was to present technical information in an understandable way so that non-expert users can make informed decisions. They performed a controlled experiment to evaluate the usability of their proposed approach. Their results showed that their interface facilitates users' security decision making, and helps to motivate them to interact with their security software.

[3] According to http://www.firewallguide.com

[4] A ranking of variables according to some condition of instruction (Beck, 1962).

1.4 Outline

The remainder of this thesis is organized as follows. Chapters 2, 3, and 4 present our three user studies. They all have a similar structure:

- Introduction that motivates and summarizes the corresponding study;
- Related Work that presents prior work related to that study;
- Methodology that explains the study design and protocol, participant recruitment and their demographics;
- Results that describes the main findings of the study;
- Discussion that elaborates on interpretations of the results, and where possible, recommendations for improving personal firewalls and security applications; and
- Conclusions that summarizes the findings.

Chapter 5 summarizes the contributions of this thesis, and introduces directions for future research.

Chapter 2

Usability Studies of Windows Vista Personal Firewall[5]

In Windows Vista with 180 million licenses as of August, 2008 (Microsoft, 2008a), Microsoft introduced a built-in personal firewall that provides a basic user interface (which we call VF-Basic) for home users of Windows Vista and an advanced one (which we call VF-Advanced) for IT professionals (Microsoft, 2008b). This firewall incorporates the context of network location (a change from the Windows XP personal firewall) and connection types. In VF-Advanced, a user can configure the firewall for three different network locations; however, in VF-Basic, changes are applied only to the current network location, which is automatically detected by the firewall. Such active context-aware computing may help calm the technology by shifting complexity and actions to the system (Chen and Kotz, 2000). However, concealing the impact of network context on the security state of the firewall may result in users developing an incorrect mental model of the firewall. As defined by Card and Moran (Card and Moran, 1986), a user's mental model is:

> *An abstraction of system's architecture and software structures that is simple enough for non-technical users to grasp. . . It provides an integrated package of knowledge that allows the user to predict what the system will do if certain commands are executed, to predict the state of the system after the commands have been executed, to plan methods for novel tasks, and to deal with odd error situations (Card and Moran, 1986, p. 191).*

[5] A preliminary and a full version of this chapter have been published.

- Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. 2009. Towards improving mental models of personal firewall users. In *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems* (CHI '09). ACM, New York, NY, USA, 4633-4638.
- Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. 2009. Revealing hidden context: improving mental models of personal firewall users. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (SOUPS '09). ACM, New York, NY, USA, 1-12.

A key to usable security is mitigating the gap between what a system does and the mental models that users have of its functionality (Smith, 2003; Yee, 2004). One approach is to simplify the underlying system model, but this is often infeasible for complex security applications. Therefore, a security interface must establish common ground between users and the system's security features (Johnston et al., 2003). While an effective mental model does not need to include all the system details, it does need to be functional and allow the user to predict the consequences of his actions (Chiasson et al., 2007). Concealing system details as a means of reducing complexity may leave users unable to respond to unexpected system events (Dourish et al., 2004); enough technical details must be provided so that users can make informed decisions as they interact with security tools (de Paula et al., 2005).

In this chapter, we present a study, which examines participants' mental models of firewalls, as well as how VF-Basic and our prototype interface support those mental models and participants' understanding of their firewall configuration. Our prototype interface was designed to more accurately reflect the firewall's system model by providing a more explicit representation of the network context in Windows Vista and its impact on the firewall's security state. We found that including this contextual information improved participants' mental models of the firewall and their understanding of the firewall configuration, resulting in fewer dangerous errors about the security state of the firewall.

In the rest of this chapter, we first present prior work related to this part of our research, and a brief background on the functionality and interface of the Windows Vista personal firewall. We then describe our prototype interface design, followed by our methodology for evaluating both VF-Basic and our prototype interface. Finally, we present our results and a discussion of our findings.

2.1 Related Work

The issue of overly complex systems impacts security and non-security applications alike. One approach is to present different information and configuration options to novice and more experienced users. Multiple interface design allows presentation of the most common configuration options in a simple interface to reduce the complexity for novice users (McGrenere et al., 2002). Whitten and Tygar (Whitten and Tygar, 2003) introduced the concept of safe staging for security interfaces to safely reduce immediate complexity for novice users. Cranor (Cranor, 2003) proposed layered interfaces as one solution to the challenges security interface designers face in presenting configuration options.

Another common approach is to provide users with enhanced feedback about the system state. Providing visibility of the current security state is one of Yee's (Yee, 2002) secure interaction design guidelines. Chiasson et al.'s (Chiasson et al., 2007) principles for designing security applications for administrators include providing feedback to accurately determine the current state of the system. Providing visualizations of system activity and integrating configuration and action have been proposed to help users assess whether a system is secure enough for their immediate needs (Rode et al., 2006).

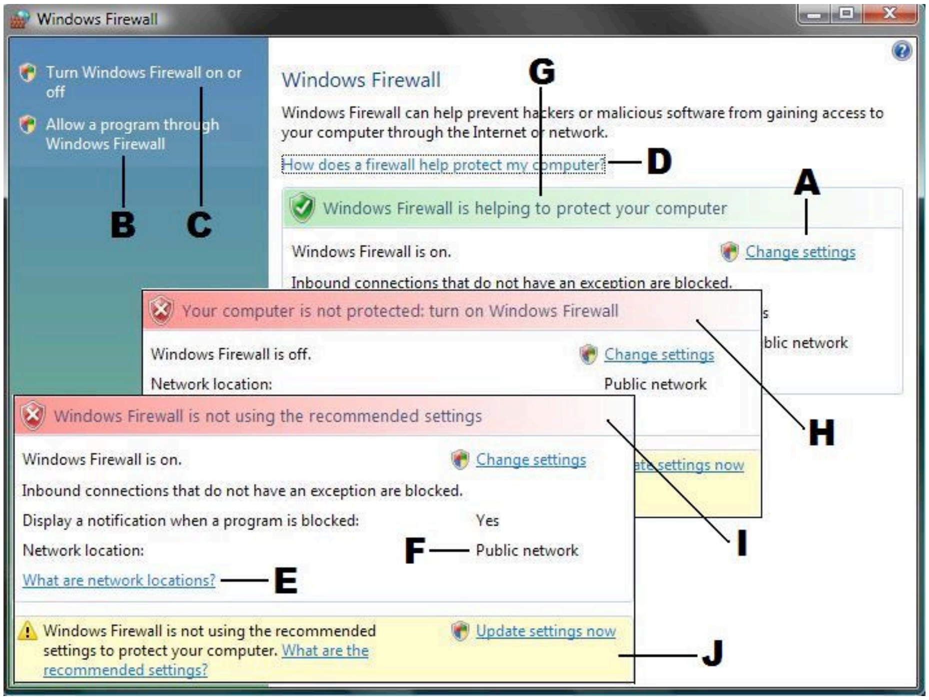
Reducing complexity through adaptivity is another approach. An active context-aware application automatically adapts to discovered context by changing its behavior, reducing the need for user actions (Chen and Kotz, 2000). The Vista firewall provides different interfaces for expert and non-expert users; it also applies adaptivity to network context in its simple interface. However, in this study we show that the system's inner complexity should not be hidden for the sake of interface simplicity if the user is then left with an ineffective mental model. This is particularly important for security interfaces in order to avoid dangerous errors.

2.2 Windows Vista Personal Firewall

In this section, we first provide background about the Vista firewall and its basic interface. Then, we briefly describe the usability issues we found in our preliminary usability studies of the Vista firewall.

2.2.1 Interface and Underlying Functionality

In Windows Vista, the first time a user connects to a network, he must classify it as Home, Work, or Public (Microsoft, 2008c). The Vista firewall defines three "network locations" that correspond to three configuration profiles: Private (applied to Home and Work networks), Public (applied to Public networks), and Domain (applied if the network administrator has specified domain settings). Which profile is *automatically* applied depends on which network location was selected for the detected network. For each network location, the user can also enable or disable the firewall for three types of connections: Wireless, Local Area Connection, and Bluetooth; this results in nine network contexts. When a user configures the firewall through VF-Basic, the changes are applied to the *current* firewall profile (Public or Private) and used in future for every network with the same network location (as long as the firewall is enabled for that connection type).


Windows Firewall

Turn Windows Firewall on or off

Allow a program through Windows Firewall

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.

Your computer is not protected: turn on Windows Firewall

Windows Firewall is off. Change settings

Network location: Public network

Windows Firewall is not using the recommended settings

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

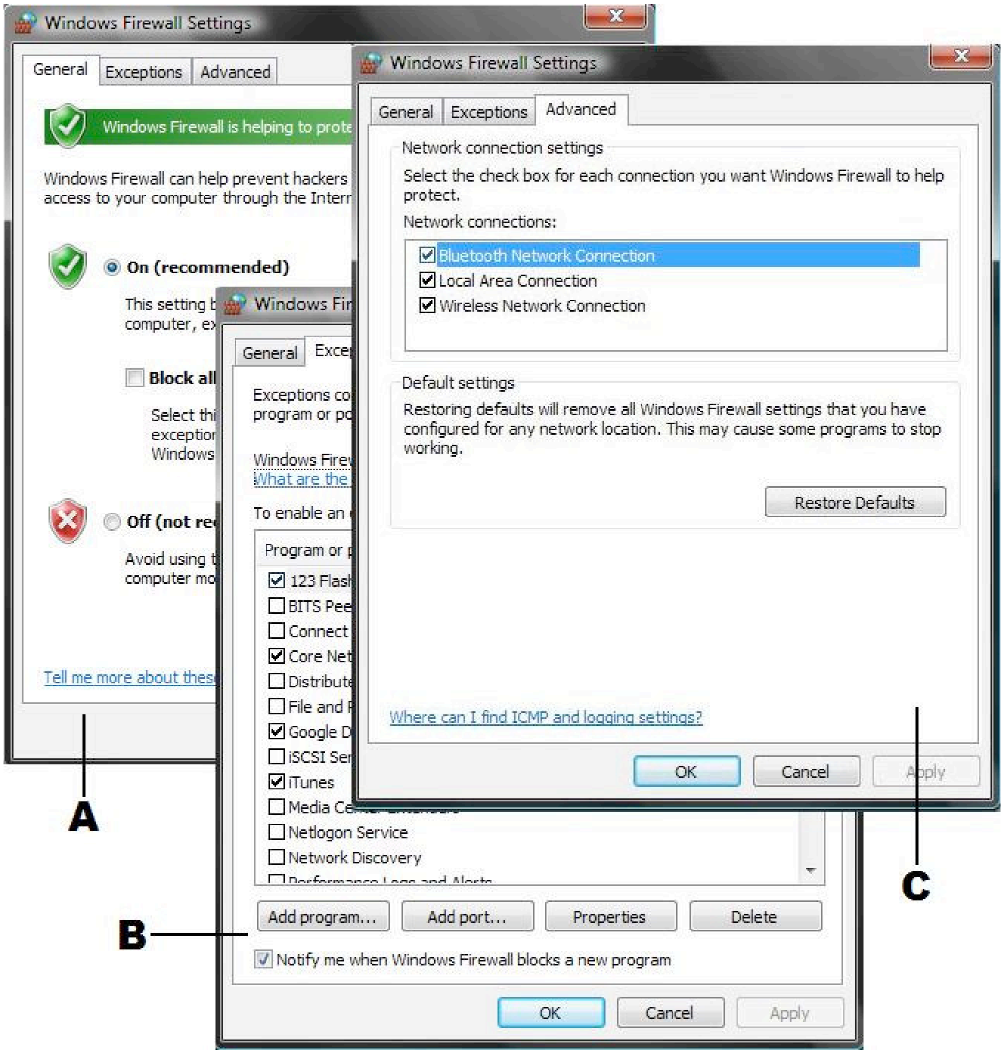
What are network locations?

Windows Firewall is not using the recommended settings to protect your computer. What are the recommended settings? Update settings now

Figure 2.1: Main window of VF-Basic, with two inset panels showing different security configurations.

The main window of VF-Basic has three links to change its settings (A, B, C in Figure 2.1) and help links about how the firewall works (Figure 2.1D) and what the network locations are (Figure 2.1E). It also provides the current network location (Figure 2.1F) and the security state of the firewall. There are three possible security states: 1) the firewall is on (protecting the computer) for all the network locations and network connections, using the *recommended settings* (Figure 2.1G); 2) the firewall is off for the current network location, (e.g., Public in Figure 2.1H); and 3) the firewall is on for the current network location, but it is not on for all the network locations and connections (Figure 2.1I). In the last two cases a yellow bar is displayed (Figure 2.1J), which says the firewall is not using the recommended settings and gives the “Update settings now” link to apply them and a link to an FAQ.

When a user clicks on a link to change the firewall settings, a second window with three tabs is displayed (Figure 2.2). In the “General” tab (Figure 2.2A), the user can turn the firewall on or off. When he turns the firewall on, he also has the option to block all incoming connections. In the “Exceptions” tab (Figure 2.2B), the user can set exceptions of programs and ports for which inbound connections are allowed. In the “Advanced” tab (Figure 2.2C), the user can enable or disable the firewall for different network connections and restore the default settings of the firewall (note: the Advanced tab in VF-Basic is not same as the VF-Advanced).



Windows Firewall is helping to prote

Windows Firewall can help prevent hackers access to your computer through the Intern

● On (recommended)

This setting b computer, ex

☐ Block all

Select thi exception Windows

○ Off (not re

Avoid using t computer mo

Tell me more about thes

Exceptions co program or po

Windows Firew
What are the

To enable an

Program or p

☑ 123 Flash
☐ BITS Pee
☐ Connect
☑ Core Net
☐ Distribut
☐ File and F
☑ Google D
☐ iSCSI Ser
☑ iTunes
☐ Media Ce
☐ Netlogon Service
☐ Network Discovery
☐ Performance Logs and Alerts

☑ Notify me when Windows Firewall blocks a new program

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
☑ 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.

Where can I find ICMP and logging settings?

Figure 2.2: Tabs in the second window of VF-Basic: A. General, B. Exceptions, C. Advanced.

2.2.2 Initial Analysis of Usability Issues

The research we present in this chapter builds upon three course projects, which investigated the usability of the Vista firewall. A heuristic evaluation (Jaferian, 2008) and a lab experiment with 12 participants (Arjmandi et al., 2007) identified several usability problems; we focus on two of these problems. First, VF-Basic has very limited functionalities; it does not support common user tasks, such as defining exceptions for *outgoing* connections. Second, the location of VF-Advanced, which contains the remaining functionality, is not obvious to users and is not consistent with the location of other Windows Vista security applications. Moreover, there are no explicit links between the two interfaces so that users can easily switch between them.

A third study (lab experiment) evaluated a medium fidelity prototype for the Vista firewall in which a link was provided between the two interfaces (Chebium et al., 2008). The results showed that the participants (9) were able to find the required features more easily as they performed their tasks; however, they felt VF-Basic should include more of the functionality that they frequently used. This study also revealed that VF-Basic does not provide the necessary contextual information (network location and connection) for the functionalities that it does support. In VF-Advanced a user can configure the firewall for each network location; however, in VF-Basic, configuration changes are only applied to the current network location and this is not obvious.

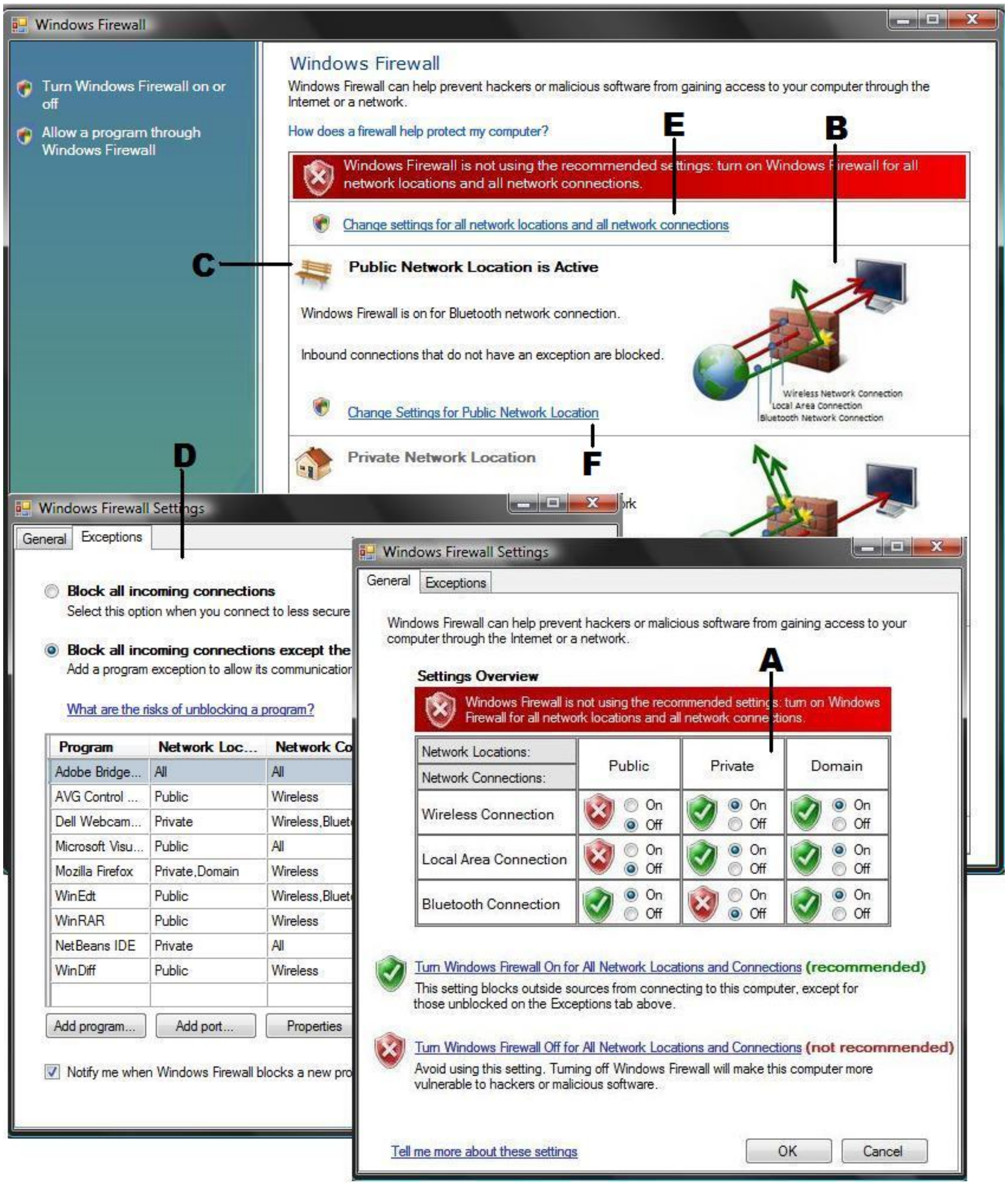
This prior work motivated our prototype interface design, which we present next. The Vista firewall provides a multi-layer interface, but VF-Basic has insufficient contextual information and configuration options. We propose providing the contextual information in all the firewall interfaces to avoid inconsistencies between users' mental models and how the firewall works.

2.3 Prototype Interface Design

To evaluate whether inclusion of the contextual information in VF-Basic can help users develop a richer mental model of the Vista firewall's system model, we designed a prototype for an enhanced basic interface. To isolate the effect of our changes, we designed the prototype interface to mimic Vista's design, using its colors, images, text, and terminology. We used elements from VF-advanced to incorporate network context. It should be noted that we incorporated only the network context information and did not include all the functionalities of VF-Advanced, such as IPSec configuration and monitoring security associations (VF-Adanced is shown in Appendix A).

Our prototype interface provides a visualization of the two context parameters that have an effect on the security state of the firewall: network location and connection. We also provided the option to set the firewall for different network locations; and, in each network location, the opportunity to configure it for different network connections. This way, a user can understand the security state of the firewall in all the possible network contexts without having to leave the basic interface.

We iteratively refined our prototype interface with 13 pilot testers who performed the study tasks. As we applied their feedback to our design, we consulted them to ensure that the changes made addressed their concerns.



Windows Firewall

Turn Windows Firewall on or off

Allow a program through Windows Firewall

Windows Firewall

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

How does a firewall help protect my computer?

Windows Firewall is not using the recommended settings: turn on Windows Firewall for all network locations and all network connections.

Change settings for all network locations and all network connections

Public Network Location is Active

Windows Firewall is on for Bluetooth network connection.

Inbound connections that do not have an exception are blocked.

Change Settings for Public Network Location

Private Network Location

Windows Firewall Settings

General | Exceptions

○ Block all incoming connections
Select this option when you connect to less secure

● Block all incoming connections except the
Add a program exception to allow its communication

What are the risks of unblocking a program?

Program	Network Loc...	Network Co
Adobe Bridge...	All	All
AVG Control ...	Public	Wireless
Dell Webcam...	Private	Wireless,Bluet
Microsoft Visu...	Public	All
Mozilla Firefox	Private,Domain	Wireless
WinEdt	Public	Wireless,Bluet
WinRAR	Public	Wireless
NetBeans IDE	Private	All
WinDiff	Public	Wireless

Add program... | Add port... | Properties

☑ Notify me when Windows Firewall blocks a new pro

Windows Firewall Settings

General | Exceptions

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

Settings Overview

Windows Firewall is not using the recommended settings: turn on Windows Firewall for all network locations and all network connections.

Network Locations: Network Connections:	Public	Private	Domain
Wireless Connection	✗ ○ On ● Off	✓ ● On ○ Off	✓ ● On ○ Off
Local Area Connection	✗ ○ On ● Off	✓ ● On ○ Off	✓ ● On ○ Off
Bluetooth Connection	✓ ● On ○ Off	✗ ○ On ● Off	✓ ● On ○ Off

✓ Turn Windows Firewall On for All Network Locations and Connections (recommended)
This setting blocks outside sources from connecting to this computer, except for those unblocked on the Exceptions tab above.

✗ Turn Windows Firewall Off for All Network Locations and Connections (not recommended)
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings

OK | Cancel

Figure 2.3: Prototype interface. Main window with dynamic configuration image (B) and enhanced context (C). Secondary window: General tab with configuration table (A), Exception tab with enhanced context (D).

Our final prototype provides the configuration table (Figure 2.3A) recommended by three early pilot testers and a dynamically updated image (Figure 2.3B, modified from one in Vista firewall's help (Microsoft, 2008d)) to help users visualize different contexts for the Vista firewall and its security state in each context. This image includes the security state of the network connections for each network location. Each connection is shown with an arrow: a green arrow indicates that the firewall is on for that connection and the connection is protected, while a red arrow means that the connection is not protected. We included icons from the "Customize Network Settings" window of Windows Vista (Figure 2.3C) to help users distinguish the different network locations (e.g., a bench for Public).

In the "General" tab of our secondary window, we included the *configuration table* (Figure 2.3A) mentioned above. This reveals all the possible combinations of the network locations and connections and allows users to turn the firewall on or off for each network context. This integration of configuration of the firewall with information about the firewall state is supported by design principles for security systems (Rode et al., 2006; Reeder et al., 2008; Stoll et al., 2008). In the "Exceptions" tab (Figure 2.3D), we included information about network location and connection. We gave users the option to choose the network location and connection for each exception rule. As the ability to enable/disable the firewall for different network connections was incorporated throughout our prototype, we no longer required an "Advanced" tab.

It is important to note that the underlying operation of the firewall did not change between VF-Basic and the prototype interface; the prototype interface merely explicitly revealed the effect of the network location and connection context on the firewall settings.

2.4 Methodology

Our prototype interface was designed to provide users with the contextual information needed to make them aware of not only the security state of the current network connection in the current network location, but also the security state in all the network contexts. We conducted a lab experiment with a diverse set of participants to examine the mental models that users have of the Vista firewall, and how VF-Basic and our prototype interface support their mental model of the firewall's system model and their understanding of its configuration.

2.4.1 Study Design

Our study was not intended as a comparative evaluation of a fully improved prototype with VF-Basic, but as an investigation of the impact of specific changes to the interface on the development of participants' mental models and their understanding of system configuration. In order to learn about how these changed after using each interface, we initially conducted a within-subjects study with 30 participants. In this study, all the participants used VF-Basic before our prototype interface (condition VF-P). However, there were concerns that this may have introduced a practice effect, priming the participants about the study protocol when using VF-Basic so that they were more careful about the network context when using our interface. Therefore, we counterbalanced the presentation order of the interfaces by performing the same study with an additional 30 participants who used our prototype interface before VF-Basic (condition P-VF).

2.4.2 Study Protocol

Each participant completed a one-hour session. We gave a brief introduction to the concept of a network location in Windows Vista and different types of network connections for those network locations so that all the participants were familiar with these concepts before beginning the experiment. We also told them the active network location and connection (Public-Wireless) on the experimental computer, a Dell XPS M1330 laptop running Microsoft Windows Vista Home Premium edition. The initial settings for the Vista firewall was off for the Public and Private network locations (enabled for Bluetooth only), and on for the Domain network location (enabled for all the network connections). Screen and voice recording software was used to record the session to augment the researcher's notes.

After completing a background questionnaire, participants were given picture cutouts of a computer, a firewall, and the Internet cloud. This was done to examine their mental model of the firewall more accurately. As Jonassen and Cho (Jonassen and Cho, 2008) discuss, "drawings can be a complementary method of verbal reports" for capturing users' mental models. We asked the participants to arrange these picture cutouts on a sheet of paper and draw arrows to show how they think the firewall works and how its settings will be applied to their computer. Figure 2.4C shows representative drawings reproduced from ones drawn by the participants. For each interface, they were asked to comment on the security state of the firewall based on information visible in the interface before undertaking two common firewall tasks.

The first task was to turn the firewall on. The second task was to block a program (Yahoo messenger) that had been previously set as an exception for both the Public and Private network locations.

After performing the tasks with each interface, we asked the participants to re-draw their mental model and briefly interviewed them about their general understanding of the effects of their actions on the security state of the computer. We then had them fill out a configuration table indicating whether they thought the firewall was on, off, or they were unsure for each of the nine possible network location/connection contexts. They did this first without looking at the interface (to see if they were aware of the effects of their actions) and then while looking at it (to see if the interface allowed them to determine the firewall's security states in both the current and future network contexts). At the end of the experimental session, the participants were given the opportunity to provide additional feedback on both interfaces and their elements. We did not comment on the correctness or completeness of their responses throughout the session so as not to provide feedback, which might influence their mental models.

2.4.3 Participants

For condition VF-P, we recruited 30 participants from both the university and general community. We sent out messages to email lists of several departments in the university, including Computer Science, Electrical and Computer Engineering, History, and Psychology. We also posted messages on two public online classifieds: Craigslist and Kijiji. Moreover, we posted and handed out flyers both at the university and local public places. To ensure diversity, we screened interested participants by email. We asked their age, gender, last educational degree and major, whether or not they were students, their occupation (if not a student), and whether or not they had used Windows Vista or a firewall. We did our best to recruit participants with similar demographics for condition P-VF to reduce individual differences which could affect the development of their mental models. All were given a $10 honorarium for their participation.

Table 4.2 shows our participants' demographics. They had a wide range of educational levels (from high school to PhD), backgrounds (e.g., mining, computer science, art), and occupations (e.g., research assistant, personal trainer, author). All were daily users of computers, but their expertise varied. The majority (21/30 in both groups) considered themselves as regular or advanced users of basic programs (e.g., web browsers, email), while the rest considered themselves more advanced (e.g., able to configure operating systems). Most (VF-P: 26/30; P-VF: 23/30) used their computers in a variety of network contexts (network locations and connections).

Condition		VF-P	P-VF	Total
Group Size (N)		30	30	60
Age	Mean Range	29.6 20-58	28.2 19-56	28.9 19-58
Gender	Female Male	15 15	15 15	30 30
Student	Yes No	15 15	15 15	30 30
Firewall Experience	Yes No	15 15	15 15	30 30
Vista Experience	Yes No	15 15	15 15	30 30

Table 2.1: Participants' demographics for each condition.

2.5 Results

We now present our results. These include the participants' mental models of how the Vista firewall works, how well they understood the effects of their configuration tasks on the security state of the firewall, and qualitative feedback about both VF-Basic and our prototype interface.

2.5.1 Mental Models

We categorized our participants' drawings of the functionality of the Vista firewall and its system model into four categories:

- **incorrect mental model**: incorrect basic understanding of the inner workings of the firewall,
- **incomplete mental model**: correct basic understanding of the firewall operation, without the context of network location and connection,
- **partially complete mental model**: correct basic understanding of the firewall operation, with either the context of network location or connection, or
- **complete mental**: correct basic understanding of the firewall operation, with both contexts of the network location and connection.

Figure 2.4C shows representative drawings of each category reproduced from ones drawn by the participants. We examined participants' transitions between these categories of mental models (Figure 2.4A,B).

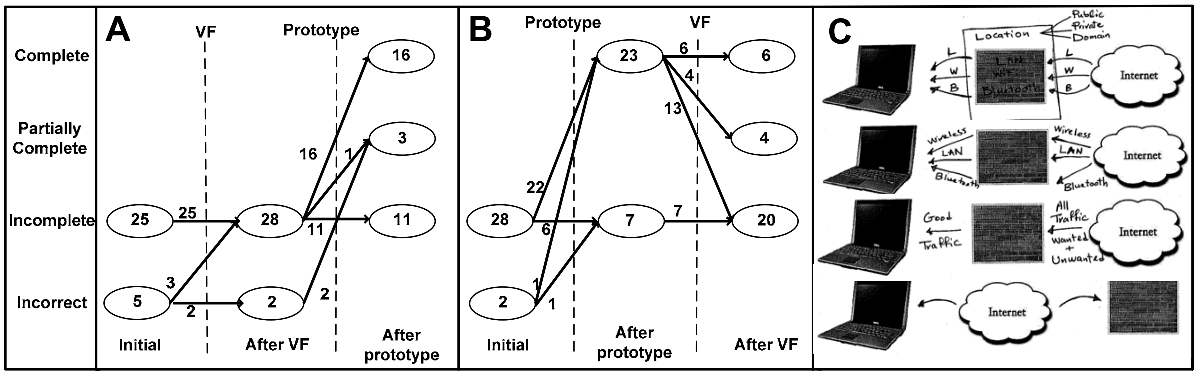


Figure 2.4: Transitions in the participants' mental models (A: condition VF-P, B: condition P-VF) and representative drawings for each category of mental models (C).

In condition VF-P, before working with the interfaces, five participants had an incorrect mental model of firewalls, while 25 participants had a correct but contextually incomplete mental model. After using VF-Basic, 3/5 participants moved from the incorrect mental model to an incomplete mental model; however, none changed their mental model to a partially complete or a complete one. After using our prototype interface, the two participants with an incorrect mental model moved to a partially complete mental model, as did one of those with an incomplete mental model. They included the context of network location in their mental model. 16/28 participants with an incomplete mental model also incorporated the full context of network location and connection into their mental model (complete). However, 11 participants still drew a contextually incomplete mental model.

In condition P-VF, before working with the interfaces, two participants had an incorrect mental model of firewalls, while 28 participants had a correct but contextually incomplete mental model. After using our prototype interface, one participant with an incorrect mental model moved to an incomplete one and the other moved to a complete mental model. 22/28 participants with an incomplete mental model also incorporated the complete context of network location and connection in their mental models. Interestingly, after using VF-Basic, only 6/23 participants with a complete mental model kept that mental model; 4/28 moved to a partially complete mental model, which included only the network connection context (visible in the advanced tab of VF-Basic (Figure 2.2C)). The rest (13/23) downgraded to an incomplete mental model.

These results contrast how our prototype interface and VF-basic affected participants' mental models of the Vista firewall's functionality and its system model.

Several comments from participants as they drew their mental models illustrate their changing understanding. One from condition VF-P, whose first two mental models were classified as *incomplete*, described her *complete* mental model drawn after working with the prototype interface, “If you put all the connections in one wire, it would be the same [as drawn after using VF-Basic], but there are three smaller wires in that wire. It will have a little more arrows to show the differences between Bluetooth, Local Area Connection, and Wireless in Public or Private and all the three have different settings.” This participant attributed her understanding to the configuration table in the prototype, “It makes everything very clear, what is wrong and what is not.” Another participant from condition P-VF, whose mental model transitioned from *incomplete* to *complete* after using our prototype interface, said “I learned that you can customize it for different locations and connections.” One participant from condition P-VF described her mental model of both VF-Basic and our prototype interface through an example. She compared VF-Basic to a light switch at the entrance of a house, which controls the light for the house as a whole, but said that our interface gives her the ability to turn the light on or off for each room.

2.5.2 Configuration Paths

Not all the participants took the same path through the interfaces as they configured the firewall. We describe their configuration paths for each interface, as these impact the configuration of the firewall.

When participants turned the firewall on in VF-Basic, it was on for the current network location (Public). They were then faced with a warning that the recommended settings were not in place (as it had not been turned on for the Private network location). Most participants (VF-P: 23; P-VF: 19) ignored this warning, in which case only Public-Bluetooth was on as Bluetooth was the only enabled network connection (CP1 in Table 4.3). The remainder (VF-P: 7; P-VF: 11) applied the recommended settings (“Update settings now” (Figure 2.1J) or “Restore defaults”(Figure 2.2C)), resulting in the firewall being turned on for all the network locations and connections (CP2 in Table 4.3). With the prototype, participants could turn the firewall on for each network location (Figure 2.3F, CP1 in Table 4.3) or for all the network locations and connections (Figure 2.3E, CP2 in Table 4.3). For those who used CP1 (VF-P: 11, P-VF: 9), three participants (VF-P: 1; P-VF: 2) turned the firewall on only for the Public network location; the rest turned it on for all the network locations and connections. All the participants who used CP2 (VF-P: 19; P-VF: 21) turned on the firewall for all the network locations and connections.

		VF-P								P-VF							
		VF-Basic				Prototype				Prototype				VF-Basic			
		Public		Private		Public		Private		Public		Private		Public		Private	
		B4	Aft.	B4	Aft.	B4	Aft.	B4	Aft.	B4	Aft.	B4	Aft.	B4	Aft.	B4	Aft.
CP1	μ	.850	1.06	.890	1.30	3.0	3.0	2.73	2.73	2.72	3.0	2.61	3.0	2.16	2.56	1.87	1.60
	σ	.438	1.01	.398	.938	0	0	.904	.904	0.19	0	0.20	0	.226	.162	.183	.182
CP2	μ	2.50	2.07	2.71	1.36	3.0	3.0	3.0	3.0	3.0	3.0	3.0	3.0	2.18	2.77	1.73	0.96
	σ	.866	1.24	.488	1.38	0	0	0	0	0	0	0	0	.255	.156	.319	.228
T	μ	1.23	1.30	1.32	1.32	3.0	3.0	2.9	2.9	2.92	3.0	2.88	3.0	2.17	2.63	1.82	1.37
	σ	.898	1.13	.886	1.03	0	0	.548	.548	.324	0	.364	0	.922	.642	.886	.83

Table 2.2: Participants' scores for configuration understanding before (B4) and After (Aft.) checking each interface. Scores reported by configuration path (VF-Basic: did not apply (CP1) or applied (CP2) recommended settings; Prototype: changed settings for each (CP1) or all (CP2) network contexts) and in total (T).

2.5.3 Understanding of the Firewall Configuration

We now present our analyses of participants' understanding of the effects of their firewall configuration tasks from two sources: participants' completion of the configuration table and their comments as they did so. The configuration table was completed twice for each interface: before checking the interface and then after checking the interface. As the domain settings are not actually within the control of the end user, we omit that data. We focus on participants' understanding of the firewall settings for six network contexts: three network connections (Wireless, Local Area Connection , and Bluetooth) within two network locations (Public and Private). We assigned a value of 0 for an incorrect response, 0.5 for an unsure response, and 1 for a correct response, and computed a raw score (with the maximum of 3 for each network location and 6 total) representing the correctness of participants' understanding of the firewall configuration. Table 4.3 provides the mean and standard deviation of scores, summed for each network location. We first present participants' overall understanding of their configuration, before examining the pseudo understanding exhibited by those who applied the recommended settings in VF-Basic. We then identify misunderstandings that result in the dangerous error of mistakenly thinking the firewall is on.

Overall Understanding of Configuration

A fully repeated measures 2x2x2x2 mixed ANOVA, with one between-subjects factor (order of interface presentation) and three within-subjects factors (interface, checking interface, network location) showed a significant main effect for interface (F(1,58) = 254.908, p $<$ .001). Participants' understanding of the

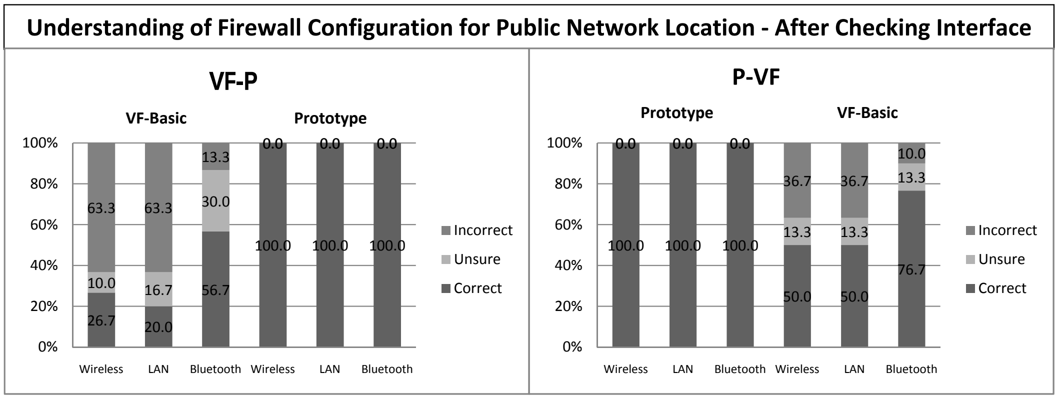


Figure 2.5: The average percentage of correct, incorrect and unsure answers in the Public network location after checking the interface for both condition VF-P and condition P-VF.

firewall settings after using our prototype interface (μ = 11.800 (out of 12, 6 for before/after checking the interface), σ = .8982) was significantly higher than after using VF-Basic (μ = 6.575, σ = 2.8371). We also found a significant interaction between interface and order (F(1,58) = 18.519, p $<$ .001), and interface, order, and location (F(1,58) = 12.053, p $<$ .01). Further analyses revealed that participants' understanding of the settings after using VF-Basic in condition P-VF (μ = 7.983, σ = 2.0021) was significantly (t(58) = -4.404, p $<$ .001) increased in contrast to condition VF-P (μ = 5.167, σ = 2.8748). This suggests that the mental models developed while using our prototype interface not only helped the participants understand its configuration, but also that this understanding often continued when they later used VF-Basic.

A within-subjects analysis (fully repeated measures 2(interface) x 2(checking) x 2(network location) ANOVA) of condition VF-P revealed no significant main effect for checking the interface or for the network location context. It also did not reveal any significant interactions between the factors. Whether or not the participants' checked the interface to confirm their answers or considered the Public or Private network location, working with the prototype improved their understanding of the firewall configuration. After working with VF-Basic, less than 30% of the participants in condition VF-P correctly understood the firewall settings for each network context, even when given the opportunity to check the settings through the interface. The exception to this was for Bluetooth, which was initially the only enabled network connection for the Public location (Figure 2.5 shows the results for the Public networklocation).

A similar within-subjects analysis of condition P-VF showed a significant main effect for network location (F(1,29) = 35.578, $p < .001$), and a significant interaction between interface and location (F(1,29) = 35.730, $p < .001$), location and checking (F(1,29) = 12.847, $p < .01$), and interface, location and checking (F(1,29) = 12.835, $p < .01$). A fully repeated measures 2(location) x 2(checking) ANOVA for our prototype showed network location and checking do not have a significant main effect on participants' understanding of the firewall settings; however, a similar analysis for VF-Basic showed a significant main effect for network location (F(1,29) = 38.184, $p < .001$) and a significant interaction between checking and network location (F(1,29) = 13.210, $p < .01$). Participants had a better understanding of the firewall configuration for the Public network location than for the Private network location as VF-Basic provides information about the Public network location (Figure 2.1F).

Since VF-Basic only shows the firewall settings for the current network location and our prototype shows the settings for all the network contexts, we also compared participants' responses with what we expected them to answer based on the information visible in the interfaces. For the Private network location (raw score of 0 to 6), it is correct to be unsure as only the settings for the Public network location is visible. A fully repeated measures 2(interface) x 2(checking) ANOVA, revealed a significant main effect for interface (VF-P: F(1,29) = 64.51, $P < .001$; P-VF: F(1,29) = 5.009, $P < .03$) indicating that participants' understanding of the settings after using our prototype interface (VF-P: μ = 5.80, σ = 1.0954; P-VF: μ = 5.883, σ = .3640) was still higher than for VF-Basic (VF-P: μ = 1.97, σ = 2.282; P-VF: μ = 5.343, σ = 1.0726), even accounting for the lack of visible information in VF-Basic. Again, there was no significant effect on the scores for checking the interface. However, we found that for the Private network location, our participants had more unsure answers in condition P-VF than in condition VF-P; this demonstrates the learning effect of our prototype interface. After using the prototype, participants were more aware of the network contexts when working with VF-Basic. In particular, they were aware that they do not know how the firewall protects their computer for the Private network location. As one participant in condition P-VF noted, "for the private, I am just sure about the unsure one."

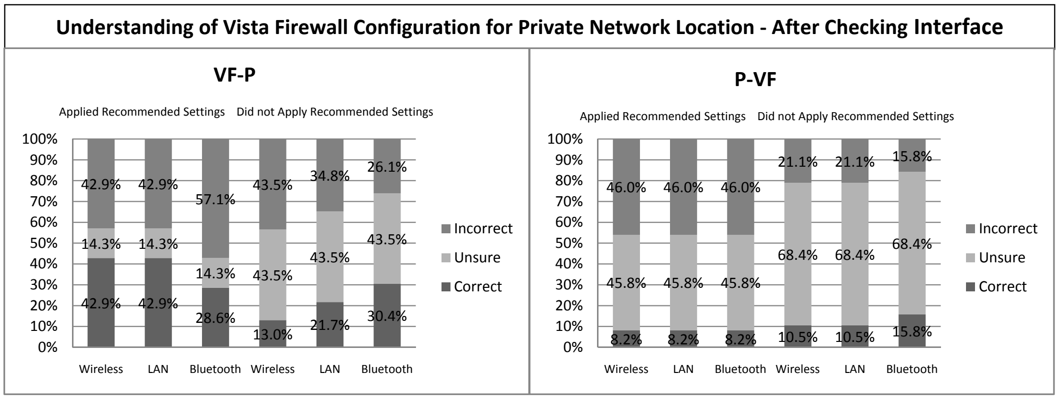


Figure 2.6: The average percentage of participants with correct, incorrect and unsure answers for the firewall settings in the Private network location after checking VF-Basic.

Pseudo Understanding of Configuration

Regardless of which configuration path our participants used with the prototype, they understood the firewall settings in both conditions VF-P and P-VF (Table 4.3). During our post-hoc analysis based on the configuration paths through VF-Basic, we found that in condition VF-P those seven participants who applied the recommended settings, had a higher percentage of correct responses than those who did not apply the recommended settings. A fully repeated measures 2x2x2 mixed ANOVA, with one between-subjects factor (applied/did not apply the recommended settings) and two within-subjects factors (checking the interface and network location) showed that this difference is statistically significant (F(1,28) = 15.163, $p < .001$). However, when compared the results for the Public and Private network locations, we saw that these participants had an increase in their incorrect answers for the Private network location after checking the interface (F(1,28) = 9.698, $p < .01$)(Figure 2.6). This suggests that their apparent understanding of the firewall configuration was shallow at best.

Upon inspection, we found that the participants were unaware that the recommended settings had been applied to the Private network location as well as their current Public network location. Their comments confirmed their pseudo understanding of the settings after clicking the “Update settings now” link (Figure 2.1J). Before the six[6] participants did so, only one correctly thought the link would enable the recommended settings. The other five had different interpretations of its functionality such as being unsure what it would do or thinking that it would provide more detailed settings, enable the recommended

[6] Seven participants in condition VF-P applied the recommended settings; six clicked the “Update settings now” link and one clicked the “Restore Defaults” link.

Windows updates, or block all incoming connections. After clicking the link, the firewall was turned on for all the network locations and connections. However, there was no feedback in the interface about what had been done to bring the firewall into the recommended state. Not surprisingly, the participants were still left with their misconceptions about what they had accomplished. Even the participant who had appeared to understand that clicking on the link would apply the recommended settings, discussed how the firewall would now be more efficient, so it is unclear exactly which recommended settings he thought were applied.

In condition P-VF, we did not find any significant difference between the scores of those who did and those who did not apply the recommended settings. In general, we had a larger percentage of unsure answers in condition P-VF both for those who did and who did not apply the recommended settings than in condition VF-P. However, as can be seen in Figure 2.6, in condition P-VF there were more incorrect answers for those participants who applied the recommended settings compared to those who did not. These participants thought that the firewall was off for the Private network location when it actually was on. This could be the effect of using our prototype interface before VF-Basic; our prototype made them aware of different network contexts, and since they could not see any information about the Private network location in VF-basic they may have thought that it was only on for the Public network location. Their comments about the “Update settings now” link (Figure 2.1J) were similar to those made in condition VF-P; none in condition P-VF understood that this link would apply the recommended settings (i.e., turn the firewall on for all the network contexts).

Dangerous Misconceptions

There are two types of incorrect answers: incorrectly believing that the firewall is turned off when it is on, and incorrectly believing that the firewall is turned on, when it is actually turned off. It is this second type of error in understanding the firewall configuration that leaves users in a dangerous state, vulnerable to attacks and malicious software. As one participant said, “The thing is because you think you put a firewall, you will be more careless because you think you have been protected rather than there is not any firewall.” None of the participants were left in this dangerous state after using the prototype interface for both condition VF-P and condition P-VF.

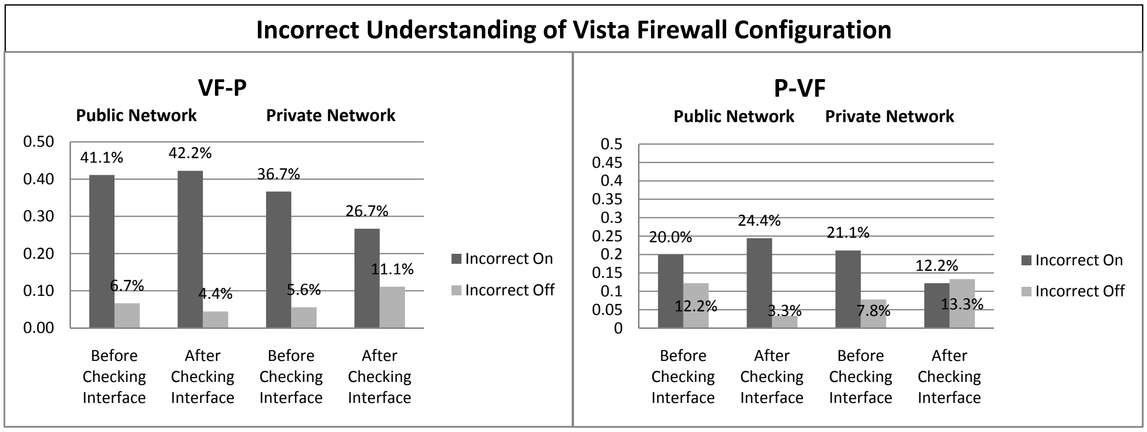


Figure 2.7: The percentage of incorrect responses after checking VF-Basic. “Incorrect On” indicates the incorrect belief that the firewall is on, when it is off. “Incorrect Off” indicates the incorrect belief that the firewall is off, when it is on.

After working with VF-Basic, there was a relatively high proportion of incorrect responses for both condition VF-P and condition P-VF (Figure 2.7). Even after checking the interface, 42.2% of the responses from condition VF-P and 24.4% from condition P-VF were incorrect for the current network location (Public); these participants had an incorrect belief that they were protected for all the network connections at the current network location. This is because VF-Basic’s main window shows the current network location (Figure 2.1F), but does not indicate if the firewall is turned on for all the network connections in that location. This information is only visible in the “Advanced” tab of its second window. For the Private network location, even after checking the interface 26.7% of the responses from condition VF-P and 12.2% from condition P-VF indicated dangerous misconceptions of the firewall being turned on when it was not.

As can be seen in Figure 2.7, the participants in condition P-VF had fewer dangerous misconceptions than those in condition VF-P. This could be the effect of presenting our prototype interface before VF-Basic which increased their awareness of the network contexts, resulting in more unsure answers than dangerous misconceptions. As one participant from condition P-VF mentioned, “the experience from previous firewall [prototype] helped me to understand the state.”

2.5.4 Qualitative Feedback on the Interfaces

VF-Basic: Recommended Settings Unclear

During the experiment, VF-Basic showed a warning that indicated that the recommended settings were not in place because the firewall was not on for all the network locations and connections. As discussed above, the firewall was only turned on for the Bluetooth connection in the Public network location unless the recommended settings were applied. All the participants were confused about the state of the firewall as they had explicitly turned it on, but then saw the warning about not using the recommended settings (as shown in Figure 2.1I). As one participant from condition VF-P said, “for some particular reason it is not on, the first thing that I am looking at is this red. This state to me is actually not right. It says it is on. If it is on, this should not be highlighted in red. This should be highlighted in green saying that it is on.” Another participant from condition P-VF also said, “I thought I activated it, let me do it again. It is saying it is on, but it is red, maybe the protection is weak.”

We asked our participants what they thought the security state of the firewall was given the feedback that it was turned on, but not using the recommended settings. Almost all (56/60) were confused about why the firewall was not using the recommended settings: 31 participants had no idea; 11 thought they should block all incoming connections (after they did so, and the warning was still there, they did not know); six participants thought that the firewall should be updated, as one said after clicking on the “Update settings” link, “Now it is on and uses its latest version;” four participants thought that it was because the Public network location was not a secure location and after reading the help files, thought that they should change it to Private; three participants thought that the update feature of Windows should be turned on; and one participant thought that the firewall protection was weak. Only four participants recognized that it had to be turned on for all the network locations and connections (three after following the help link provided in the warning, one after checking Wireless and Local Area Connection under the “Advanced” tab and restoring the default settings).

Furthermore, our participants had difficulty in understanding what to do with the information. As one from condition VF-P noted, “I do not know much about firewalls, I prefer to use the recommended settings, but I cannot find it.” Another participant from condition P-VF wanted to change the settings again after clicking on the “Update settings” link and said, “I do not know what happened. Something happened. I do not know if I want that to happen or not. There is no redo? I do not know how to take it to the previous situation. I do not know what the previous state was and how to take it to that state.” In general, we found that our participants did not know what the recommended settings were, why the firewall did not use the recommended settings, and how they could apply the recommended settings. VF-Basic did not provide them with enough information about the context of network location and connection that had affected the security state of the firewall.

Prototype Interface: Portrayal of Firewall State

Our participants commented on their preference for the prototype when we asked them how to improve the interface at the end of the session. The vast majority (56/60) explicitly mentioned that they preferred the prototype to VF-Basic. They liked the increased information about the network context that was provided in both the state diagram and the configuration table. As one from condition VF-P said, “The way that the second interface [prototype] presents the information about location is a lot more obvious.” They also appreciated the interaction abilities afforded within the interface. One from condition VF-P explained, “This interface [prototype] is much better. The pics are very instructive. I have more control about the interface and that is nice.”

Several refinements were suggested for the firewall state diagram (Figure 2.3B), including colour coding the arrow labels. There was some confusion expressed as a result of the terminology used (the term active for the network location could be misinterpreted as the firewall being active in that location). It was also suggested that the text explain what is off, instead of what is on. Two participants in condition VF-P and three in condition P-VF commented that the picture should be modified with respect to the way that the incoming connections are portrayed, providing more details about the exceptions in place. One of them drew a revised image; in his version, the arrow rebounding off the firewall should only be portrayed as such if all the incoming connections are blocked. Otherwise, the arrow should be shown going through the firewall, but narrower on the other side to represent the exceptions.

Underlying Functionality: Multiple Firewall Profiles

Participants were asked how they would prefer the firewall settings to be applied to their computer. The majority (39/60) indicated they would like to have changes applied to all the network locations and connections. This was thought to make the firewall easier to use as they would not have to worry about context, as P8 noted: “It is not a good idea to check your settings whenever you change your location.” Another perspective was that a single firewall setting would avoid confusion: “I would like the computer to be protected in any possible type of connection, regardless of where it is or how it is connected to the Internet” (P41). For these participants, the multiple firewall profiles that are applied according to the context of network location and connection adds overhead without a perceived benefit. Unfortunately, because the changes are only applied to the current network location, unless users pay attention to the changing context, they may inadvertently leave themselves in an unprotected state. The remaining 21 participants wanted some variation of what the Vista firewall currently offers: 13 participants wanted the flexibility of having more control in specific locations; four participants wanted the settings applied to their current location; three wanted to have them applied to all, but have the ability to exclude some; one wanted the flexibility for different network connections, but not locations. One participant had the interesting notion of having changes that would increase security applied to all the connections/locations, but changes that would make things less secure applied only to the current one.

2.6 Discussion

There are several implications of our findings. We first discuss whether the firewall settings should change depending on the network context. We then discuss ways of supporting users’ mental models of the underlying system model, and ways to balance security and complexity through multiple user interfaces. Finally, we discuss providing education to users of complex security systems.

2.6.1 Responding to Shifting Contexts

As is common (Klasnja et al., 2009), our diverse set of participants used their laptop computers in different network contexts. Our results showed that they often exhibited misunderstandings of the firewall configuration when working with VF-Basic. VF-Basic does not make it clear to users how the firewall reacts to changes in the network context; therefore, the user is not always aware of the system state. The design of VF-Basic would work well with a non-changing network context (i.e., a desktop computer with a single network connection), but does not provide sufficient information for mobile users. In fact, those that are unaware that their configuration is limited to the current network context may be left with the dangerous misconception that the firewall is protecting their computer for all the network contexts.

One interesting result of our study is that users don't necessarily want the correlation between network context and the firewall settings. For the large proportion of users who do not want to have their firewall settings change according to their network context or for those who are not mobile, one option would be to allow them to configure their firewall to only have one profile. This would resolve the problem of dangerous misconceptions.

There may also be a preference for explicit changes by the user (McGrenere et al., 2002), rather than trusting the system. We believe that having Vista detect the change in network context is appropriate as security is a secondary consideration of users and they may not remember to adjust their profiles appropriately (Yee, 2004). However, Vista firewall's system model has to be more clearly portrayed to the user so that they can develop an effective mental model of configuration changes.

2.6.2 Supporting Users' Mental Models

Our results suggest that the inconsistency between users' mental model and Vista firewall's system model is due to insufficient information in VF-Basic. The incomplete knowledge likely resulted in their increased uncertainty about the system state (Yee, 2002).

Working with VF-Basic did not promote inclusion of the impact of network context on the firewall settings. Revealing the hidden context of the impact of network context through the addition of the configuration table and dynamic firewall image resulted in our prototype being more effective. Still, approximately one-third of the participants in both groups did not move to a contextually complete mental model after using the prototype. It is possible that they were not aware that they should include those aspects in their drawing as they did exhibit a correct understanding of the firewall settings after using our prototype.

Beyond adding the contextual information, we suggest that throughout Windows Vista the connection between network context and the firewall state should be made explicit. When a user is choosing a network location (i.e., home, work, public) for a newly connected network, it needs to be clarified that these are mapped to the firewall profiles (i.e., Private, Private, Public). This is necessary to help users develop a mental model of how the Vista firewall will decide which settings to apply. We suggest that designers consider the impact of contextual factors when designing the user interface of any security application.

2.6.3 Balancing Complexity and Security

One of the main usability problems with the Vista firewall is that its basic and advanced interfaces are designed at the two extreme ends of the complexity versus simplicity spectrum (Chebium et al., 2008). Our findings demonstrated that VF-Basic does not provide enough contextual information to support users' mental model of how the firewall works. As shown by the difficulties participants had determining why the recommended settings were not in place, the basic interface either needs to provide more details or have better links between it and the advanced interface.

An open question is whether there needs to be separate interfaces for novice and more expert users for the Vista firewall and security applications in general. We found no obvious differences in the results attributable to participants' demographics; regardless of their backgrounds, most participants struggled with understanding their configurations with VF-Basic. If separate interfaces are indeed necessary, how can developers bridge the gap between them and support the full continuum of user knowledge and abilities with respect to both computers and security? As with other multiple interface applications, users should be able to easily switch between the two interfaces (McGrenere et al., 2002). However, unlike general applications (e.g., word processors), contextual information needs to be considered in the design of multiple interfaces for security applications. If the context impacts how the application behaves, contextual information cannot be removed from a basic interface for the sake of simplicity. Furthermore, the interface should provide enough information about the security state both for the current and future contexts.

2.6.4 Role of Education

A common thread in usable security research is educating users (Whitten and Tygar, 1999). As our results show, using our prototype before VF-Basic had some learning effect on participants' mental model of the firewall and made them aware of the network contexts, as shown by the higher percentage of unsure answers for VF-Basic in condition P-VF. It is also important to note, however, that even interaction with the prototype could not completely solve the problems that exist with VF-Basic as the interface does not provide enough contextual detail to its users. As one participant in condition P-VF mentioned, "the first one [prototype] was sensitive to my location but this one [VF-Basic] is not". Although this participant had a complete mental model after working with the prototype, he did not maintain his mental model when working with VF-Basic; the lack of information in VF-Basic led him to think the underlying functionality of the two interface is different.

We suggest that providing an interactive tutorial for the firewall may help provide a platform for users to learn about the firewall and the impact of network context on firewall configuration. This is particularly important as the link between the two at the time that network locations are created is not explicit. Gentler methods (e.g., warning messages, wizards) of providing users with guidance at the time of decision making have been proposed as alternatives to extensive tutorials (Whitten and Tygar, 1999). However, given the complexity of the firewall, opportunities for more in-depth training seem warranted in addition to revealing the effects of network context within the interface.

2.7 Summary

Supporting users' understanding of the impact of their computing context on their security software is particularly crucial as users become more mobile. We presented a study investigating how VF-Basic supports mental models of its system model and whether the addition of information about the network context could better support users' mental models of the firewall and their understanding of its configuration. We found that our proposed interface for the firewall helped participants to develop a more complete mental model of the firewall and dramatically increased their understanding of their firewall configuration. After using the contextually augmented prototype, no users had dangerous misunderstandings about the security state of the firewall. We discussed that although hiding system features and operational details can make interfaces more usable, in the case of security software complexity must be balanced against security.

Chapter 3

Expectations, Perceptions, and Misconceptions of Personal Firewalls[7]

One interesting finding of our usability studies of the Vista firewall was that the majority of our participants did not see the need for a personal firewall that changed its profiles depending on the network location it detected; rather, they only wanted a single level of protection. We realized that it was important to better understand users' knowledge, requirements, expectations, perceptions, and misconceptions of personal firewalls. This understanding is required to successfully manage design tradeoffs (Grinter and Smetters, 2003; Nielsen, 1993). To attain this goal, we performed a follow-up study, where we conducted semi-structured interviews with a diverse set of 30 participants and analyzed the data using qualitative description (Sandelowski, 2000).

Our analysis revealed that most of our participants were not aware of the functionality of personal firewalls and their role in protecting computers. Several participants required different levels of protection from their personal firewalls in different contexts. The requirements and preferences for their interaction with a personal firewall varied based on their levels of security knowledge and expertise. However, the interaction of most of them with their personal firewall was mainly limited to responding to firewall warnings.

In the rest of this chapter, we first describe our methodology. We then present our findings and provide recommendations for designing more usable and effective personal firewalls and firewall warnings.

[7] A preliminary and a full version of this chapter have been published.

- Fahimeh Raja, Kirstie Hawkey, Konstantin Beznosov, and Kellogg S. Booth. 2010. Investigating an appropriate design for personal firewalls. In *Proceedings of the 28th International Conference Extended Abstracts on Human Factors in Computing Systems* (CHI EA '10). ACM, New York, NY, USA, 4123-4128.
- Fahimeh Raja, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, and Kellogg S. Booth. 2010. It's too complicated, so I turned it off!: expectations, perceptions, and misconceptions of personal firewalls. In *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration* (SafeConfig '10). ACM, New York, NY, USA, 53-62.

3.1 Methodology

We conducted semi-structured interviews with a diverse set of participants to answer the following research questions:

- What do users know and what misconceptions do they have about personal firewalls and the protection provided by them?
- What expectations do users have of personal firewalls?
- How do users prefer to interact with their personal firewall (i.e., level of automation, feedback)?
- Do users need to have different levels of protection offered by their personal firewall? Why or why not?
- What factors, do users think, affect their required level of protection from a personal firewall?

We chose interviews because they are useful for investigating events that occur infrequently and irregularly (Giacoppo, 2001), which is the case for users' interaction with personal firewalls. Interviews were much cheaper, easier, and faster to conduct than a field study. In contrast to questionnaires, interviews are more interactive; we could ask follow-up questions to further probe participants for more details and also reasons behind their responses. Because our study was exploratory, interviews could provide us with the background information to identify potential areas for more in-depth investigations and to generate hypotheses that can be tested through controlled experiments. Moreover, interviews have been successfully employed in usable security research to gain insights about users' security perceptions and misconceptions (Friedman et al., 2002; Downs et al., 2006; Gross and Rosson, 2007).

There are three types of interview protocols: unstructured, semi-structured, and structured interviews. Semi-structured interviews provide researchers with more control over questions and answers than unstructured interviews. Additionally, in contrast to structured interviews where questions and their ordering should not vary, semi-structured interviews provide researchers with the freedom to more thoroughly explore interesting issues as they arise during the interview. Unstructured interviews were not appropriate for our study because we did have specific research questions to answer. As we did want flexibility to probe interesting topics as they emerged, we selected semi-structured interviews.

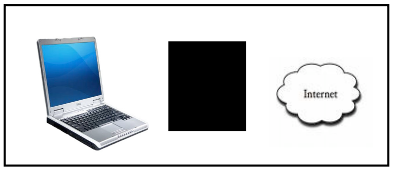


Figure 3.1: The black-box figure used to assess participants' perceptions and requirements of a security application such as a personal firewall.

3.1.1 Study Protocol

We conducted a one-hour, audio-recorded, semi-structured interview with the participants. They first completed a consent form and background questionnaire. This included an assessment of their security knowledge and experience with the following tasks taken from the "Security Center" of Windows Vista (Windows Security Center, 2010):

- installing updates,
- scanning for viruses, spyware, and other potentially unwanted software,
- deleting browsing history and cookies,
- setting different security controls for different users, and
- managing browser plug-ins.

We chose these tasks because they are common security tasks that a home computer user might perform on any operating system and with any web browser. We asked the participants to describe what they knew about the tasks and their importance, and to specify how often they performed those tasks.

To assess participants' requirements, expectations and perceptions of a security application such as a personal firewall, we showed them a picture of a black box located between a computer and the network (Figure 3.1) and told them that the box is a security application, which will be designed to protect their computer. We used a black box to avoid biasing their discussion to current firewall functionality. However, in the course of the interview, we explicitly talked about personal firewalls and asked the participants questions about their knowledge of and experience with personal firewalls to determine if they knew what a personal firewall is, what its purpose is, how it works, how it can meet their security needs, and how it differs from other security software such as anti-virus software.

We asked the participants questions such as:

- What do you want this application to do? What are your expectations of such an application?
- What is important for you to be protected against by this application?
- What security software do you have on your computer? Anti-virus? Firewall?
- What do you like/dislike about your security software?
- How do you want to interact with the software? (We asked about automation and feedback)
- Do you want the software to always have the same behavior?
- What are the factors that would affect your requirements of the software and its protection? (We asked for type of information, location, connection type, etc.)
- In general, what is your reaction to security alerts? If the software asks you to Allow or Block a program?

For all the questions, we probed the participants for the reasoning behind their responses.

We generated additional questions based on participants' responses to gain a more in-depth understanding of their actual practices because in self-reported data, participants' claims about their actions may be different from their actual behavior (McGrath, 1995). In particular, responses may be influenced by what participants think the interviewer is looking for or what they think is the correct answer. We also tried to ask the same question in multiple ways, using different wordings, at different times during the interview to examine if participants gave consistent responses to the questions about their attitudes, beliefs, desires, and experiences. Moreover, we asked questions about participants' activities with their personal computers. Based on those activities, we generated personalized use-case scenarios to understand their experience using personal firewalls. For example, if a participant mentioned online gaming in his activities, we used a scenario of connecting to a game server.

The same interviewer conducted all the interviews. This provided some opportunities to follow up on interesting responses of earlier participants, allowing us to probe other participants to determine whether they had similar experiences and to adjust interview questions based on the responses.

3.1.2 Participants

We recruited 30 participants from both the university and general community. To recruit participants, we sent out messages to email lists of several departments in the university, including Electrical and Computer Engineering, Computer Science, History, and Psychology. We also posted messages to two online classifieds, Craigslist and Kijiji. Moreover, we posted and handed out flyers both at the university and local public places. To ensure diversity, we screened interested participants by email. We asked their age, gender, last educational degree and major, whether or not they were students, and their occupation (if not a student). All participants were given a $10 honorarium for their participation.

Our participants had a wide range of educational levels (from high school to Ph.D.) and backgrounds (e.g., mining, business, computer science, art, pharmacy, and material), as well as occupations (e.g., research assistant, librarian, accountant, teacher). All were daily users of computers, but their expertise varied. The majority (19/30) considered themselves as regular or advanced users of basic programs (e.g., web browsers, email), while the rest considered themselves more advanced (e.g., able to configure their operating system(s)). Almost all (28/30) used a laptop in a variety of networks.

Based on the responses to our background questionnaire (see Section 4.3.2 for more details about the questionnaire), we classified our participants' security knowledge and experience into three categories: high, medium, and low. The categorization was done to understand users' expectations, perceptions, and misconceptions of a personal firewall in relation to their level of security knowledge and expertise. To increase the reliability of our categorization, two researchers independently rated the participants' security knowledge and experience. An inter-rater reliability analysis using the Kappa statistic was performed to determine consistency between the raters. The reliability was found to be Kappa = .897 ($p <$ .001). While this shows a high agreement between raters, two participants were categorized differently. The two researchers subsequently discussed the categories with each other and achieved consensus on the categorization. They moved one participant who was categorized as high by the second researcher to medium, and one who was categorized as medium by the first researcher to low. Table 4.2 shows the demographics of the participants in each group.

It should be noted that those participants in group H were not security experts who practice security as their primary task (i.e., security practitioners), but their security knowledge and expertise was high compared to average users of computers.

Group		**L**	**M**	**H**	**Total**
Security Level		Low	Medium	High	N/A
Group Size (N)		13	11	6	30
Age	Mean	28.4	26.5	26.2	27.3
	Range	20-51	22-32	26-27	20-51
Gender	Female	9	3	1	13
	Male	4	8	5	17
Student	Yes	5	6	4	15
	No	8	5	2	15
Primary OS	XP	2	2	1	5
	Vista	8	6	3	17
	Mac	3	3	2	8
	Linux	0	0	0	0
Secondary OS	XP	2	1	1	4
	Vista	0	0	1	1
	Mac	0	0	1	1
	Linux	0	1	3	4

Table 3.1: Participants' demographics for differing levels of security knowledge and expertise.

3.2 Data Analysis

We transcribed the audio records of the interviews and analyzed the data using Qualitative Description (Sandelowski, 2000). We iteratively coded the interviews to conceptualize the data in them. We started by *open coding* where we coded the interviews with concepts that emerged from the data itself. We continued with *axial coding* by constantly comparing and modifying the codes, eventually merging some of them into new codes. Then, we organized and classified these codes into higher-level categories, and reviewed and synthesized them to obtain a "big picture" of the results.

One potential threat to validity in qualitative research is researcher bias, i.e., "the researchers find what they want to find, and then they write up their results" (Johnson, 1997, p. 283). An effective strategy for increasing the validity of the analysis is to use multiple investigators in interpreting the data (Johnson, 1997). In our study, the data was analyzed by two researchers. The first was the researcher who designed the study, collected the data, and knew the whole context of the interviews; the second was another researcher who was not involved in the project before data analysis and, therefore, was less biased to find specific results.

3.3 Results

We classified our findings into four different categories: (1) perceptions of the black-box, (2) knowledge about a personal firewall, (3) context, and (4) interaction. Next, we present our results.

3.3.1 Perceptions of the Black-Box

When the participants with a higher level of security knowledge and experience (all 6 in group H, 5 in group M) saw the black-box, they asked if it was existing security software, a new type of software, or a combination of both. When we asked what they needed, they all said they prefer to have all-in-one security software that combines the existing security solutions. Everyone in group H thought that this would make the configuration of security software easier for end users; as H26[8] said, *"an all-in-one because at the moment we have anti-viruses, anti-spyware, anti-malware, firewalls, monitoring devices, logging devices. Each of them has a different way of configuring and setting up and that's confusing to users."* Participant H1 also mentioned that users lack knowledge about the protection provided by security software, so having an all-in-one solution can prevent a false sense of security: *"a home user does not know what a firewall is. If you ask him, he'll tell [you] it protects you from viruses. When he buys a firewall, he expects it to protect him from viruses. So it is a good thing to have them all in one, because he actually buys what he expects."* M4 also stated that he wants the black-box only if it is an all-in-one software which replaces all of his current software: *"One of the hassles of the current system is that you have to use multiple things at the same time: firewall, anti-spyware, adwares, anti-virus. The ideal solution would be to add all of this into one package. If I had to add it on top of the current ones then I don't need it. I think five is enough, I do not really want the sixth one."*

Comments from the participants with a lower level of security knowledge and experience also revealed requirements and expectations from the black-box that can be met only by integrating several types of security software: *"First of all I like something that prevents unwanted applications to come to my computer, and prevent scanning data from my computer, and I don't like to see something running on my computer that I don't have any control over when I browse a website, and also I don't like that some software can send my data to unknown place. Also I like to remove my data, especially information of my bank account, to reduce the risk"* (L20).

[8] In this chapter, we refer to individual participants by their grouping by level of security knowledge (L, M, H) from Table 4.2 and participant number (1..30).

3.3.2 Knowledge about Personal Firewalls

None of our participants with a low level of security knowledge and experience knew about the functionality of a firewall or the protection it provides. They did not know the difference between a firewall and anti-virus software and why they need both; as L3 said, *"the only thing that I know, firewall always comes automatic, and anti-virus, I know you have to purchase it online or install it by disk."* Comments from six participants in group L showed their misconceptions about the protection provided by their different security software. For example, L16 incorrectly thought his anti-virus controls access to his computer, which is actually what a firewall does: *"Me and some other people are complaining; we don't know what's happening, I don't have a connection, I can not call with my computer, it's probably a security software. Q: Do you know which software it is? I mean, what kind of security software? A: Anti-virus."* We also noticed that most of the participants in group L (except L20) had a general awareness of anti-virus software. They had anti-virus software installed on their computer and had some prior interaction with it, such as installing updates for it or scanning for viruses. But most of these participants did not know whether or not they have a personal firewall installed on their computer.

Everyone in group H and six in group M knew about the functionality of a firewall and had previous experience configuring a firewall; they needed to do so in order to perform activities such as playing games (4 in group M), sharing files (all in group H, M4, M8, M29), and downloading and installing applications (4 in group H, M4, M8, M29). Others in group M were not sure about the exact functionality of a firewall, although they knew it was different from an anti-virus. Some comments from these participants (M18, M21, M24) show that they faced problems during configuration of their firewall. For example, M18 described his problems when configuring his firewall to allow a legitimate connection, which resulted in him turning his firewall off: *"We had a printer in my office, and we wanted to share it between the computers. We followed the normal routine for sharing but it didn't work. I could see the printer in my computer, I could send a print, but it wouldn't print anything. We didn't know what was the problem, we asked the computer staff to solve the problem and he came to my computer through remote tests, he changed some settings and he told me that the problem was with my firewall and I had to do these things. I wanted to make a change, but for me it was too complicated and I didn't know what the consequences were, so I turned it off. I don't know the meaning of inbound and outbound. There were a lot of things actually. Just for a file, there was not just one with this name, but ten or twelve."*

Some personal firewalls can filter both incoming (from the network to the computer) and outgoing (from the computer to the network) traffic. We examined if our participants knew why they need bidirectional protection. Several participants (2 in group M and 6 in group L) did not know why, but stated various preferences for either incoming or outgoing protection, as L17 said: *"I can download some files from the Internet and I don't want them to have viruses. From my computer to Internet, what can it do? I don't care."* Other participants preferred to have protection in both directions: *"If your computer has a malicious code on it and you don't know that, it could prevent it and vice versa, preventing the malicious codes for getting into the system"* (H3). However, none of the participants mentioned the dual role of blocking outgoing connections. They either mentioned that it would protect other users in the network from malicious connections coming out of the user's system (3 in group H, 4 in group L): *"A good design practice would be to take care if the system is actually compromised to stop the spread of the compromise to other systems"* (H1), or mentioned that it prevents malicious applications from sending private information of the user to unknown sources (H22, M4).

3.3.3 Context

We examined if the participants' required level of protection from their security software, including personal firewalls, varied depending on the usage context. All in group H and seven in group M wanted varying levels of protection based on:

- **their activity**, e.g., file sharing, computer programming, online gaming, and working on sensitive or confidential information (5 in group H and 6 in group M): *"For some tasks, I like to have complete protection, but it is somehow annoying. You want to open a port for peer-to-peer software, it's very dangerous in terms of security but you need it. So when I want to work with my bank account, I don't like any software, not even well-known software to connect to the Internet. But for my regular tasks, I'm not really picky"* (M22).

- **trust and familiarity with the network and its infrastructure** (4 in group H, M4, M28): *"Because sometimes we have different environments, for example if I am connected to my work network, I would expect a set of settings or policies, because I trust the network, but when I go to a coffee shop and I connect to their network, basically it is an untrusted network, I would use different policies which are tougher and more restrictive"* (H25).

- **the type of network connection** (4 in group H, 3 in group M): *"I think different access to the Internet needs different levels of protection, the LAN is safer than the wireless"* (M10).
- **security of the network** (5 in group H and M4): *"When we are talking about wireless connections there is further refinements. It could be a very secure wireless connection that is only supposed to be used by a small group and is encrypted, or it could be something anyone in a particular location can use and is not encrypted... They're both wireless connections but definitely something encrypted and meant for a smaller group is more secure"* (H9).
- **the people in the network** (all in group H, M2, M8, M28): *"when I am in LAN or even wireless with my friends, I don't need security, less security. I trust my friends"* (M8).
- **more technical features** such as host name and IP address (H1, H6): *"I'd rather use something more technical, maybe some IP settings, or a nickname for each network"* (H6).

Participants also liked the ability to choose and control their level of security in different contexts (H1, H6, H26, M4); however, some participants (H1, M13, M18, M28) mentioned they would use different levels of protection provided by the firewall only if it is easy to do that. Several participants (all in group H, 4 in group M, 4 in group L) thought non-expert users want to have the same protection in all contexts, *"because [otherwise] you would be getting into complications, and for my little brain, it is just too much"* (L12). Four participants in group L did not know why they would ever need a lower level of protection, preferring the highest level of protection everywhere: *"Always the highest. Why should it be low? How can it affect me? Why should I choose different levels?"* (L17). The remainder thought an intermediate level of security is the best: *"A basic level of security for a novice user is probably the best. A higher level will bother him in situations he cannot solve, whereas a low level will leave him exposed"* (H1).

While the focus of this study was not specifically on the Vista firewall, we discussed its use of multiple profiles to provide the user with different levels of protection. As described before, Windows Vista uses the concept of Network Location to classify different networks in three categories: Home, Work, and Public. These categories then will be mapped into two profiles for the firewall: Private and Public. We examined on what basis the participants would choose the network location, and if they relate these categories to the protection provided by their firewall.

None knew about the effect of choosing a network location on the firewall settings. None in group H and M would choose the network location based on their physical location, *"Even if I am at home, I put it as a Public location so no one can connect and intervene"* (M4). However, several participants (3 in group H, 4 in group M) believed that less knowledgeable users might choose only based on their physical location. Indeed, L5, L16, L19 and L30 confirmed that; as L19 said, *"I don't know what it is for, I just choose Home because it is home, even at a party maybe Home; at a coffee shop, Public."* L7, L11, and L17 also mentioned that they do not think about security when they choose the network location: *"For example I go to a hotel and they have several connections and I don't pay for the Internet, I'm just choosing free WiFi, so I need public access, but if I'm at home and I choose public maybe it will be available for everybody. I don't want them to use it otherwise I will go over my limit"* (L17).

3.3.4 Interaction

Personal firewalls usually generate warnings that prompt users to ask whether a connection should be allowed or blocked. We probed if our participants understood the warnings and their reaction to them. Many of the participants did not make informed decisions in response to the warnings. There were three different reasons for the lack of an informed decision:

- **Not understanding the warnings**: All in group L and three in group M did not understand the warnings. Some of them thought if they don't understand a message, the safe choice is to ignore it: *"In my own opinion they are not quite easy to understand and quite straightforward most of the time. If I don't understand what the message says I just ignore it"* (L15).
- **Interference with a primary task**: Several participants (4 in group H, 2 in group M, 8 in group L) turned their firewall off or did not pay attention to the messages because the warnings interfere with their primary task: *"If you really want that game or movie, you just choose ignore. But for me, don't even alert us because we don't even know what it means"* (L7).
- **Previous experience**: Some participants (H1, H9, M4, L3, L7, L17) noted previous experience can affect users' decision making about the warnings: *"Users tend to get used to them and disregard them even if it's a critical pop-up. So it's just Allow, Allow, Allow. Because they hit Allow a thousand times and nothing wrong happens"* (H1). L15 also mentioned he decides based on others' experience: *"As long as many friends have it [the game] installed, I would install it."*

Ignoring firewall warnings can come in different forms:

- **Uninstalling the firewall** (H1, H25, M10): *"Last time I installed a firewall, there were a lot of alarms. This program should be stopped. I think that's very boring. That is why I put the firewall away to lose the pop-ups"* (M10).
- **Switching to another firewall** (M2, L5, L7, L12): *"I don't use that firewall anymore. It is too sensitive. I got alerts all the time. This one [the new one] gives me alerts but not so often"* (M2).
- **Turning the firewall off** (H22, H26, M4, L16, L19): *"It's like locking the classroom door when the class is about to start; you have to open the door for everybody, so you would prefer [to] keep it open"* (M4).
- **Getting habituated to warnings** (7 in group M and L27, L30): *"Most of the time I say Allow. That is what I have found, otherwise I can't go forward. I don't want to read all of this. If I am downloading something, I say Allow, but if in the middle of nowhere it pops up then I will read it. But most of the time the reaction would be Allow. I know that it is trying to protect my computer, but there is a tradeoff. I can not pay attention to each and every pop-up"* (M10).

All the participants except H26 and M28 thought frequent warnings are frustrating or annoying for them and are one of the reasons they disliked security software: *"I don't like how some security software start popping up something. It's kind of annoying"* (L14). We asked them how they would rather interact with their firewall. Our results showed that the level of automation and control required by our participants depends on their security knowledge and expertise. None in group H wanted full automation for their security software, preferring to retain some level of control: *"everything automated is an annoyance"* (H1), *"the software cannot decide on your preferences"* (H6). On the other hand, participants agreed that users with a low level of security knowledge and experience need full automation, stating that they lack the required knowledge and experience to configure their security software (all in group H, 5 in group M, 9 in group L) and the motivation to learn and understand security (4 in group H, M4, 5 in group L): *"You cannot expect normal people to understand those complexities. There is no reason for them to understand the details; it is not their job"* (L19). Some participants thought the software should be intelligent and learn from users' behaviour (3 in group H, 4 in group M); H25 specifically talked about automating decisions made in a specific context.

Four participants in group L mentioned that, because they do not have the required knowledge to judge the firewall warnings, the software should provide them with a recommended action. Some (M8, L3, L23, L27) also wanted to know the threat level associated with their action: *"I need to get a specific message with some information, maybe a threat level. Maybe the software can give a number from 1 to 100 for example. If it's under 30, it is okay"* (L3). Quotes from four participants in group L revealed that those with a low level of security knowledge and expertise may be willing to follow the software recommendations. As L17 said, *"One thing is that McAfee shows you, Bad site, Good site, you know? It shows you on the right: green or red or yellow, be careful. Q: What's your reaction to them? A: I never go to the red ones."*

3.4 Discussion

Next, we discuss the interpretations of our results about (1) participants' knowledge of personal firewalls, (2) participants' required level of protection based on context, and (3) participants' interaction with their personal firewalls. We describe how our findings can affect the design of personal firewalls and their warnings.

3.4.1 Knowledge about Personal Firewalls

Our findings show that many of our participants, especially those with a low-level of security knowledge, were unaware of the functionality of a firewall, or even its existence on their computers. Most of the participants did not have a useful mental model of firewalls. They, therefore, had problems during their previous experiences (if any) configuring a firewall. Lack of awareness of firewalls and their functionality may result in a false sense of protection. Therefore, it is essential to provide a greater awareness of personal firewalls and their functionality. While there are several possible means of promoting such awareness, we suggest that the following two options may be most appropriate.

The first option is to have an all-in-one security solution. Our findings show that users are willing to have an all-in-one security package. Providing a package that integrates different security functions might reduce confusion and misconceptions about the protection provided by specific software. This is also in line with the findings of Dourish et al. (Dourish et al., 2004) that "a technology deployed to solve [just] one problem" may not be appropriate for end-users.

The second approach is to design firewall warnings that provide users with a functional mental model of a personal firewall. We noticed that many of our participants interact with their firewall only when the firewall prompts them to make a security decision. This could be an appropriate "teachable" moment. Therefore, providing textual or visual information about the functionality of a firewall in its warnings may be a good method for communicating a useful mental model of personal firewalls.

3.4.2 Context

Our results show that most of our participants, especially those with a low level of security knowledge and experience, are unable to make an informed decision considering context. They do not know what contextual factors affect their security requirements at the moment, and how they affect them. They also do not know when and where they need a higher or lower level of protection. On the other hand, those with a higher level of security knowledge and expertise prefer to have control over the configuration of their security software. They want different levels of protection based on several contextual factors.

Three types of contextual factors appeared to determine the required level of protection from a personal firewall: type of activity (e.g., online banking versus online gaming), network characteristics and settings (e.g., wireless versus wired), and people in the network (e.g., family members versus people in a coffee shop). We recommend providing an option for more advanced users to customize the security level of their personal firewall, and their security software in general, based on the contextual factors that affect their security requirements. However, to be effective, it should be possible for users to switch between different levels of security when required.

3.4.3 Interaction

We found that the interaction of most of the participants with personal firewalls is limited to responding to firewall warnings. Considering Cranor's classification of security communications (Cranor, 2008), firewall warnings fall into the "active prompts" category that do not let the user proceed with his primary task until he decides whether to allow or block the connection. There are several factors that affect the success or failure of a communication (Cranor, 2008), including the characteristics of the communication and the human receiver. As our results show, one important factor in the failure of our participants in responding to firewall warnings is the human receiver, "the human who receives the security communication and whose actions will impact system security" (Cranor, 2008, p. 2).

Most of our participants lack the required knowledge to assess the consequences of allowing or blocking a connection. At the same time, because blocking the connection does not allow them to perform their primary task, they are not motivated to do such an assessment, and may, therefore, allow a malicious connection. Moreover, as Cranor (Cranor, 2008) discusses and our results also show, a key factor in users' attitudes and beliefs about warnings is their previous experience with those warnings. A personal firewall prompts the user with the same warnings for both legitimate and malicious connections. Thus, the user may have experienced allowing legitimate connections without any security problems and, therefore, be less concerned about malicious connections. They may even go beyond ignoring the warnings and disable their firewall when they receive frequent warnings.

Our results also reveal that many of our participants, especially those with a low level of security knowledge and expertise, prefer to have a firewall that automatically decides whether to allow or block a connection. Automation can be one solution for reducing the frequency of warnings. According to our findings, the action of allowing or blocking connections in a firewall could be automated based on (1) the user's prior decisions, (2) the user's expected behavior, or (3) other users' behavior. Prior research (DiGioia and Dourish, 2005; Besmer et al., 2010) also show that relying on a community consensus can be effective for users without the required expertise to make an appropriate decision.

If a personal firewall automates security decisions, it should have a mechanism for providing awareness of the decision outcome(s). Such feedback allows the user to be aware of the status of the system, and also might assist him in dealing with failures of the system. Passive notices would be one way to provide such awareness. These notices should be designed to be understandable, with short, unambiguous, and jargon-free descriptions (Cranor, 2008). If a decision about a connection attempt cannot be made automatically, the firewall should provide the user with active warnings. However, unlike current firewall warnings that only ask the user to allow or block the connection, the warnings should provide information about the level of risk associated with allowing the connection, and also a recommended action. This is in line with suggestions made by prior research on phishing warnings (Egelman et al., 2008; Downs et al., 2006; Cranor, 2008). Moreover, visualizations, such as the approaches proposed in our previous study and those by Stoll et al. (Stoll et al., 2008), can be used to help users make more informed decisions. As we discussed before, in addition to their immediate function, firewall warnings should be designed in a way that helps users understand the functionality of the personal firewall. This could help users be aware of the existence of the firewall, and help them in their future decisions.

3.4.4 Summary of Design Recommendations

Now, we summarize our recommendations for improving the design of personal firewalls.

- ***All-in-one solution:*** Provide personal firewalls as an integrated solution with other security software. Provide consistent configuration and terminology throughout the interface.
- ***Awareness in warnings and notices:*** Allow users to obtain a functional mental model of personal firewalls by showing their functionality in firewall warnings and notices.
- ***Recommendation in warnings:*** Recommend an action in firewall warnings. Recommendation can be either an explicit recommended action or can provide the threat level and instructions that help users find the most appropriate action in response to firewall warnings.
- ***Decision based on context:*** Help users identify relevant contextual factors and relate those factors to the level of security required.
- ***Allow easy change of the security level:*** Provide users with a visible and straightforward way for changing the level of security when a relevant contextual factor changes.
- ***Automate possible actions:*** Identify and automate those actions that can be automated with high probability of success.
- ***Awareness about automated decisions:*** Provide users with passive notices about automated decisions.
- ***Adapt to users' knowledge and expertise:*** Determine the level of user's knowledge and expertise and change the behavior of the firewall accordingly.

3.5 Summary

We presented a study investigating participants' knowledge, requirements, perceptions, and misconceptions of personal firewalls. Our qualitative analysis of the data revealed that participants with different levels of security knowledge have varying levels of awareness of the functionality of a personal firewall, and its role in protecting computers. Our results also suggest that context is an important factor in our participants' security decision making. We found several contextual factors that affect our participants' decisions; however, we also found that most participants lack the knowledge to determine the required level of security based on contextual factors. Our results also showed that the interaction of most of our participants with personal firewalls was limited to responding to firewall warnings; however, many of them had problems making informed decisions when they receive those warnings, which results in them ignoring these warnings. Based on our results, we provided implications for the design of personal firewalls. Our recommendations will benefit those designing personal firewalls, other security software, or complex systems that need to adapt to changing contexts, or provide warnings in the interaction with end-users.

One limitation of our study is that it is based on self-reported data. We did our best to probe participants both for their experience and belief, not just what they thought the researcher is looking for. However, we believe complementary research methods, such as observational research, are required to confirm our findings.

Chapter 4

Personal Firewall Warnings based on a Physical Security Mental Model[9]

One interesting finding of our study of users' knowledge and perceptions of personal firewalls was that the interaction of most of our participants with firewalls was limited to responding to firewall warnings. Therefore, a correct response to these warnings is key to the correct configuration, and thus, the effectiveness of personal firewalls. However, we also found that users do not make an informed decision in response to the warnings. One of the most important reasons identified for this behavior was that users lack the required knowledge to understand the warnings. One solution is automation; however, full automation with no user intervention is difficult to achieve; it is often infeasible to completely remove the human from the loop (Edwards et al., 2007; Cranor, 2008). We suggested to design firewall warnings that provide users with a functional mental model of firewalls and that better communicate the risks.

There is evidence that communicating risk to home users of computers has been unsuccessful in the field of computer security (Downs et al., 2006; Egelman et al., 2008; Sunshine et al., 2009; Motiee et al., 2010). In the warning science literature, one successful technique for risk communication is the mental model approach, which is a risk communication method based on the recipients' mental model (Morgan, 2002). This approach has been successfully applied in areas, such as medical (Jungermann et al., 1988) and environmental (Ronnfeldt, 1997) risk communication; but not in computer security. Risk communication in computer security has been based on experts' mental models, which are not good models for typical users. Experts' mental model of security is different from non-experts' (Asgharpour et al., 2007; Camp et al., 2007). This gap could lead to ineffective risk communication to non-experts. Asgharpour et al. (Asgharpour et al., 2007) proposed that the design of risk communication such as security warnings

[9] A short version of this chapter has been submitted for publication.

- Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Clement Wang, and Konstantin Beznosov. 2011. Promoting A Physical Security Mental Model for Personal Firewall Warnings. Submitted for publications.

should be based on non-experts' mental models and metaphors from the real world. They emphasized that:

> *The purpose of risk communication is not conveying the perfect truth, but rather prompting the users to take an appropriate action to defend their system against a certain threat. While mitigation of a risk requires knowledge of the general nature of the risk, efficacy of the risk communication requires communication that is aligned with the mental model of the target group. Effective risk communication often requires more of an understanding of the risk perception of the communication target, as opposed to a communication optimized for technical accuracy* (Asgharpour et al., 2007, p. 368).

An open question is what an appropriate mental model is to use for firewall warnings. Interviews by Wash (Wash, 2008, 2010) showed that one of the most common mental models of security is the physical security and burglar mental model. Liu et al. (Liu et al., 2008) also performed a quantitative analysis to evaluate the five mental models proposed by Camp et al. for computer security (Camp et al., 2007): physical security, medical infections, criminal behavior, warfare, and economic failure. Their results showed that for 70% of the risks, non-expert users have physical and criminal mental models; for firewalls, the physical mental model was the closest to both expert and non-expert users' mental models. This suggests that the physical security mental model could be an appropriate mental model for risk communication to non-expert users in computer security, particularly for personal firewalls.

In this chapter, we present a study in which we examined the effectiveness of using a mental model of physical security in firewall warnings. We used an iterative process in the design of the firewall warnings in which the functionality of a personal firewall is visualized based on a physical security mental model and the metaphor of a firewall. Our goal was to determine the degree to which the warnings are understandable for our participants, and the degree to which they convey the risks and encourage safe behavior. Our results showed that compared to warnings based on those of the most popular personal firewall, our proposed warnings were more understandable for the participants; they helped the participants develop a better mental model of the functionality of a personal firewall, better communicated the risks, and increased the likelihood of safe behavior.

Next, we provide prior work on the usability of security warnings.

4.1 Related Work

Prior research investigated the effectiveness of warnings in usable security. Zurko et al. (Zurko et al., 2002) evaluated the usability of Lotus Notes security warnings in a 500-person organization. The purpose of Lotus Notes security warnings is to prohibit users from running unsigned active content. They found that 59% of their participants allowed the unsigned content to run because they were not aware of the risks. Based on their findings, the authors suggested educating users or including more information in security-related warnings.

Downs et al. (Downs et al., 2006) performed interviews with 20 non-expert users to understand their reactions when encountering phishing sites. They found that users have little awareness of phishing, and security warnings provide little or no meaning to many of them. They recommended describing the intuition behind recommended actions in a non-technical way.

Cranor (Cranor, 2008) proposed the human-in-the-loop framework that provides a systematic approach for identifying reasons for human failures in interaction with security applications. Her framework can be used to find out why a particular security warning is ineffective. She provided an example of how the framework can be used to evaluate anti-phishing warnings.

Egelman et al. (Egelman et al., 2008) performed a laboratory experiment to examine the effectiveness of both active and passive phishing warnings in web browsers. They found that active warnings are more effective than passive warnings, and passive warnings are not different from not having any warning at all. Based on the results, they suggested that security warnings should interrupt users' primary task, convey the recommended action clearly, fail safely if the user ignores or misunderstands the warning, and prevent habituation.

Sunshine et al. (Sunshine et al., 2009) performed a survey of around 400 Internet users to investigate their understanding of and reactions to SSL warnings. Their survey showed that risk perception is correlated with decisions to obey or ignore security warnings and that the participants who understood security warnings perceived a different level of risk associated with the warnings. They designed two new warnings and compared them with three existing SSL warnings in a laboratory study with 100 students. They evaluated three strategies: "explain the potential danger facing users, make it difficult for users to ignore, and ask a question users can answer." Based on the results, they suggested improving the design of warnings using appropriate colors and text, and decreasing their frequency.

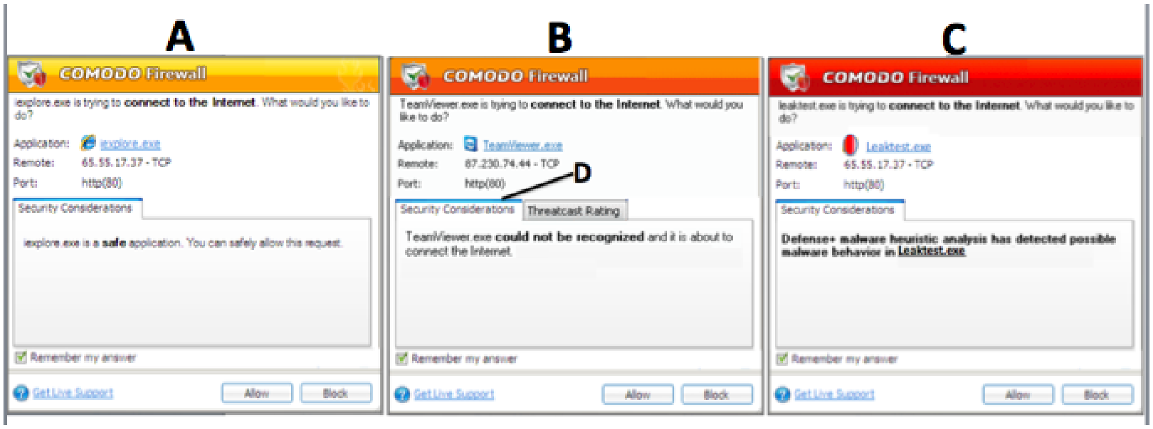
Motiee et al. (Motiee et al., 2010) performed a laboratory experiment and contextual interviews to investigate the motives, understanding, behaviour, and challenges users face when responding to User Account Control (UAC) prompts in Windows Vista and Windows 7. They found 69% of the participants do not use the UAC approach correctly and suggested using educational prompts to convey the purpose of UAC and reducing the number of prompts when a user initiates an action.

While prior research informed our study of firewall warnings, none evaluated the effectiveness of the mental model approach for computer security warnings. The goal of this part of our research is to mitigate this gap.

4.2 Prototype Interface Design

We designed two sets of warnings: our proposed one, which is based on a physical security mental model (which we call P-warnings (Fig. 4.3)), and one based on the Comodo personal firewall warnings (which we call C-warnings (Fig. 4.2)). We selected the Comodo personal firewall to compare to our proposed warnings because the Comodo personal firewall is the most popular personal firewall (PCWorld, 2010b; TopTenReviews, 2010), and is generally considered the top one not only for its protection (TopTenReviews, 2010; ConsumerSearch, 2010; Gizmo's Freeware Reviews, 2010; Bhamra, 2010; PCmag, 2010), but also for its "warning features that make it easy for novices to understand how to respond to those warnings" (TopTenReviews, 2010). Comodo is also ranked first for its warning design in a survey of ten state of the art personal firewalls (PCWorld, 2010a).

The Comodo personal firewall includes a database, which is a classification of all known executable files. It categorizes different applications in three categories based on their level of risk: safe, unrecognized, or malicious. Using this database, the Comodo personal firewall provides "security considerations" (Fig. 4.1.D) in its warnings to help users make informed decisions in response to the warnings. This is in line with recommendations for designing risk communications and security warnings (Stewart and Martin, 1994; Egelman et al., 2008). Based on this classification we designed six different interfaces, three for P-warnings: P-safe (Fig. 4.3.A), P-unrecognized (Fig. 4.3.B), P-malicious (Fig. 4.3.C), and three for C-warnings: C-safe (Fig. 4.2.A), C-unrecognized (Fig. 4.2.B), C-malicious (Fig. 4.2.C).



iexplore.exe is trying to **connect to the Internet**. What would you like to do?

Application: iexplore.exe
Remote: 65.55.17.37 - TCP
Port: http(80)

iexplore.exe is a **safe** application. You can safely allow this request.

TeamViewer.exe is trying to **connect to the Internet**. What would you like to do?

Application: TeamViewer.exe
Remote: 87.230.74.44 - TCP
Port: http(80)

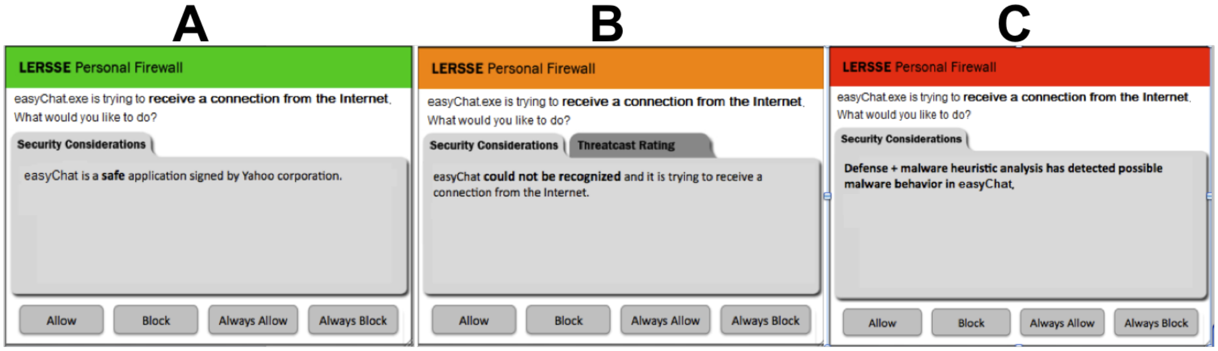
TeamViewer.exe **could not be recognized** and it is about to connect the Internet.

leaktest.exe is trying to **connect to the Internet**. What would you like to do?

Application: Leaktest.exe
Remote: 65.55.17.37 - TCP
Port: http(80)

Defense+ malware heuristic analysis has detected possible malware behavior in Leaktest.exe

Figure 4.1: The original warnings of Comodo personal firewall (A: Safe, B: Unrecognized, C: Malicious, D: Security Considerations).



easyChat.exe is trying to **receive a connection from the Internet**. What would you like to do?

easyChat is a **safe** application signed by Yahoo corporation.

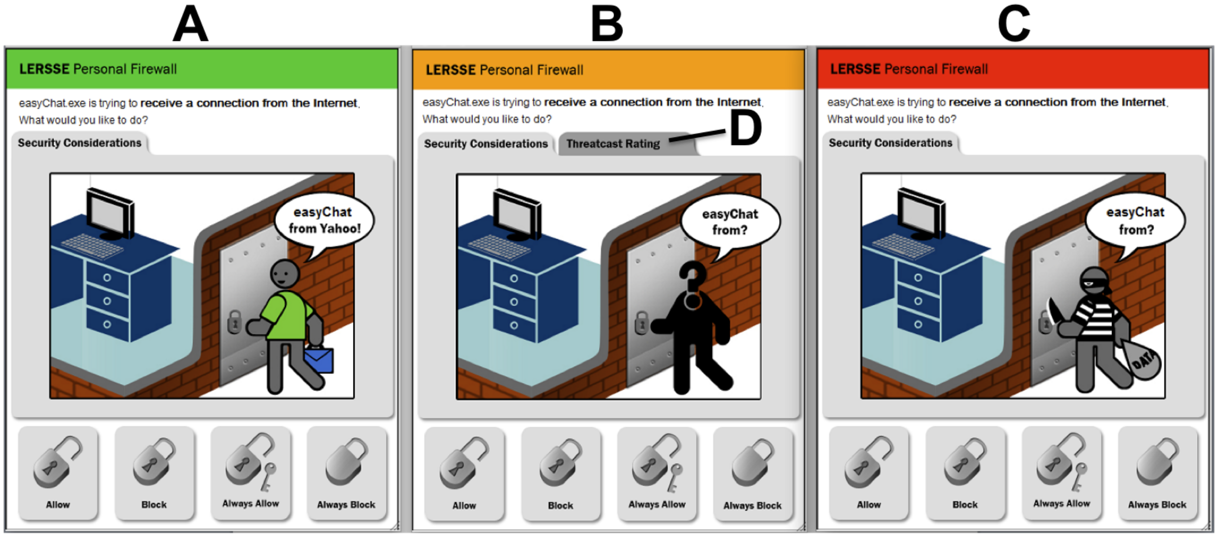
easyChat.exe is trying to **receive a connection from the Internet**. What would you like to do?

easyChat **could not be recognized** and it is trying to receive a connection from the Internet.

easyChat.exe is trying to **receive a connection from the Internet**. What would you like to do?

Defense + malware heuristic analysis has detected possible malware behavior in easyChat.

Figure 4.2: Warnings designed based on the warnings of Comodo personal firewall (A: Safe, B: Unrecognized, C: Malicious).



easyChat.exe is trying to **receive a connection from the Internet**. What would you like to do?

Figure 4.3: Our proposed warnings based on a physical security mental model (A: Safe, B: Unrecognized, C: Malicious).

To design C-warnings, we made several changes in Comodo's warnings (Fig. 4.1). As recommended in the usable security literature (Downs et al., 2006; Cranor, 2008), security warnings should be jargon-free. Therefore, we removed three pieces of technical information (i.e., protocol (TCP or UDP), remote IP address, and port) from Comodo's warnings. We also removed the recommended action, even though it is recommended in the usable security literature (Egelman et al., 2008) to eliminate its effect on participants' intention. Comodo's warnings also show how other people who are using the Comodo personal firewall have responded to the warning for a specific unrecognized application. Prior research (DiGioia and Dourish, 2005; Besmer et al., 2010) found that relying on a community consensus can be effective for non-experts to make an appropriate decision. We kept this feature in our warnings. However, similar to Comodo's design it was not in the first window of the warnings, but hidden under a second tab (Fig. 4.3.D). We did not want this feature to affect our participants' risk perception.

For P-warnings, we mimicked Comodo's layout. We applied an iterative process for the design of each element in the interfaces. After Internet searches and asking friends and family for feedback, we determined common metaphors for physical security. Those included locks, keys, doors, walls, doormen, policemen, and stop-signs. We then performed two series of formative studies. The first formative study was performed with 10 participants on paper prototypes of the warnings. In this study, we had three different designs for conveying the functionality of a firewall through a physical security mental model (See Appendix B). We also had several icons for each action (i.e., Allow, Block, or Remember my answer). Based on the participants' feedback, we selected the most appropriate design, and redesigned the interfaces (See Appendix C). We performed another study with 10 more participants, and then based on the participants' feedback, we finalized the design of the warnings. We hired a graphical interface designer to develop the interfaces for us. This ensured consistency in presentation of all the warnings.

In the final P-warning interfaces we used a brick wall and a metal door to suggest a physical firewall and a fire exit, which are the actual metaphors for a computer firewall.We added a lock on the door, which was recognized as the most familiar and understandable metaphor for controlling access in physical security by our formative study participants. We put a computer inside the wall to show that the wall is preventing access to the computer. We used a figure who wants to go through the door to represent the application that wants to make a connection through the firewall. We also used a cloud to show the name of the application and its developer.

For actions (Allow, Block, Always Allow, Always Block),[10] we added icons corresponding the lock on the metal door. One had the lock unlocked to allow access once through the door, one kept the lock locked to deny access, give the key to grant permanent access, and one had a lock without a keyhole to permanently block access.

To indicate different levels of security risk, we used different colors and different figures with different cloud quotes. For the interface for safe applications, we used a figure wearing a green shirt with a smile on his face, and with a quote representing he was developed by Yahoo! (Fig. 4.3.A). Our formative study revealed that this figure is friendly, trustworthy, and would give participants a positive impression, thereby leading them to grant access. For the interface for unrecognized applications, we used a figure coloured in black with a question mark as its head to show that the application was unidentified (Fig. 4.3.B). For the malicious interface, we used a figure dressed in a prisoner's uniform, who carries a knife and a thief's bag (Fig. 4.3.C). According to our formative study participants "the message that the interface conveys is very clear: It is very dangerous!"

4.3 Methodology

Based on the human-in-the-loop framework (Cranor, 2008), there are three steps in processing warning information: (1) communication delivery (attention switch and maintenance), (2) communication processing (comprehension and knowledge acquisition), and (3) application (knowledge retention and transfer). The focus of our research was on step (2), the communication processing. It is an important step because if the user does not understand a warning he can not make an informed decision in response to that warning.

We were not concerned with communication delivery, step (1), because firewall warnings are "active warnings." That is, they interrupt users' primary tasks and force them to pay attention to the warning and decide whether to allow or block the connection in order to proceed with their primary tasks (Cranor, 2008). We also did not attempt to examine how users transfer the knowledge gained from their interaction with our warnings to other types of warning, step (3). We did not want to evaluate any long term effects of our warnings; we wanted to first investigate what our participants understand from the warnings.

[10] Our formative study revealed that participants prefer "Always Allow" and "Always Block" to "Remember my answer."

Our research questions in this study were:

- Do our participants understand what the warnings mean when they encounter them for the first time?
- What are participants' misunderstandings or confusions about the warnings?
- Are our proposed warnings more understandable for the participants than those designed based on Comodo's warnings?
- How do the warnings affect participants' intention to act?
- Which kind of warnings would participants prefer to have for their personal firewall? Why?

There are two approaches in the warning science literature for evaluating comprehension and the degree of initial clarity of warnings: open-ended and multiple choice tests (Young and Lovvoll, 1999; Leonard et al., 1999). We used an open-ended test because open-ended tests provide more information about confusion and the types of errors people make (Wolff and Wogalter, 1998; Leonard et al., 1999). This information might assist in subsequent redesign work. Moreover, the cognitive process in open-ended tests is more similar to the cognitive process people perform when encountering a warning in the real world. People usually do not choose from a list of answers. Therefore, the ecological validity of open-ended tests is more than for multiple choice tests (Wolff and Wogalter, 1998). One issue with open-ended tests is that the evaluation of the responses is less clear-cut and, therefore, more difficult. There is usually some subjective judgment about the correctness of open-ended responses; therefore, the responses should be evaluated by more than one evaluator (Young and Lovvoll, 1999; Leonard et al., 1999). In our study, we used three evaluators to increase the reliability of our evaluations.

As is common in warning science, we used "risk perception" to measure intention. Risk perception is considered the most important factor of intention (Young and Lovvoll, 1999). Risk perception is defined as the "perceived chance of injury, damage, or loss" (McKechnie, 1983). There are multiple known contributing variables to risk perception, including:

- hazardousness of the situation,
- likelihood of damage or loss, and
- severity of the potential damage or loss (Young and Lovvoll, 1999).

We used the most common approach for evaluating warnings on each dimension, which is using Likert-type scales ranging from 0 to 7, followed by an interview for clarifications (Young and Lovvoll, 1999; Wogalter et al., 2002). We also used the self-reported likelihood of choosing any action as the behavioral intention for performing that action.

It should be noted that intention is not actual behavior. Evaluating users' behavior in response to warnings would require the study to be conducted in a real context (Young and Lovvoll, 1999). That is not always possible in the case of security warnings (Egelman et al., 2007), and especially firewall warnings. Direct observation of users' behavior in response to firewall warnings is time and labor consuming because users' interaction with these warnings is infrequent and sporadic. Laboratory studies also may not be generalizable to real world situations because providing a believable risk situation, which is actually safe, is very challenging (Sotirakopoulos et al., 2010). On the other hand, allowing unsecure situations to occur in laboratory studies to simulate the real context has serious ethical concerns (Young and Lovvoll, 1999).

We did not design our study to evaluate users' behavior in response to the warnings, but to examine whether or not the changes that we propose for firewall warnings were understandable for our participants. We also wanted to determine the degree to which our proposed warnings convey the risk, and how they might impact participants' intended action, compared to current firewall warnings.

4.3.1 Study Design

We performed a within-subjects study to compare our proposed warnings based on a physical security mental model (P-warnings) with the ones designed based on Comodo's warnings (C-warnings). We felt this was more appropriate than a between-subjects design, because we had concerns about controlling individual differences between our participants; as discussed by Cranor (Cranor, 2008), each individual "brings to the situation a set of personal variables, intentions, and capabilities" that impact the warning information processing. However, to reduce the practice effect introduced by a within-subjects design, we counterbalanced the presentation order of the warnings. We had two conditions; in the first condition (P-C) all participants saw P-warnings first, while in the second condition (C-P), they saw C-warnings first. We also counterbalanced the presentation order of safe, unrecognized, and malicious interfaces within each condition.

	P-C	C-P
Order 1	PsCs – PuCu – PmCm	CsPs – CuPu – CmPm
Order 2	PsCs – PmCm – PuCu	CsPs – CmPm – CuPu
Order 3	PuCu – PsCs – PmCm	CuPu – CsPs – CmPm
Order 4	PuCu – PmCm – PsCs	CuPu – CmPm – CsPs
Order 5	PmCm – PsCs – PuCu	CmPm – CsPs – CuPu
Order 6	PmCm – PuCu – PsCs	CmPm – CuPu – CsPs

Table 4.1: Presentation order of the warnings (P: our proposed warnings based on Physical security mental model, and C: warnings designed based on Comodo's warnings; s: safe, u: unrecognized, and m: malicious).

In our initial study design, we presented all safe, unrecognized, and malicious interfaces of one warning design (P or C) before the other one (C or P). However, during our pilot study, we realized that presenting one set of warnings (P or C) to the participants primes them about the existence of three levels of risk for the other set (C or P). Thus, they were more careful when specifying their perceived risk level for the second set of warnings. Moreover, the only difference (if any) they would express between safe, unrecognized, and malicious interfaces in each set was the level of risk. Seeing one interface from a specific set did not affect their understanding of the later interfaces from the same set; they maintained their understanding of one interface when they saw the other two in the same set of warnings. Therefore, to reduce the bias from risk priming, we changed our design. We decided to show one interface (safe, unrecognized, or malicious) from one set (P or C) and then show the corresponding interface (safe, unrecognized, or malicious) from the other set (C or P), and examine participants' understanding for the first interface they see from each set. Based on this study design, we had 12 presentation orders of the interfaces presented in Table 4.1. We randomly assigned participants to each order.

4.3.2 Study Protocol

Each participant completed a one-hour session in a meeting room in our department. There were three researchers in each session of the study. Voice recording software was used to record the session to augment researchers' notes. In the study, the participants were first given a brief introduction about the purpose of the study and the procedure. Then, they completed a consent form and background questionnaire. This included an assessment of their security knowledge and experience.

We assessed participants' security knowledge and experience with the following six tasks taken from the "Security Center" of Windows Vista (Windows Security Center, 2010):

- installing updates,
- scanning for viruses, spyware, and other potentially unwanted software,
- changing security settings of web browsers,
- deleting browsing history and cookies,
- setting different security controls for different users, and
- managing browser plug-ins.

We chose these tasks because they are common security tasks that a home computer user might perform on any operating system and with any web browser. We asked the participants to describe what they knew about the tasks and their importance, and to specify how often they performed those tasks. To find out if any participants had special computer security knowledge or expertise, we asked them if they had attended any computer security course, workshop, or conference; and if they have had any computer security related-jobs.

We then described a scenario for the participants; this is recommended in the warning science literature to provide context for participants when examining their understanding and comprehension of warnings (Young and Lovvoll, 1999). We asked participants to assume that they are in an urgent need of using a chat application that gives them the ability to do video conferencing with four other people in different locations. We told them to assume that they want an application which provides videos of all the four other people with whom they are chatting. For this purpose, they do research on the Internet, and find an application, called easyChat, with these specifications. They download and install the application and send it to others to start using it. But, when they want to use the application, they get a warning from their security software. We used this scenario because chat application traffic must be allowed through personal firewalls in order to connect to the Internet, and also because chat applications are commonly used by home users of computers. We then presented the participants with the interfaces using one of the orders in Table 4.1.

After presenting each interface, we had an interview with the participants to examine their understanding and also possible misunderstandings of the interface and its elements. We asked them what would be their reaction to the warning. Then we asked them to fill out a questionnaire and specify their perceived level of hazard, likelihood of damage or loss, and severity of potential damage or loss on a scale of 0 to 7. If their responses was greater than 0, we asked the participant to describe the potential hazards. We also asked the participants to specify the probability with which they would choose one of the options provided for them to respond to the warning (Allow, Block, Always Allow, Always Block). We then had a brief interview with them about the reasoning for their answers. We repeated the same procedure for the other interfaces. At the end of the experimental session, we opened all the interfaces and asked the participants about their preferred warning design and their reasoning. Finally, the participants were given the opportunity to provide additional feedback on both warnings and the textual and pictorial elements.

4.3.3 Participants

We recruited 61 participants from both the university and general community. We had to exclude one participant because of his inconsistent responses about his demographics in the screening email and in the questionnaire used during the study. To recruit participants, we sent out messages to email lists of several departments in the university, including Computer Science, Electrical and Computer Engineering, Mining Engineering, History, and Psychology. We also posted messages to our university's online classified, as well as two public online classifieds, Craigslist and Kijiji. Moreover, we posted and handed out flyers both at the university and local public places. To ensure diversity, we screened interested participants by email. We asked their age, gender, last educational degree and major, whether or not they were students, and their occupation (if not a student). All participants were given a $15 honorarium for their participation.

Table 4.2 shows the demographics of the participants. They had a wide range of occupations (e.g., professor emeritus, physician, diamond trader, telephone representative). All except one, who used a computer weekly, were daily users of computers, but their expertise varied. Over half (18/30 (P-C), 20/30 (C-P)) considered themselves regular or advanced users of basic programs (e.g., web browsers, email), while the rest considered themselves more advanced (e.g., able to configure operating systems).

Condition		**P-C**	**C-P**	**Total**
Group Size (N)		30	30	60
Age	Mean	31.4	31.2	31.3
	Range	18-67	19-68	18-68
Gender	Female	16	14	30
	Male	14	16	30
Student	Yes	16	17	33
	No	14	13	27
Educational Level	Highschool	5	6	11
	Bachelor	13	15	28
	Master	10	7	17
	PhD	2	2	4
Background	Computer Sci./Eng.	6	5	11
	Science	5	2	7
	Engineering	7	9	16
	Art	8	12	20
	Business	4	2	6
Primary OS	Windows XP	9	9	18
	Windows Vista	6	9	15
	Windows 7	7	6	13
	Mac	7	5	12
	Linux	1	1	2
Security Level	High	2	3	5
	Medium	8	9	17
	Low	20	18	38

Table 4.2: Participants' demographics for each condition.

Based on the responses to our background questionnaire (see Section 4.3.2 for more details about the questionnaire), we classified our participants' security knowledge and experience as high, medium, and low. The categorization was done to understand our participants' comprehension of the warnings in relation to their level of security knowledge and expertise. To increase the reliability of our categorization, three researchers, who performed the study, independently rated the participants' security knowledge and experience. An inter-rater reliability analysis using the Fleiss's Kappa statistic was performed to determine consistency among the raters. The reliability was found to be Kappa = .796 ($p < .001$), which shows a high agreement among the raters. The researchers subsequently discussed the categories with each other and achieved consensus on them.

Participants in group H are not security experts who practice security as their primary task (i.e., security practitioners), but their security knowledge and expertise is high compared to average users of computers. None of our participants had attended any computer security course, workshop, or conference. None had have any computer security-related jobs.

4.4 Data Analysis

We used a card sorting approach (Nielsen, 1995) to analyze the data. We first wrote our participants' responses to the interview questions on index cards. Then, we iteratively sorted the index cards for each question into multiple piles so that cards representing similar responses were in the same pile. We then associated a theme with each pile, that represented participants' understandings, misunderstandings, risks perception, and preferences for the warnings. This process was done iteratively to classify the responses.

4.5 Results

Results include (1) our participants' understandings of the warnings, (2) the effect of the warnings on their risk perception and intended action in response to the warnings, and (3) their preferences for the warnings.

4.5.1 Warning Understanding

We report our participants' initial understanding of the warnings for the two first interfaces viewed, one P-warning and one C-warning. When we asked our participants to describe what they understood from the warnings, most of them started with repeating the text at the top of the warnings. Further assessment of their comments revealed that P-warnings made them more aware of the protection provided by the firewall.

With P-warnings, most of the participants (48 (80%): 23 in (P-C), 25 in (C-P)) said that the warning was generated by security software that was preventing access to their computer: "it is from your software, which is kinda a barrier" (P34). They also explained what would happen if they choose each of the options provided for them in response to the warnings. As P8 noted: "it is a door and you control the lock. Nice ... so your computer is presumably safe in a locked up space. I think this is what your firewall does, now there is this new software [easyChat] which is trying to access the computer through the door, and you have the control of the lock, so you can either allow or block it. Cool ... I like it. It tells you the whole story."

With C-warnings, 57% of the participants (34: 23 in (P-C), 11 in (C-P)) talked about the prevention provided by the firewall; however, it should be noted that most of these participants had seen P-warnings first. They mainly mentioned that the warning conveys a similar message as P-warnings and just emphasized different presentations of the message (17 participants), or different levels of risk that they convey (16 participants). From the remaining 26 participants, most of them (18 participants) read the text in C-warnings and emphasized the terms written in bold. The rest (eight participants), either had misunderstanding about the warnings or said they did not understand the warnings, why they would get the warning, or what would happen if they clicked on *Allow* or *Block*.

Some participants misunderstood the warnings. For P-warnings, nine participants (six in (P-C), three in (C-P)) thought that the warning was generated by the chat application, asking them if they wanted to chat with someone from Yahoo! (for safe applications), someone unknown (for unrecognized applications), or someone malicious (for malicious applications): "somebody from Yahoo! is connecting to me, how does this guy from Yahoo know me?" (P54). Three participants also thought that the warning was about their wireless connectivity, asking them whether or not they wanted to have a connection to the Internet. For C-warnings, beside those who did not understand what the warning message was and those who only read the text in the warnings, we had one participant who thought that the message was from easyChat; another one thought there was a problem in his Internet connection: "it says it needs to connect to the Internet, but it can't, maybe I need to refresh my Internet, or turn the router off and on" (P49); and the last one thought that the warning was for the security of his Internet connection: "now if I allow it, my Internet is safe, and I can check my emails securely."

In addition to participants' understanding of the warnings as a whole, we assessed their understanding of each element of the warnings as well. For P-warnnings, we found that the question mark on the top of the figure for unrecognized applications, and also the quote "from?" was not clear for five participants; two thought that the figure had a question, and that was why he wanted to connect to them; the other three noted that they did not know what that quote and question mark meant. For C-warnings, three technical terms were not understandable for some of the participants; three showed confusion about the term "signed" in the warning for safe applications, as P24 mentioned: "It says it can steal your Yahoo! password to sign in to my Yahoo! ID." Two mentioned that they did not understand "could not be recognized" for unrecognized applications: "unrecognized by whom?" Five participants also mentioned that they did now know what "malware" means.

4.5.2 Risk Perception and Intended Action

A fully repeated measures 2x6x2 mixed ANOVA, with one within-subjects factor (warning type (P-warning, C-warning)) and two between-subjects factors (warning type order (P-C, C-P) and threat order (SUM, SMU, USM, UMS, MSU, MUS)[11]) was conducted to evaluate the effect of the warnings on participants' risk perception and intended action. We present our results for the warnings based on the level of risk they convey.

Warnings for Safe Applications

For safe applications, we did not find a significant main effect for any factor (the warning type, the warning type order, and the threat order) on participants' perceived hazardousness of the situation, likelihood of damage or loss, severity of the potential damage or loss, and their reported likelihood of allowing or blocking the program. There was no significant interaction between the factors. These results suggest no difference between P-warnings and C-warnings for safe applications with respect to participants' risk perception and intended action. For both warnings, their perceived level of risk was appropriately low and most of them were more likely to allow the program (See Table 4.3).

Our participants mentioned several factors that could affect their low level of risk perception and their intention to allow the safe application. For P-warnings, 33 participants pointed out that the interface does not have any element that conveys risk to them, as P25 said: "this particular image doesn't not give any signal for any danger." Twenty four participants mentioned that the appearance of the figure in the image is friendly; more specifically they noted that the smile on his face is a sign of safety: "a smile would definitely tell you that it's OK" (P54). Some (17 participants) noted "Yahoo!" is a trusted corporation, thereby allowing the program; as P22 mentioned "easyChat is from Yahoo! this encourages us to relax." Twelve participants pointed to the green color as an indicator of safety: "the green really signals to go ahead." For C-warnings, the most important factors for most participants was the term "safe" (46), the name of "Yahoo!" corporation (37), and the green color (27).

[11] S: Safe, U: Unrecognized, M: Malicious.

	Risk Perception	Safe				Unrecognized				Malicious			
		P-warning		C-warning		P-warning		C-warning		P-warning		C-warning	
		μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ
P-C N=30	Level of Hazard	1.6	1.6	1.3	1.4	3.9	1.9	3.3	1.8	6.0	1.2	5.1	1.4
	Likelihood of loss	1.7	1.5	1.3	1.4	3.8	1.9	3.1	1.9	6.0	1.1	5.0	1.5
	Severity of loss	1.9	1.9	1.3	1.5	3.5	1.9	3.3	2.1	5.9	1.3	5.1	1.5
	Allow	65.1	38.5	55.6	43.4	50.0	41.2	61.8	32.9	10.3	19.0	19.7	29.9
	Block	9.2	20.3	9.7	21.2	20.9	30.5	26.7	28.5	35.7	41.1	43.5	38.6
	Always Allow	21.0	34.4	34.3	44.6	8.2	21.6	3.8	9.4	6.3	19.7	1.0	2.8
	Always Block	4.7	18.3	0.3	1.3	20.9	38.4	8.0	25.5	47.3	46.8	35.5	40.6
C-P N=30	Level of Hazard	1.4	1.4	1.4	1.5	3.6	1.7	3.0	1.8	6.3	0.9	4.4	1.7
	Likelihood of loss	1.3	1.3	1.2	1.3	3.5	1.5	2.9	1.6	6.1	0.8	4.2	1.7
	Severity of loss	1.8	2.0	1.5	1.6	3.6	1.8	3.0	1.9	6.0	0.9	4.3	1.7
	Allow	66.1	37.0	50.8	37.8	50.0	33.8	63.6	36.3	12.4	22.4	30.0	32.4
	Block	8.1	16.1	10.4	18.7	35.1	31.6	18.7	26.0	47.3	39.2	43.0	38.1
	Always Allow	22.3	36.7	36.2	42.6	2.8	7.2	6.7	19.4	1.2	4.7	4.2	15.0
	Always Block	3.4	9.9	2.7	6.8	12.1	27.0	10.9	27.1	39.1	41.2	22.8	34.6
Total N=60	Level of Hazard	1.5	1.4	1.3	1.4	3.8	1.8	3.2	1.8	6.1	1.0	4.7	1.6
	Likelihood of loss	1.5	1.4	1.3	1.3	3.6	1.7	3.0	1.8	6.0	1.0	4.6	1.6
	Severity of loss	1.8	1.9	1.4	1.5	3.6	1.8	3.1	2.0	6.0	1.1	4.7	1.6
	Allow	65.6	37.4	53.2	40.4	50.0	37.3	62.7	34.4	11.4	20.6	24.8	31.3
	Block	8.7	18.2	10.1	19.8	28.0	31.6	22.7	27.4	41.5	40.3	43.3	38.1
	Always Allow	21.7	35.3	35.3	43.3	5.5	16.2	5.3	15.2	3.8	14.4	2.6	10.8
	Always Block	4.0	14.6	1.5	5.0	16.5	33.2	9.4	26.1	43.2	43.9	29.2	38.0

Table 4.3: Participants' perceived level of hazard, likelihood of damage or loss, and severity of the potential damage or loss in a scale of (0..7), and the probability of choosing Allow, Block, Always Allow, and Always Block. P: warnings based on a physical security mental model, C: warnings based on the Comodo personal firewall warnings. Highlighted columns show the significant results.

Warnings for Unrecognized Applications

For unrecognized applications, participants' risk perception was significantly higher for P-warnings than for C-warnings (See Table 4.3 a, b, c). Our analysis showed a significant main effect for the warning type on participants' perceived level of hazard (F(1,48) = 7.515, $p <. 01$, Partial Eta Squared = .135), likelihood of damage or loss (F(1,48) = 9.915, $p < .01$, Partial Eta Squared = .171), and severity of the potential damage or loss (F(1,48) = 4.445, $p < .05$, Partial Eta Squared = .085). Moreover, we found a significant effect for the warning type on the probability of allowing the program (F(1,48) = 8.615, $p < .01$, Partial Eta Squared = .152). There was no significant interaction between the factors. These results suggest that with P-warnings, participants' risk perception was higher, and they were less likely to allow the unrecognized application than with C-warnings.

Quotes from participants revealed that they might be more cautious when they encounter P-warnings than C-warnings for unrecognized applications. According to 36 participants, the question mark on the head of the figure in P-warnings is a sign of risk, as P42 mentioned "the question mark says it all, who is it from? It is alarming, indicating I should be aware." Some (17 participants) mentioned that the question mark made them "question the application;" P8 stated that "it is giving you a very good feeling of do you do know what is sneaking upon you." 13 participants even noted that as the firewall cannot provide information about the application, they would do more research on the application, such as searching in the Internet to find reviews about the application, asking friends, family, or others who they think would be more security knowledgeable: "it looks more like a warning, the application is not familiar to the firewall, I might go on the Internet and see if I can find something else, if not and I am in urgent need I will ask people who know more about computers than me" (P37). If they could not find more information they would prefer to block the program "to be safe than sorry, because it is something questionable. It is better to block it" (P57).

Warnings for Malicious Applications

For malicious applications, warning type had a significant effect on participants' perceived hazardouness of the situation (F(1,48) = 36.258, $p < .001$, Partial Eta Squared = .430), likelihood of damage or loss (F(1,48) = 37.831, $p < .001$, Partial Eta Squared = .441), severity of the potential damage or loss (F(1,48) = 28.447, $p < .001$, Partial Eta Squared = .372), and probability of allowing the program (F(1,48) = 10.539, $p < .01$, Partial Eta Squared = .180). More interestingly, we found that type of warning had a significant main effect on the probability of always blocking a malicious program (F(1,48) = 7.980, $p < .01$, Partial Eta Squared = .143). There was no significant interaction between factors. These results show that P-warnings convey more risks to the participants than do C-warnings.

According to 31 participants, P-warnings make the connection with theft in the real world. As P8 noted, "cognitively, I know it is not any different from the other one [C-warnings], but it just hints at you if you let it in, it is like inviting a burglar in your house." This made them think about consequences of allowing the program (47 participants), such as it accessing their computer and stealing their information. They found the bandit appearance of the figure and the knife in his hand to be very scary (23 participants) and that it conveyed the risk well (43 participants). In addition to these factors, the red color in the interface (26 participants) contributed to the decision of participants to block the application.

Risk Perception	Safe				Unrecognized				Malicious			
	P-warning		C-warning		P-warning		C-warning		P-warning		C-warning	
	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ
Level of Hazard	2.2	1.7	1.1	1.3	3.5	2.3	2.6	1.9	6.6	0.7	4.6	1.9
Likelihood of loss	2.1	1.7	0.9	1.2	3.2	2.3	2.9	1.3	6.5	0.7	4.2	1.9
Severity of loss	2.7	2.5	1.6	1.9	2.9	2.1	2.6	1.8	6.5	1.0	4.0	2.0
Allow	38.0	38.2	44.0	36.4	67.5	41.1	63.3	39.6	3.0	6.7	31.0	35.7
Block	10.0	17.0	1.0	3.2	15.0	30.9	19.0	29.5	53.0	46.4	25.0	40.1
Always Allow	40.0	45.0	52.5	38.1	4.0	8.1	8.5	19.1	6.0	19.0	2.5	6.3
Always Block	12.0	31.2	2.5	6.3	13.5	31.4	9.2	20.2	38.0	43.7	41.5	41.3

Table 4.4: Participants' (N=10) perceived level of hazard, likelihood of damage or loss, and severity of the potential damage or loss in a scale of (0..7), and the probability of choosing Allow, Block, Always Allow, and Always Block (for only the first interface they saw). P: warnings based on a physical security mental model, C: warnings based on Comodo personal firewall warnings. Highlighted columns show the significant results.

Post-Hoc Analysis

To examine if our within-subjects study design had affected our results, we performed further analysis of the data. To minimize priming effects, we took the first interface everyone saw and performed a between-subjects analysis (N=10 for each interface). The results showed that for malicious applications, warning type still had a significant main effect on participants' perceived level of hazard (F(1,18) = 9.783, $p < .01$, Partial Eta Squared = .352), likelihood of damage or loss (F(1,18) = 13.188, $p < .01$, Partial Eta Squared = .423), severity of the potential damage or loss (F(1,18) = 13.235, $p < .01$, Partial Eta Squared = .424), and probability of allowing the program (F(1,18) = 5.929, $p < .05$, Partial Eta Squared = .248). With P-warnings, participants' risk perception was higher, and they were less likely to allow the malicious application than with C-warnings (See Table 4.4).

To evaluate whether priming had actually impacted our findings, we compared our participants' perceived level of hazard, likelihood of damage or loss, severity of the potential damage or loss, and probability of allowing the program when they saw each interface first (before seeing any interface) and when they saw it last (after seeing all the interfaces). Our results showed no significant difference between the last exposure to each interface and the first exposure. The lack of evidence that our design primed the participants and impacted their consideration of later warnings suggest that our results are valid.

The above analyses show that our study design was appropriate given our objectives, the diverse population that we wanted to study, and the feedback we received in our pilot testings.

4.5.3 Warning Preference

Most of our participants (40/60) preferred P-warnings; some (13 participants) noted that P-warnings provide them with a mental model of the functionality of a firewall, as P60 commented: “this one (C-warning) is just a warning of a firewall. [The] brick wall and the locked door is very good. It tells me the theory of the firewall.” Some participants also found P-warnings more intuitive (16 participants), and easier (37 participants) and faster (nine participants) to understand. P38 mentioned that when “multitasking, [such as] talking to your friends, this [P-warnings] is very effective. It tells you everything at a glance, you make less mistakes.” P18 also said something similar, “it just takes my time to read it [C-warnings], and at the end I do not know, OK, what? but, I understand this image instantly. I do not need to concentrate on every single thing in it.” Some (11 participants) also emphasized that P-warnings convey the risk and the consequences of allowing the program more clearly; as P32 said, “the top one [P-Warnings] is clear, it tells you what the risk is, and if it’s acceptable, if there’s a threat.” P51 also noted: “I like that one (P-warnings), especially that bandit’s outfit, trying to steal something, my data, can’t get any more clear than that.”

In addition, several participants (12) thought P-warnings grab attention better; while eight participants mentioned C-warnings are more ignorable: “you do not decide to see or not to see this [P-warnings], but you can choose to read or not to read this one [C-warnings]” (P18). Five participants also stated that P-Warnings are more universal, as P19 commented: “this one [P-Warning] is better, especially for old people that cannot see clearly or children that may not understand security, or those who do not know what a firewall is.”

Only one third of our participants (20) preferred C-warnings. Most of them thought C-warnings were more professional (11 participants) and they would take them more seriously (four participants): “it [P-warnings] is kind of childish” (P13). They also found C-warnings more informative (seven participants) and descriptive (two participants). Five participants noted they would understand C-warnings better. Two participants also mentioned C-warnings are more specific; they thought different people can have different interpretations for P-warnings. P2 also noted that a good feature of C-warnings is that they are text-based and users can search on the Internet by directly copying and pasting the text. P20 who had a high level of security knowledge mentioned: “I already knew how a firewall works, so I don’t need this image, but it is definitely helpful for those who know less.”

4.6 Discussion

Our findings suggest that supporting a mental model of physical security in firewall warnings could be a promising approach for improving users' comprehension of the warnings, as well as their perceived level of risk and intention for safe behavior. For most participants, our proposed warnings promoted a better mental model and understanding of the protection provided by a personal firewall. However, we noticed some misinterpretations of the warnings, as well. Some of the participants thought that the warnings were generated by their chat application because the scenario that we described for them was about using a chat application. This shows that context also plays a role in users' understanding of the warnings. Therefore, context of use should be considered in the design of the warnings.

A second implication of the role of context in the interpretation of the warnings is for the design of user studies. When evaluating the warnings, different usage contexts of the warnings and their possible impacts on the results should be considered in the study design. It is important to interpret the results based on the context in which participants consider themselves in. Taking context into account in our study might have provided us with different misinterpretations of our warnings.

Our results also show that the application of known metaphors, such as the bandit figure, in the warnings are very effective in conveying risk to the user. Our participants could relate the potential risks of the warnings to the risks from the physical world; this resulted in them better understanding the consequences of their potential actions. However, we had participants who mentioned they would take our warnings less seriously than the textual warnings. They attributed this to their personality and did not consider pictorial representations to be a professional way of communicating risk.

Another interesting finding of our study was that one third of our participants preferred C-warnings to our proposed warnings. A look at their demographics showed that all but one of these participants had a high or medium level of security knowledge and expertise. Furthermore, all the participants with a high level of security knowledge and expertise were in that group. These results indicate that the design of warnings may need to be customizable for different groups of users with different demographics.

It should be noted that our warning design was just one of the many possible designs. Our study was a first step in evaluating the effectiveness of using real world metaphors and users' mental models of security mechanisms in the design of security warnings. Our findings imply that this approach is promising for improving the design of security warnings.

4.7 Summary

We presented a user study in which we evaluated a novel approach for designing personal firewall warnings. We used an iterative process to visualize the functionality of a personal firewall based on a mental model of physical security and the metaphor of a physical firewall. We compared our warnings with those based on the warnings of one of the most popular personal firewalls. Our results showed that our proposed warnings facilitate comprehension of warning information; they helped participants develop a better mental model of the functionality of a personal firewall. They also better communicated the risk; with our warnings, participants had a better estimation of the level of hazard, likelihood of damage or loss, and the severity of potential damage or loss. They could also better describe the potential consequences of their intended actions. More importantly, our warnings increased the likelihood of their safe behavior in response to the warnings. They were also preferred by the majority of the participants.

Chapter 5

Conclusions

In this thesis, we presented three series of user studies performed in order to improve the usability of personal firewalls: (1) usability studies of the Windows Vista firewall, (2) a study of users' expectations, perceptions, and misconceptions of personal firewalls, and (3) an evaluation of firewall warnings designed based on a physical security mental model. We provide a summary of the findings and contributions of each study below.

- **Usability studies of the Windows Vista firewall**

  As a first step in our research, we performed a series of usability studies on the Microsoft Windows Vista firewall. Those studies revealed that the lack of an accurate mental model about the firewall's system model significantly contributed to users' errors when configuring the Vista firewall. We redesigned the user interface of the firewall to more accurately reflect its system model. The results of a laboratory study with a diverse set of 60 participants showed that good user interface design and helpful feedback could help users develop more effective mental models of the firewall, and improve their understanding of the firewall's configuration, resulting in fewer potentially dangerous errors. These studies showed the dangers of hidden complexities in security applications. Although hiding system features and operational details can make interfaces more usable, in the case of security applications complexity must be balanced against security. Our studies highlighted that security interfaces play a crucial role in providing users with an effective mental model of security applications, and therefore, in the correct configuration and effectiveness of those applications.

- **Users' expectations, perceptions, and misconceptions of personal firewalls**

  We conducted semi-structured interviews with a diverse set of 30 participants to gain an understanding of their knowledge, expectations, perceptions, and misconceptions of personal firewalls.

The first contribution of this part of our research is our qualitative analysis of the data, which revealed that participants with different levels of security knowledge have different understandings about the functionality of a personal firewall. Most participants were not aware of the benefits of the protection provided by a personal firewall; they were not even aware of the existence of a personal firewall on their computer. Our results also showed that context is important for several participants when making security decisions. We found different contextual factors that were important to those participants; however, we also found that they did not have the necessary knowledge to determine the required level of security based on the contextual factors. Our results also showed that the interaction of most of our participants with personal firewalls was limited to responding to firewall warnings; however, many of them had problems understanding and making informed decision about these warnings. As a result, they tended to ignore the firewall warnings or even turn their personal firewall off or completely un-install it.

Our second contribution is the examination of the implications of our findings for the design of personal firewalls. To have more usable and effective personal firewalls, we recommended providing firewalls in an integrated solution with other security software. We also recommended providing personal firewalls with facilities to determine the users' level of security knowledge and expertise so that the firewall can adjust its behavior based on the different requirements and expectations. Moreover, we proposed that personal firewalls should provide users with different levels of protection based on their context, and also with information to help them make informed security decisions in each context. Finally, we provided recommendations for designing effective methods of interaction between the firewall and the user such as providing automation, warnings, and notices.

- **A physical security mental model for personal firewall warnings**

  The most important contribution of this part of our research is the proposal of a novel design for personal firewall warnings. We proposed a firewall warning design in which the functionality of a personal firewall is visualized based on the users' mental model of firewalls, i.e., physical security. Our other contribution is the evaluation of our proposed warnings. We performed a study with a diverse set of 60 participants. The results showed that our warnings facilitated the comprehension of warning information, better communicated the risk, and increased the likelihood of safe behav-

> ior as compared to warnings based on those from a popular personal firewall. Moreover, the new warnings provided participants with a better understanding of both the functionality of a personal firewall and the consequences of their actions. These findings imply that our approach is promising for improving the design of security warnings. Our study highlights that considering users' mental models of security mechanisms in the design of security interfaces can lead to interfaces that are more understandable for users and help them make informed security decisions.

While the focus of this thesis was on personal firewalls and firewall warnings, we believe that our research will benefit the broader community of usable security, especially those who are working on the design of security interfaces for non-expert users.

5.1 Future Work

There are several directions for future research.

An open question is whether there needs to be separate interfaces for novice and expert users of security applications. In our usability studies of the Vista firewall, we found no obvious differences in the results attributable to the participants' computer and security knowledge and experience; regardless of their backgrounds, most participants struggled with understanding the configuration of the Vista firewall when they used its simple interface. However, in our second user study we found that participants with different levels of security knowledge and experience have different expectations, perceptions, and misconceptions from their personal firewall. In our study of firewall warnings, we also found that our proposed warnings were preferred by those participants with a relatively low level of security knowledge and expertise, but not by those with a high level of security knowledge and expertise. This may suggest that security applications and their interfaces should be customizable. However, further research is required to find which user attributes are important when designing and evaluating security applications and interfaces, and how those attributes can affect the design of security applications and interfaces.

Another interesting direction for future research is to study how considering different contexts of use can affect the design of security applications and their interfaces. Our user study of the Vista firewall showed that if the context of use is considered in the design of a security application, its impact on the security state should be revealed to the user; in our study of users' expectations and perceptions of personal firewalls, we realized that context is important for several participants. Additional research is required to understand how the context of use affects users' security needs and requirements and how that should be applied in the design of security applications and interfaces.

Based on the findings of our study of users' knowledge, expectations, perceptions, and misconceptions of personal firewalls, we provided several recommendations for the design of personal firewalls, security warnings, and security applications in general. More research is required for a concrete implementation of each of those recommendations and their formal evaluation.

Our study of the firewall warnings was based on self-reported data. We did not evaluate users' behavior in response to those warnings. More user studies are required to evaluate the effectiveness of those warnings based on users' behavior. Moreover, the relationship between the participants' demographics and the suitability of the choice of metaphors is not clear cut. Future research can examine how the choice of different metaphors can affect the effectiveness of security warnings.

Bibliography

Arjmandi, P., Boeck, R., Raja, F., and Viswanathan, G. (2007). Usability of Vista firewall: A labratory user study. EECE412 course project at the University of British Columbia.

Asgharpour, F., Liu, D., and Camp, L. J. (2007). Mental models of security risks. In *FC'07/USEC'07: Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, pages 367–377, Berlin, Heidelberg. Springer-Verlag.

Avolio, F. (1999). Firewalls and Internet security, the second hundred (Internet) years. *The Internet Protocol Journal*, 2(2):24–32.

Beck, S. (1962). The Q-sort method in personality assessment and psychiatric research. *Archives of General Psychiatry*, 7(3):230.

Berson, J. (2005). ZoneAlarm: Creating usable security products for consumers. In Cranor, L. F. and Garfinkel, S., editors, *Security and Usability: Designing Secure Systems that People Can Use*, chapter 27, pages 563–575. O'Reilly Media, Inc.

Besmer, A., Watson, J., and Lipford, H. R. (2010). The impact of social navigation on privacy policy configuration. In *SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–10, New York, NY, USA. ACM.

Bhamra, S. (2010). The 2010 Personal Firewall Robustness Evaluation. In *8th Australian Digital Forensics Conference*, page 18.

Bishop, M. (2003). What is computer security? *IEEE Security and Privacy*, 1(1):67–69.

Camp, L., Asgharpour, F., Liu, D., and Bloomington, I. (2007). Experimental Evaluations of Expert and Non-expert Computer Users? Mental Models of Security Risks. *Proceedings of WEIS 2007*.

Card, S. and Moran, T. (1986). User technology—from pointing to pondering. In *Proceedings of the ACM Conference on The history of personal workstations*, pages 183–198, New York, NY, USA. ACM.

Chebium, A., Jaferian, P., Kaviani, N., and Raja, F. (2008). Usability analysis of Vista firewall. CSCP544 course project at the University of British Columbia.

Chen, G. and Kotz, D. (2000). A survey of context-aware mobile computing research. Technical Report TR2000-381, Dartmouth College.

Chiasson, S., van Oorschot, P. C., and Biddle, R. (2007). Even experts deserve usable security: Design guidelines for security management systems. In *SOUPS Workshop on Usable IT Security Management (USM)*, pages 1–4, Pittsburgh, PA.

ConsumerSearch (2010). Personal firewall software review. http://www.consumersearch.com/firewalls.

Cranor, L. F. (2003). Designing a privacy preference specification interface: A case study. In *Proceedings of the Workshop on Human-Computer Interaction and Security Systems*, page 4 pages.

Cranor, L. F. (2005). Towards usable web privacy and security. In *Proceedings of the 14th international conference on World Wide Web*, WWW '05, pages 352–352, New York, NY, USA. ACM.

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. In *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security*, pages 1–15, Berkeley, CA, USA. USENIX Association.

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J., and Filho, R. S. (2005). Two experiences designing for effective security. In *SOUPS '05: Proceedings of the 2005 Symposium On Usable Privacy and Security*, pages 25–34, Pittsburgh, Pennsylvania. ACM.

DiGioia, P. and Dourish, P. (2005). Social navigation as a model for usable security. In *SOUPS '05*, pages 101–108, Pittsburgh, Pennsylvania. ACM.

Dourish, P., Grinter, R. E., de la Flor, J. D., and Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401.

Downs, J. S., Holbrook, M. B., and Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 79–90, New York, NY, USA. ACM.

Ecclestone, R. (2001). Acsac 2001 review. *Computers & Security*, 21(1):47 – 60.

Edwards, W. K., Poole, E. S., and Stoll, J. (2007). Security automation considered harmful? In *NSPW'07: Proceedings of the New Security Paradigms Workshop*, White Mountain, New Hampshire.

Egelman, S., Cranor, L. F., and Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *CHI '08: Proc. of the SIGCHI conf. on Human factors in Computing Systems*, pages 1065–1074, New York, NY, USA. ACM.

Egelman, S., King, J., Miller, R. C., Ragouzis, N., and Shehan, E. (2007). Security user studies: methodologies and best practices. In *CHI Extended Abstracts*, pages 2833–2836. ACM.

Eichin, M. W. and Rochlis, J. A. (1989). With microscope and tweezers: An analysis of the internet virus of november 1988. *IEEE Symposium on Security and Privacy*, page 326.

Friedman, B., Hurley, D., Howe, D. C., Nissenbaum, H., and Felten, E. (2002). Users' conceptions of risks and harms on the web: a comparative study. In *CHI '02: CHI '02 extended abstracts on Human factors in computing systems*, pages 614–615, New York, NY, USA. ACM.

Geng, W., Flinn, S., and DeDourek, J. (2005). Usable firewall configuration. In *PST '05: Proceedings of the 3rd Annual Conference on Privacy, Security and Trust*, page 11 pages.

Giacoppo, S. (2001). Development methods: User needs assessment & task analyses. http://otal.umd.edu/hci-rm/dvlpmeth.html.

Gizmo's Freeware Reviews (2010). Best software firewalls for maximum protection and greater user involvement. http://www.techsupportalert.com/best-free-firewall.htm.

Goecks, J., Edwards, W. K., and Mynatt, E. D. (2009). Challenges in supporting end-user privacy and security management with social navigation. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, New York, NY, USA. ACM.

Grinter, R. E. and Smetters, D. (2003). Three challenges for embedding security into applications. In *CHI Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, FL.

Gross, J. B. and Rosson, M. B. (2007). Looking for trouble: understanding end-user security management. In *CHIMIT '07: Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, page 10, New York, NY, USA. ACM.

Hazari, S. (2005). Perceptions of end-users on the requirements in personal firewall software: An exploratory study. *The Journal of Supercomputing*, 17(3):47–56.

Herzog, A. and Shahmehri, N. (2007). Usability and security of personal firewalls. *New Approaches for Security, Privacy and Trust in Complex Environments*, pages 37–48.

Hole, K., Dyrnes, E., and Thorsheim, P. (2005). Securing wi-fi networks. *Computer*, 38(7):28–34.

Ingham, K. and Forrest, S. (2002). A history and survey of network firewalls. Technical report, University of New Mexico.

Jaferian, P. (2008). Usability study of Windows Vista's firewall. EECE512 course project at the University of British Columbia.

Johnson, R. (1997). Examining the validity structure of qualitative research. *Education*, 118(2).

Johnston, J., Eloffa, J. H. P., and Labuschagneb, L. (2003). Security and human computer interfaces. *Computers and Security*, 22:675–684.

Jonassen, D. and Cho, Y. H. (2008). *Understanding Models for Learning and Instruction*, chapter Externalizing Mental Models with Mindtools, pages 145–159. Springer US.

Jungermann, H., Schutz, H., and Thuring, M. (1988). Mental models in risk assessment: Informing people about drugs. *Risk Analysis*, 8(1):147–155.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D. (2009). "when i am on wi-fi, i am fearless": privacy concerns & practices in eeryday wi-fi use. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems*, pages 1993–2002, New York, NY, USA. ACM.

Leonard, S., Otani, H., and Wogalter, M. (1999). Comprehension and memory. *Warnings and risk communication*, pages 149–187.

Liu, D., Asgharpour, F., and Camp, L. (2008). Risk Communication in Security Using Mental Models. *Usable Security*, 7.

McDermott, P. (2000). Personal firewalls...one more step towards comprehensive security. *Network Security*, 2000(11):11 – 14.

McGrath, J. E. (1995). Methodology matters: doing research in the behavioral and social sciences. *Human-computer interaction: toward the year 2000*, pages 152–169. Morgan Kaufmann Publishers Inc.

McGrenere, J., Baecker, R. M., and Booth, K. S. (2002). An evaluation of a multiple interface design solution for bloated software. In *CHI '02: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 164–170, New York, NY, USA. ACM.

McKechnie, J. (1983). *Webster's new universal unabridged dictionary*. Dorset & Baber.

Microsoft (2008a). Microsoft's annual revenue reaches $60 billion. http://www.microsoft.com.

Microsoft (2008b). Windows firewall with advanced security - content roadmap. http://technet.microsoft.com.

Microsoft (2008c). Windows Vista Help: Choosing a network location.

Microsoft (2008d). Windows Vista Help: What is a firewall.

Morgan, M. (2002). *Risk communication: A mental models approach*. Cambridge University Press.

Motiee, S., Hawkey, K., and Beznosov, K. (2010). Do windows users follow the principle of least privilege? investigating user account control practices. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*, pages 1–13, New York, NY, USA. ACM.

Nielsen, J. (1993). *Usability Engineering*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

Nielsen, J. (1995). Card sorting to discover the users' model of the information space. http://www.useit.com/papers/sun/cardsort.html.

Oppliger, R. (1997). Internet security: firewalls and beyond. *Commun. ACM*, 40:92–102.

PCmag (2010). Up-to-date coverage and product reviews of firewall software. http://www.pcmag.com/.

PCWorld (2010a). Comodo firewall is a superb security program. http://www.pcworld.com/article/188008/comodo_firewall_is_a_superb_security_program_if_you_ignore_its_bundled_software.html.

PCWorld (2010b). Popular in firewalls. http://www.pcworld.com/downloads/file/fid,63762-order,4/description.html.

Reeder, R. W., Bauer, L., Cranor, L. F., Reiter, M. K., Bacon, K., How, K., and Strong, H. (2008). Expandable grids for visualizing and authoring computer security policies. In *Proc. CHI '08*, pages 1473–1482, New York, NY, USA. ACM.

Rode, J., Johansson, C., DiGioia, P., Filho, R. S., Nies, K., Nguyen, D. H., Ren, J., Dourish, P., and Redmiles, D. (2006). Seeing further: extending visualization as a basis for usable security. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 145–155, New York, NY, USA. ACM.

Ronnfeldt, C. (1997). Three generations of environment and security research. *Journal of Peace Research*, 34(4):473–482.

Sandelowski, M. (2000). Whatever happened to qualitative description? *Research in Nursing & Health*, 23(4):334–340.

Smith, S. (2003). Humans in the loop: human-computer interaction and security. *Security & Privacy, IEEE*, 1(3):75–79.

Sotirakopoulos, A., Hawkey, K., and Beznosov, K. (2010). "I did it because I trusted you": Challenges with the Study Environment Biasing Participant Behaviours. In *SOUPS Usable Security Experiment Reports (USER) Workshop*.

Stewart, D. W. and Martin, I. M. (1994). Intended and unintended consequences of warning messages: A review and synthesis of empirical research. *Journal of Public Policy and Marketing*, 13(1):1–19.

Stoll, J., Tashman, C. S., Edwards, W. K., and Spafford, K. (2008). Sesame: informing user security decisions with system visualization. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 1045–1054, New York, NY, USA. ACM.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. (2009). Crying Wolf: An empirical study of SSL warning effectiveness. In *Proceedings of 18th USENIX Security Symposium*, pages 399–432.

TopTenReviews (2010). TopTenReviews: 2010 personal firewall software review product comparisons. http://personal-firewall-software-review.toptenreviews.com/.

Wash, R. (2008). Mental models of home computer security. In *SOUPS EA '08: Proceedings of the fourth Symposium on Usable Privacy and Security*, pages 1–1.

Wash, R. (2010). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16, New York, NY, USA. ACM.

Whitten, A. and Tygar, J. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *The 9th USENIX Security Symposium*, pages 169–183.

Whitten, A. and Tygar, J. (2003). Safe staging for computer security. In *the Workshop on Human-Computer Interaction and security Systems*, page 4 pages, Ft. Lauderdale, FL.

Windows Security Center (2010). Explore the features: Windows security center. http://www.microsoft.com/windows/windows-vista/features/security-center.aspx.

Wogalter, M., Conzola, V., and Smith-Jackson, T. (2002). Research-based guidelines for warning design and evaluation. *Applied Ergonomics*, 33(3):219–230.

Wolff, J. S. and Wogalter, M. S. (1998). Comprehension of pictorial symbols: Effects of context and test method. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 40:173–186(14).

Wool, A. (2004). The use and usability of direction based filtering in firewalls. *Computers and Security*, 37:459–468.

Xia, H. and Brustoloni, J. (2004). Detecting and blocking unauthorized access in Wi-Fi networks. *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications*, pages 795–806.

Yee, K.-P. (2002). User interaction design for secure systems. In *ICICS '02: Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290, London, UK. Springer-Verlag.

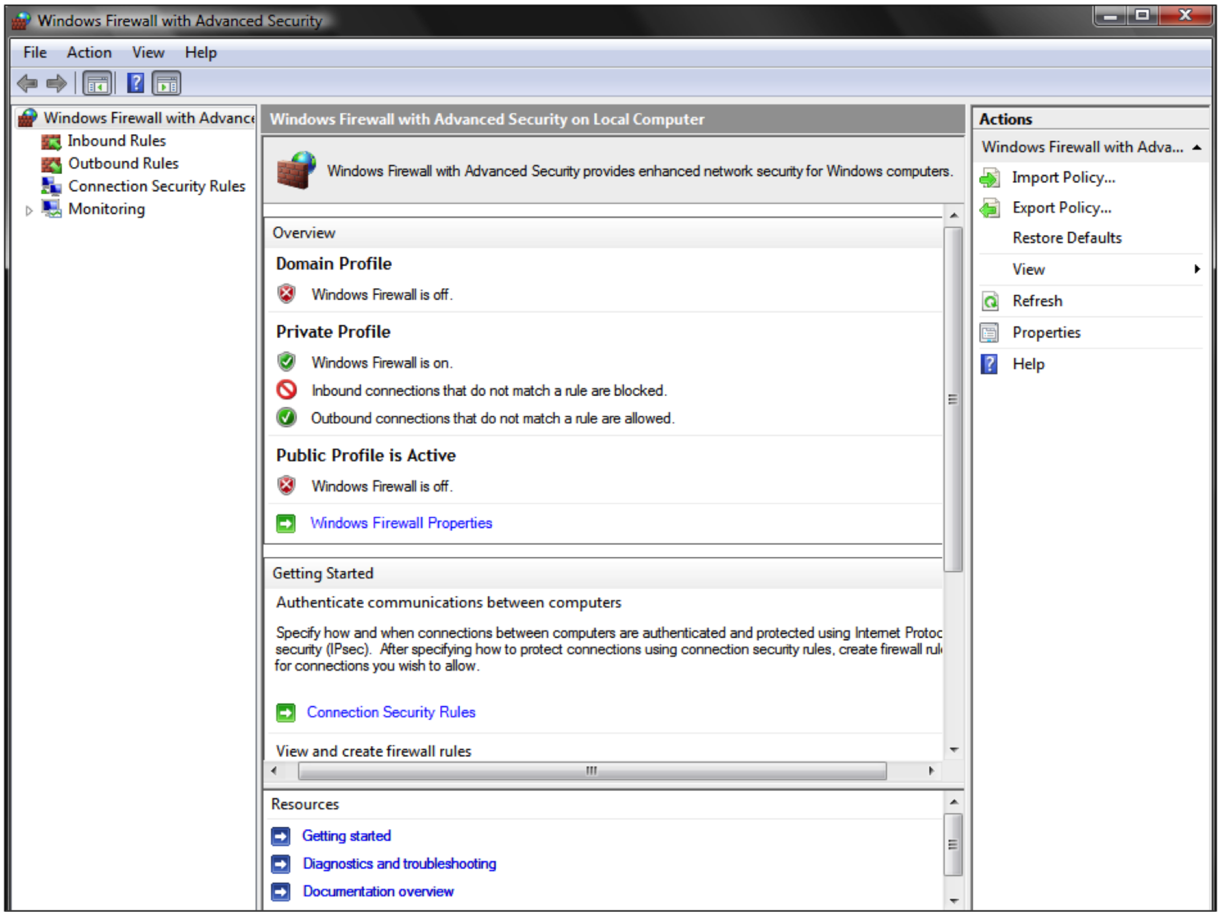
Yee, K.-P. (2004). Aligning security and usability. *Security & Privacy, IEEE*, 2(5):48–55.

Young, S. and Lovvoll, D. (1999). Intermediate processing stages: Methodological considerations for research on warnings. *Warnings and risk communication*, pages 27–52.

Zurko, M. E., Kaufman, C., Spanbauer, K., and Bassett, C. (2002). Did you ever have to make up your mind? what notes users do when faced with a security decision. In *ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference*, pages 371–381, Washington, DC, USA. IEEE Computer Society.

Appendix A

Advanced Interface of Windows Vista Personal Firewall



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides enhanced network security for Windows computers.

Overview

Domain Profile

Windows Firewall is off.

Private Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Public Profile is Active

Windows Firewall is off.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Specify how and when connections between computers are authenticated and protected using Internet Protoc security (IPsec). After specifying how to protect connections using connection security rules, create firewall rul for connections you wish to allow.

Connection Security Rules

View and create firewall rules

Resources

Getting started

Diagnostics and troubleshooting

Documentation overview

Figure A.1: Advanced interface of the Vista firewall.

Appendix B

First Formative Study Warnings

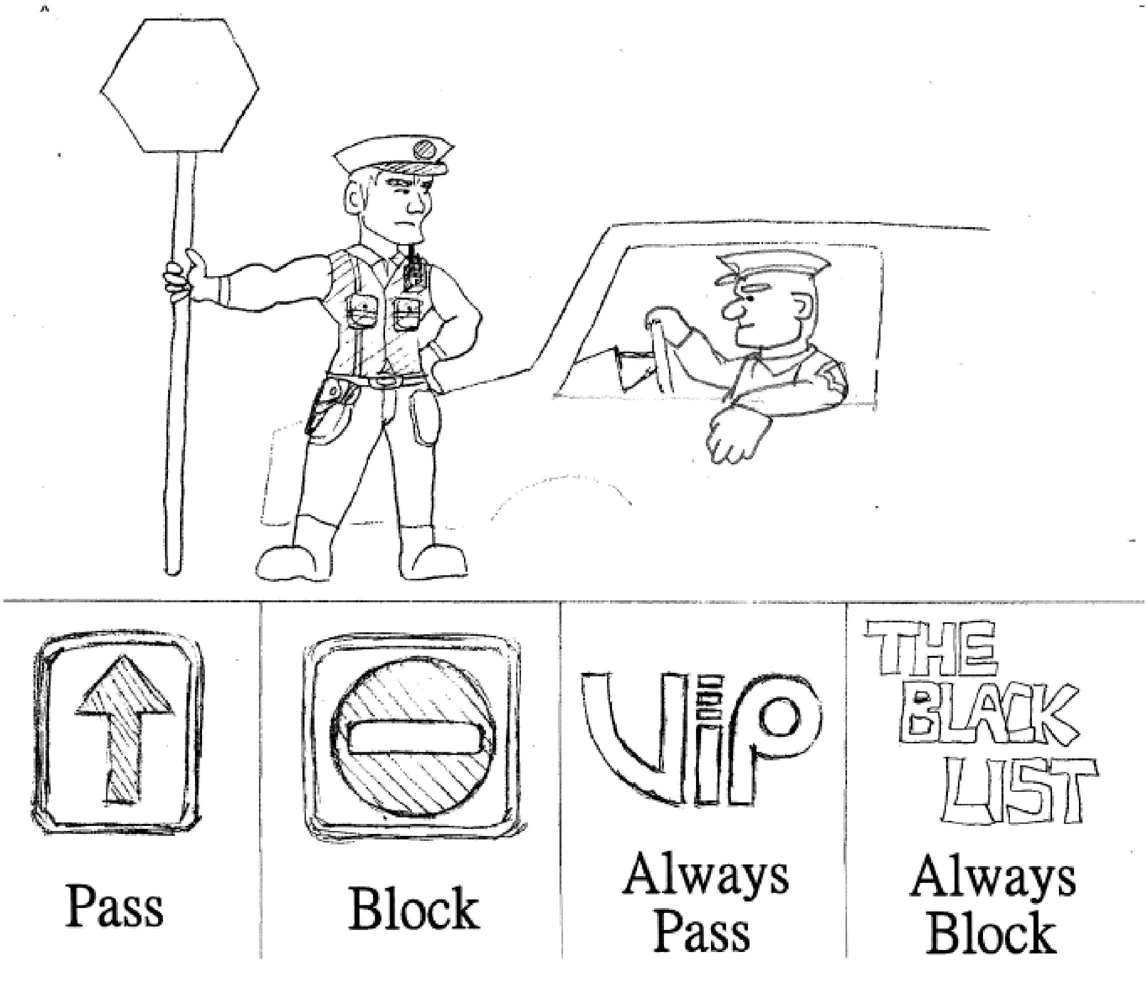


Figure B.1: Firewall warning based on physical security by a policeman (For safe applications).

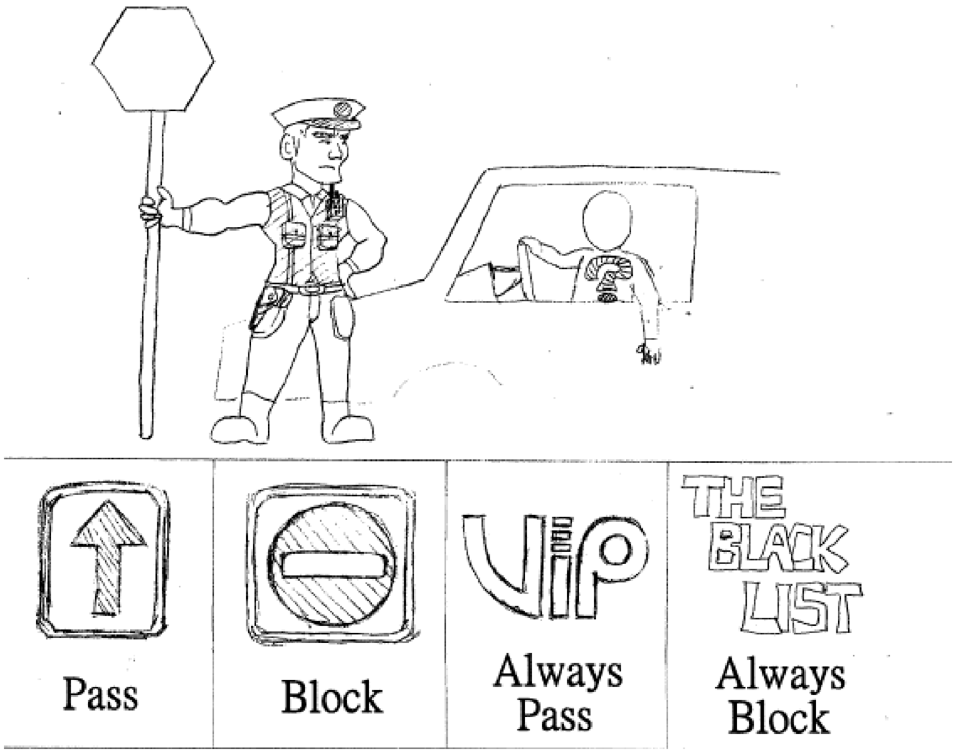


Figure B.2: Firewall warning based on physical security by a policeman (For unrecognized applications).

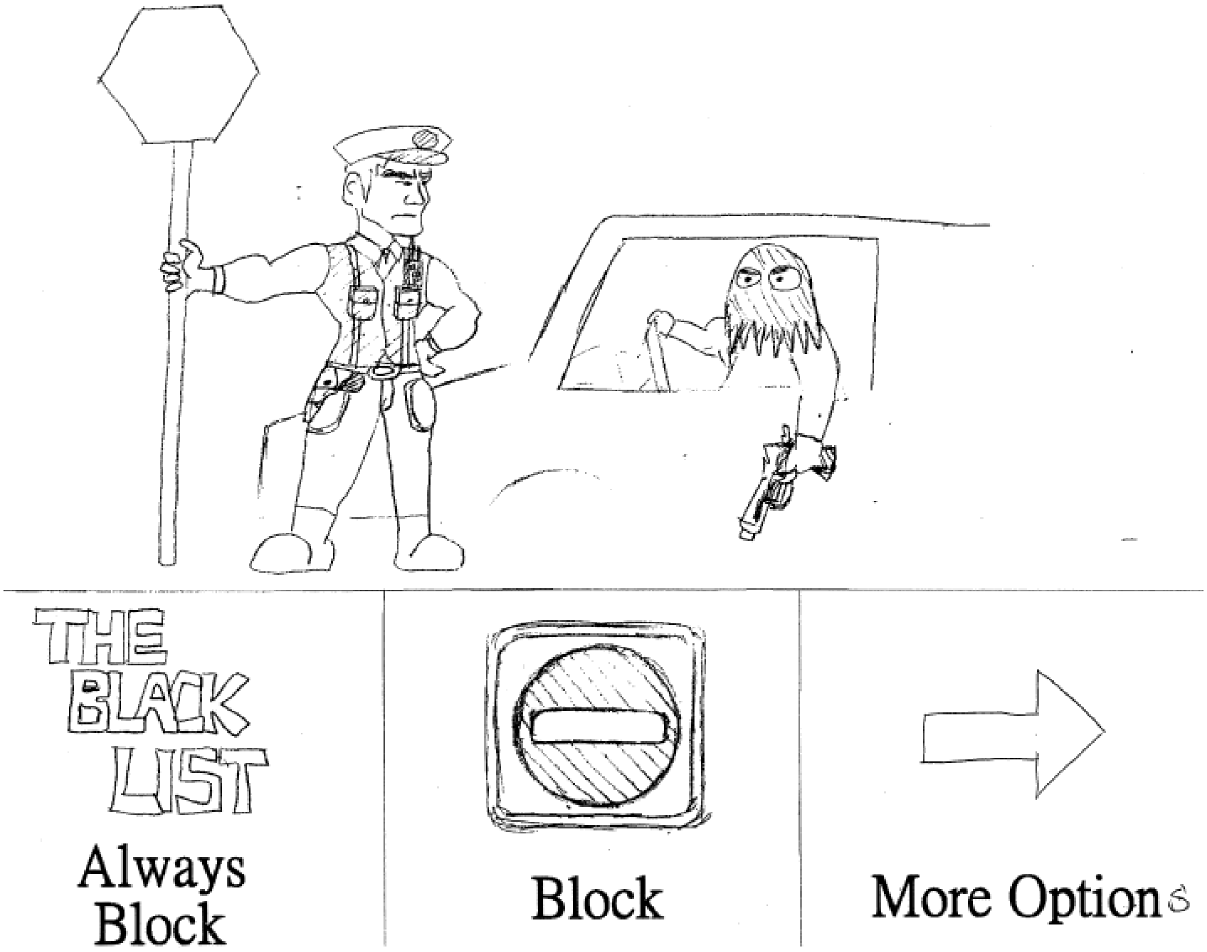


Figure B.3: Firewall warning based on physical security by a policeman (For malicious applications).

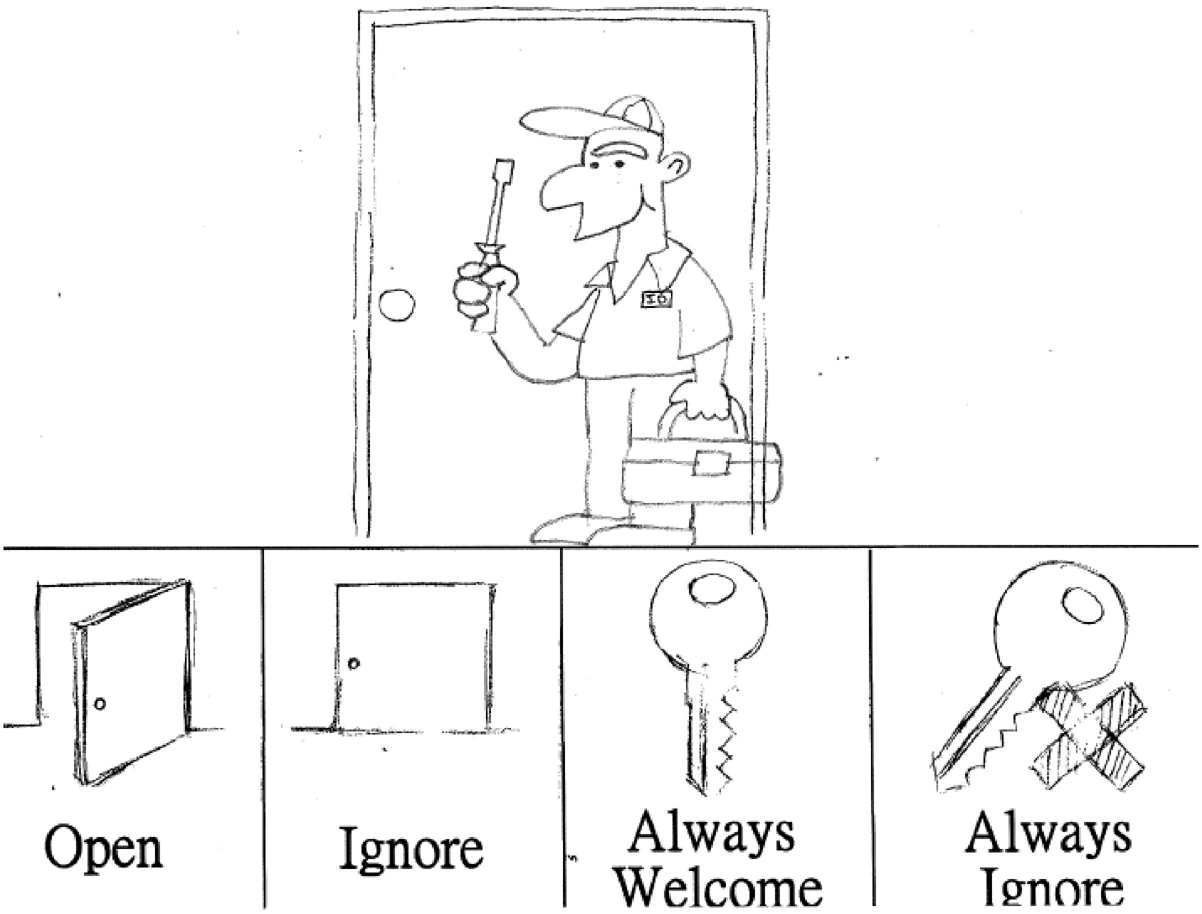


Figure B.4: Firewall warning based on physical security by a door (For safe applications).

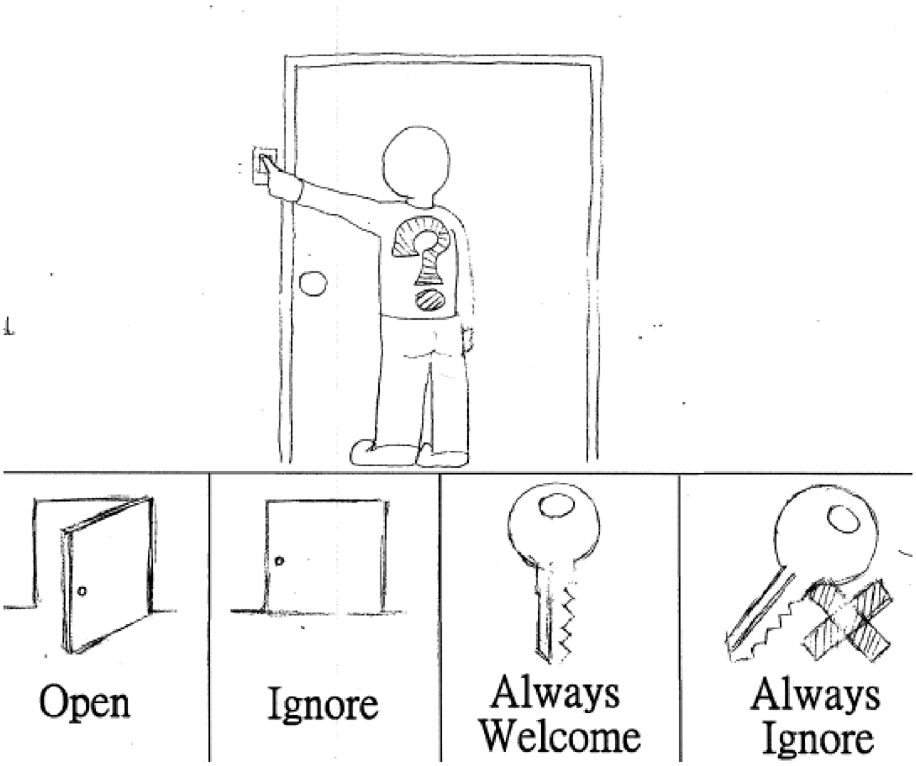


Figure B.5: Firewall warning based on physical security by a door (For unrecognized applications).

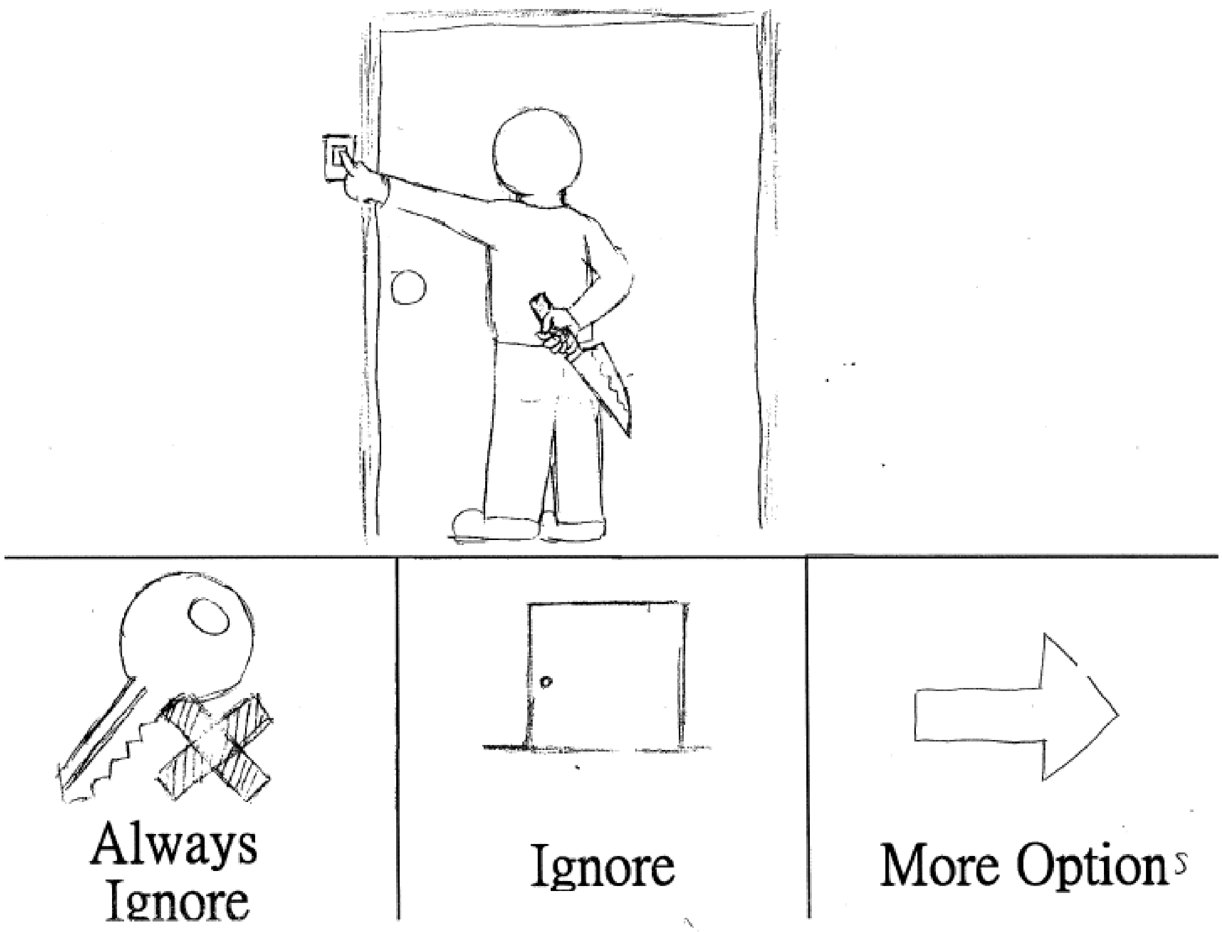


Figure B.6: Firewall warning based on physical security by a door (For malicious applications).

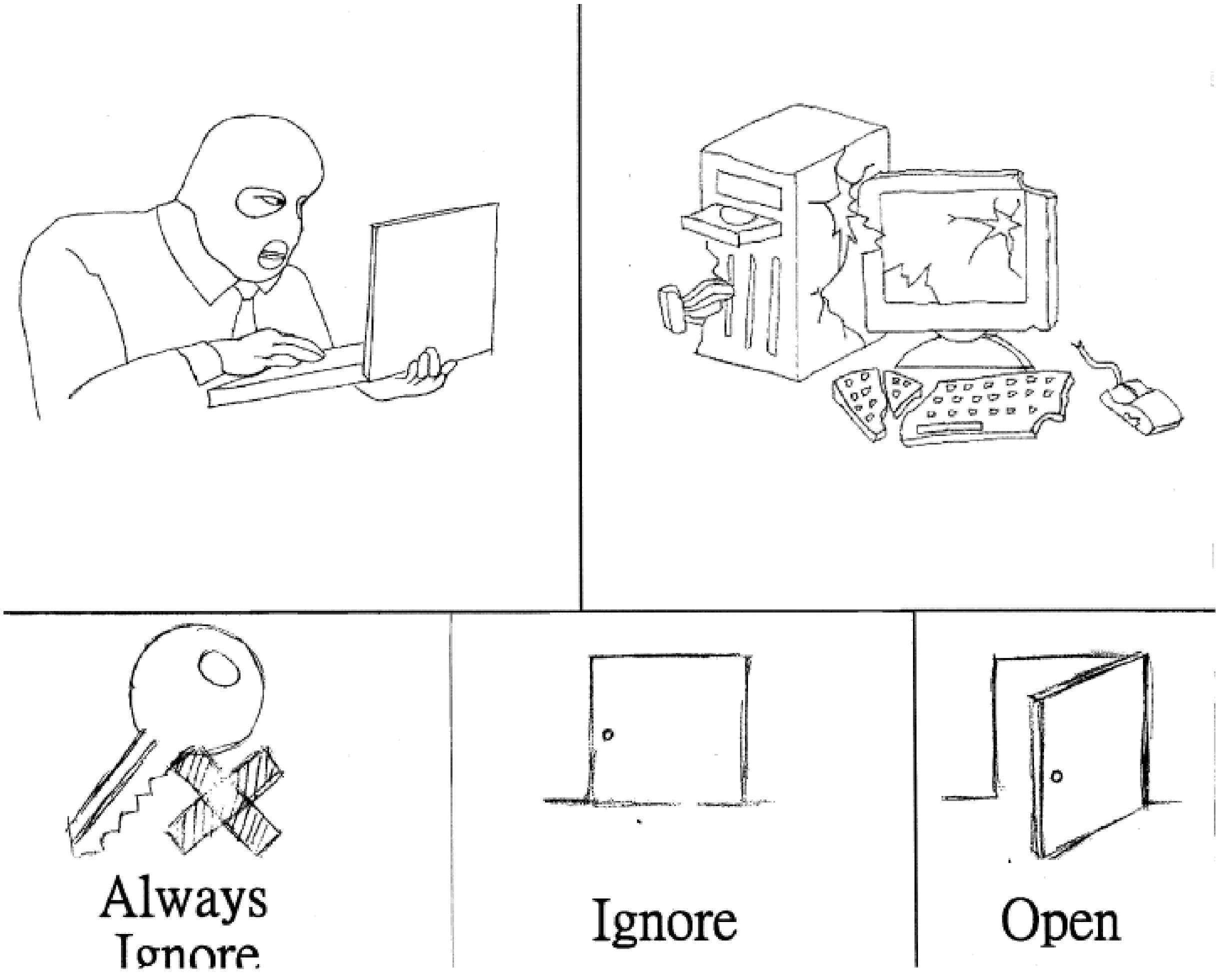


Figure B.7: An interface for showing the consequences of allowing a malicious application.

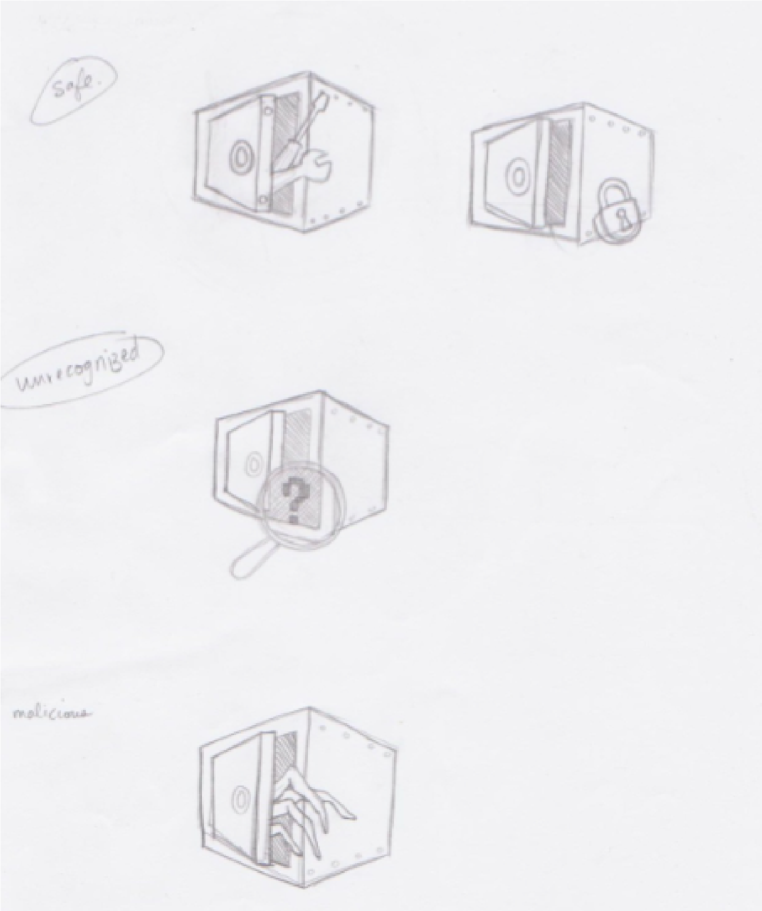


Figure B.8: Firewall warning based on physical security by a safe.

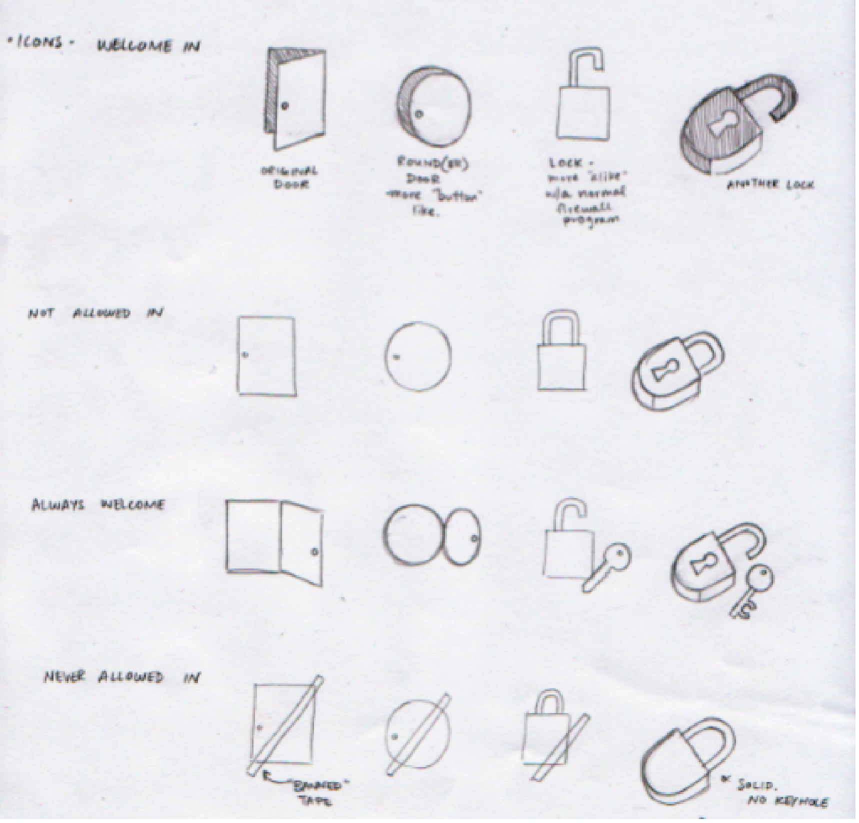
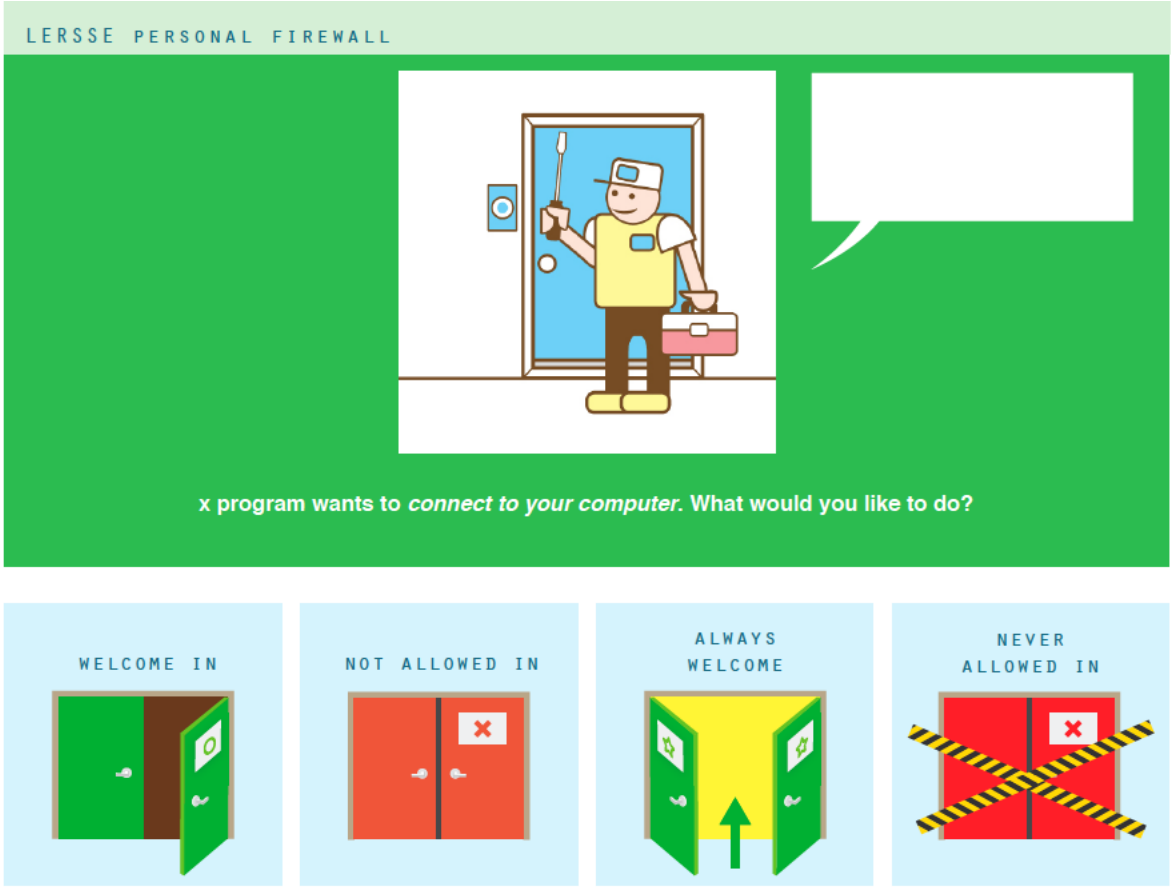


Figure B.9: A sample of our initial designs for different actions.

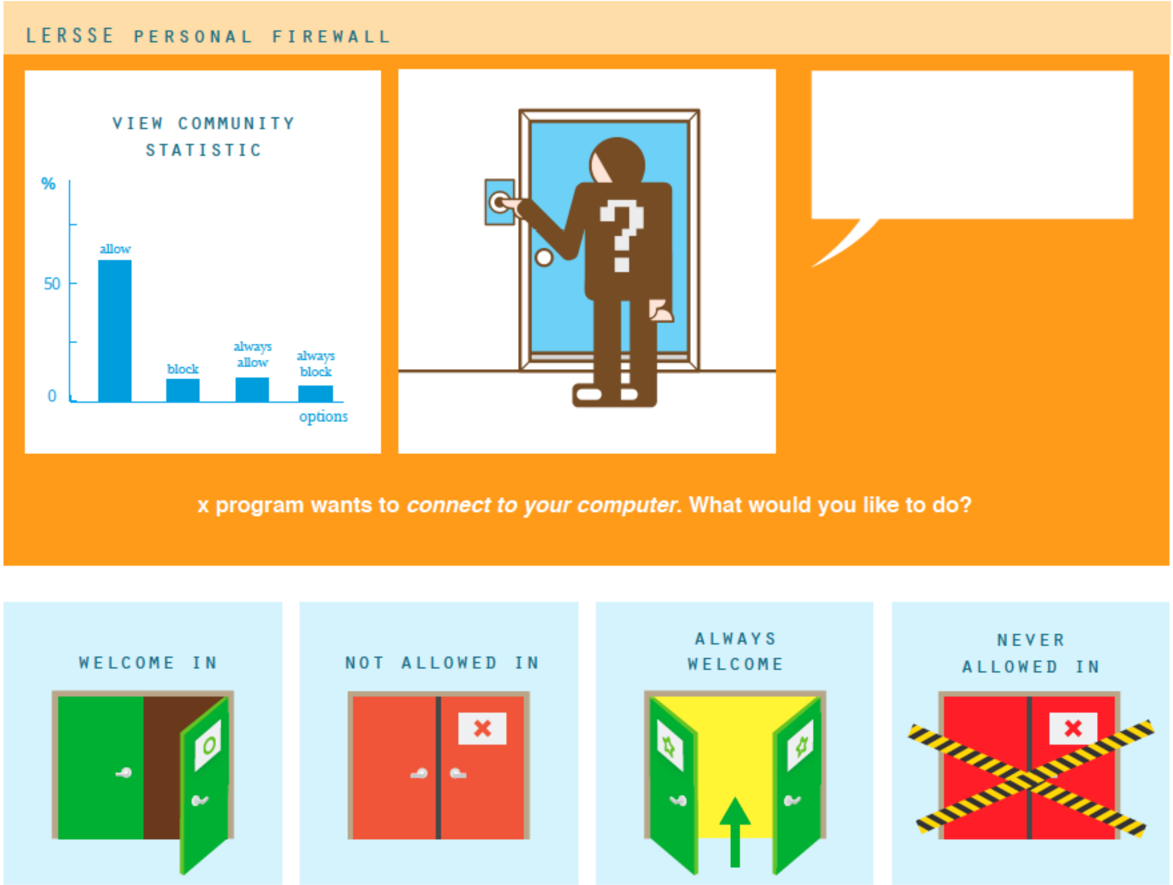
Appendix C

Second Formative Study Warnings



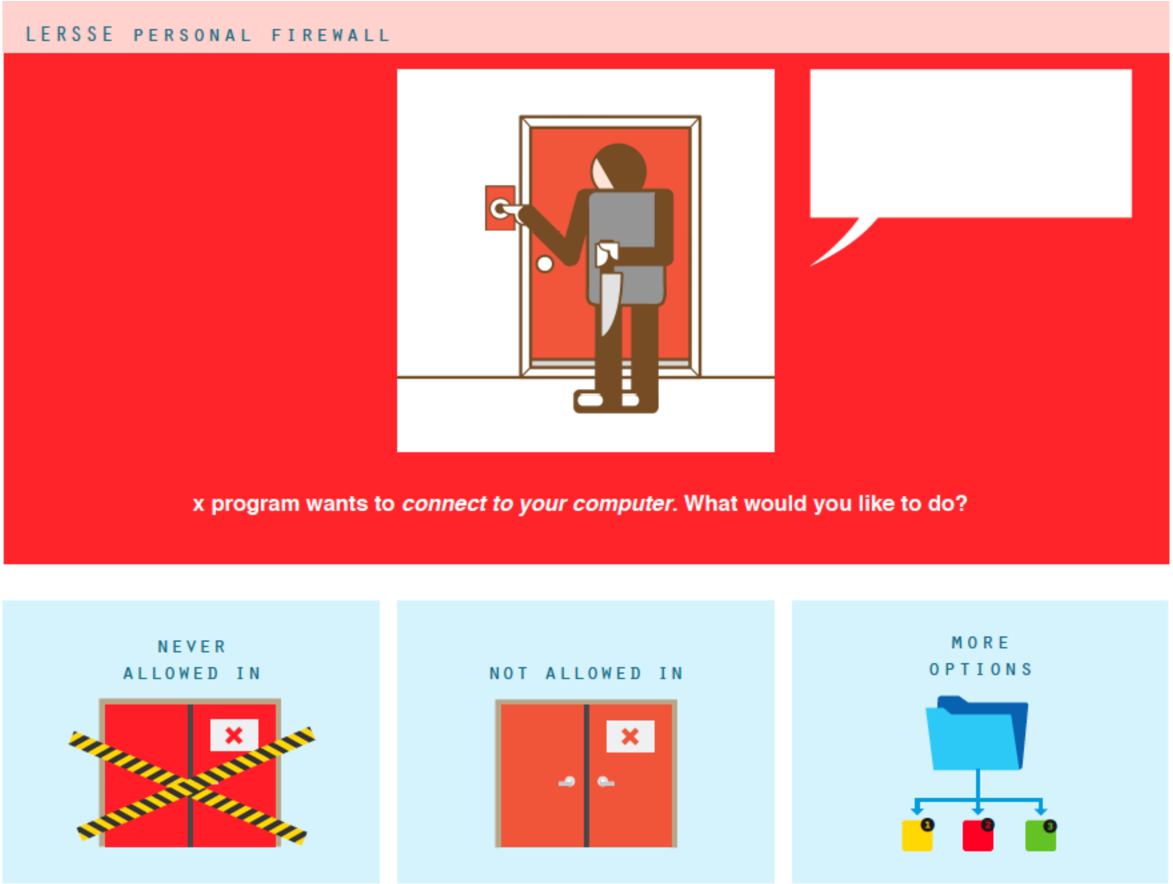
x program wants to *connect to your computer*. What would you like to do?

Figure C.1: Firewall warning based on physical security by a door (For safe applications).



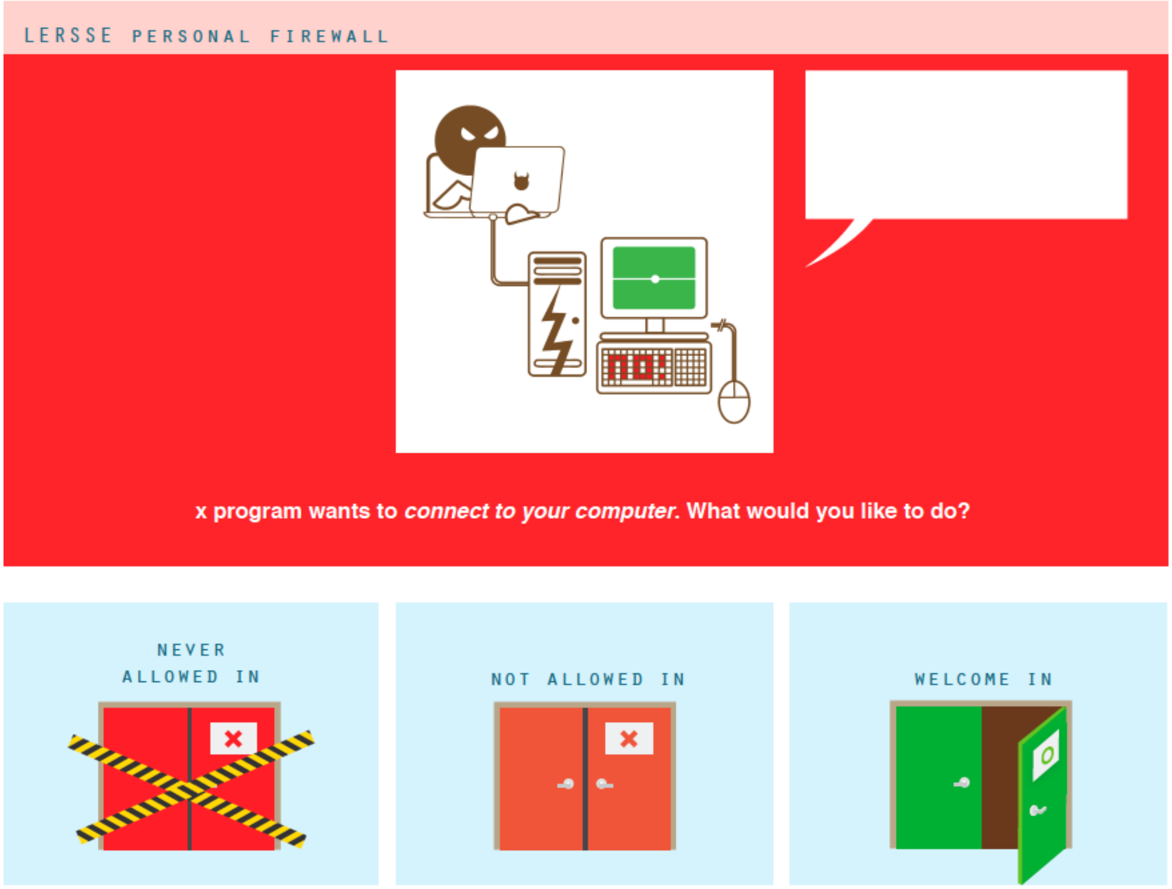
x program wants to *connect to your computer*. What would you like to do?

Figure C.2: Firewall warning based on physical security by a door (For unrecognized applications).



x program wants to *connect to your computer*. What would you like to do?

Figure C.3: Firewall warning based on physical security by a door (For malicious applications).



x program wants to *connect to your computer*. What would you like to do?

Figure C.4: An interface for showing the consequences of allowing a malicious application.

Appendix D

Initial Sketch of the Final Warning Design

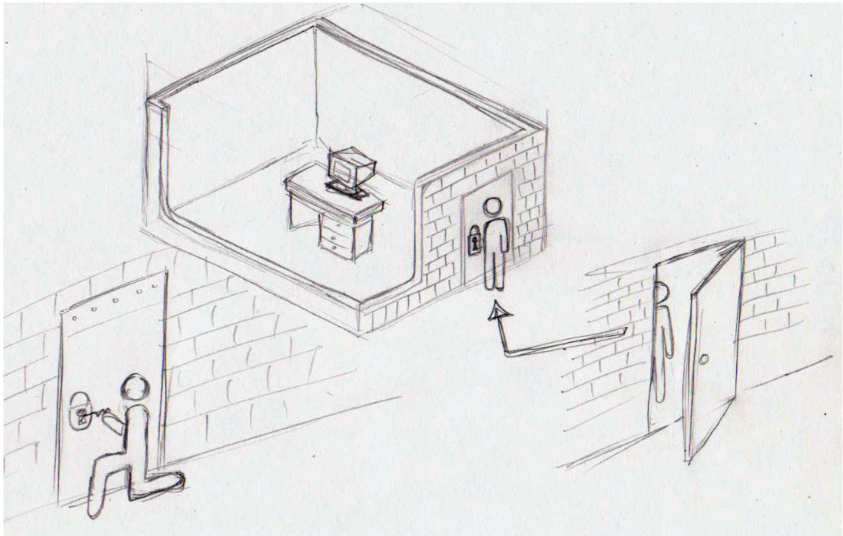


Figure D.1: The first sketch of our final design.