Investigating an Appropriate Design for Personal Firewalls

Fahimeh Raja
Department of Electrical & Computer Engineering
The University of British Columbia
Vancouver, BC, Canada
fahimehr@ece.ubc.ca

Kirstie Hawkey
Department of Electrical & Computer Engineering
The University of British Columbia
Vancouver, BC, Canada
hawkey@ece.ubc.ca

Konstantin Beznosov
Department of Electrical & Computer Engineering
The University of British Columbia
Vancouver, BC, Canada
beznosov@ece.ubc.ca

Kellogg S. Booth
Department of Computer Science
The University of British Columbia
Vancouver, BC, Canada
ksbooth@cs.ubc.ca

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04.

Abstract

Personal firewalls are an important aspect of security for home computer users, but little attention has been given to their usability. We conducted semi-structured interviews to understand participants' knowledge, requirements, expectations, and misconceptions for personal firewalls. Analysis of 10 interviews shows that different design decisions (i.e., level of automation, multiple profile settings) are appropriate for users with different levels of security knowledge and experience.

Keywords

Usable security, personal firewall.

ACM Classification Keywords

H.5.2 Information Interfaces and Presentation: User Interfaces-User-centered design; D.4.6 Software: Security and Protection-Information flow controls

General Terms

Design, Human Factors, Security

Introduction

Since the introduction of enterprise-level firewalls in the late 1980s, firewalls have been an important aspect of security. There are seven types of firewalls [11]; we focus on *personal firewalls,* designed for non-experts. Personal firewalls are "the first line of defense" for personal computers [7] and are found in mainstream operating systems. Personal firewalls check the traffic

Table 1: Demographics of all participants to date.

Demographics		N
Gender	Female	12
	Male	14
Student	Yes	14
	No	12
Computer expertise	Basic	11
	Advanced	15
Security knowledge & expertise	Low	10
	Medium	11
	High	5
Age (years)	Range	20..37
	Mean	25.5

Table 2: Six security tasks used to assess participants' security knowledge and expertise.

Tasks
Installing updates
Scanning for viruses, spyware, and other potentially unwanted software
Changing security settings of Internet browsers
Deleting browsing history and cookies
Setting different security controls for different users
Managing browsing add-ons

flowing between a computer and the network and, based on settings, allow or block elements of traffic. The protection provided by firewalls depends on their correct configuration [6]; therefore, usability is key.

Prior research has considered the usability of personal firewalls. Johnston et al. [7] performed a heuristic evaluation of the Windows XP personal firewall and proposed improvements for its interface (e.g., visibility of system features and status, interface learnability). Herzog and Shahmehri [6] performed a cognitive walk-through of 13 personal firewalls; their results highlight the need to convey firewall designs to users. Hazari [5] examined factors that affect selection of a personal firewall in an organization. Ease-of-use was found to be a high priority for users, but was not clearly defined. Stoll et al. [10] studied novel visualizations of technical information in firewall-like security applications.

We previously performed a usability study of Windows Vista Firewall (VF) [8]. Its interface has three network locations that correspond to configuration profiles for the firewall: private (applied to home and work networks), public (applied to public networks), and domain (applied if the network administrator has specified domain settings). A profile is *automatically* applied depending on the network location detected. Our study revealed that hiding the effect of network context (location) on the security state of the firewall results in users' dangerous misunderstanding of the firewall configuration. Furthermore, revealing hidden network context helps users develop a more complete mental model of the firewall and its configuration. Interestingly, 65% of participants did not see the benefits of maintaining multiple profiles.

As users become increasingly mobile, it is important for them to be able to judge whether their computer is secure enough for the current context [1]. An open question from our earlier research [8] is whether a personal firewall should change profile settings based on the network context. More generally, it is important to assess if the current design model of personal firewalls is appropriate. Specifically, the goal of this study is to understand users' knowledge, requirements, expectations, and misconceptions for personal firewalls.

Study Protocol

To date, we have conducted one-hour semi-structured interviews with a diverse set of 26 participants from both the university and general community (Table 1). Interviews have been successfully employed in usable security research to gain insights about users' security perceptions and misconceptions [2]. Our interviews were conducted in a meeting room and were audio recorded to augment researcher notes. Participants first completed a background questionnaire. In order to assess their security knowledge and experience, we provided them with a list of six security tasks taken from the "Security Center" of Windows Vista (Table 2) and asked them to describe what they know about the tasks, their importance, and how often they do them.

To assess participants' perceptions and requirements of a security application such as a personal firewall, we showed them the picture in Fig. 1 and told them that the black box is security software that will be designed to protect their computer. We used a black box to avoid biasing their discussion to current firewall functionality. We asked questions in order to understand: 1) what expectations they have of such an application, 2) what they want to be protected by the application, 3) how they want to interact with the application (what level of automation and feedback they want to have), 4) if they need to have multiple profile settings for this application, 5) what factors affect their requirements and, 6) if the concept of network location is an appropriate differentiating factor for profiles. In all cases, we probed for their reasoning. We also explicitly asked questions about their knowledge of and experience with personal firewalls to determine if they know what a firewall is, what its purpose is, how it works, and how it can meet their security needs.

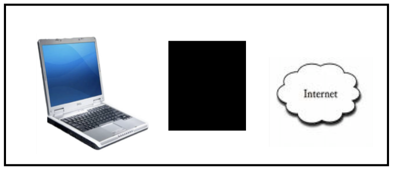

Figure 1. Security software as a black-box.

Table 3: Information about participants analyzed for this paper.

Group		**L**	**H**
Security level		Low	High
Comp. knowledge		Basic	Adv.
N		5	5
Age (mean)		26.4	26.6
Gender (M/F)		1/4	4/1
Student (Yes/No)		3/2	4/1
OS	XP	2	2
	Vista	3	3
	Mac	2	2
	Linux	0	4

Data Analysis

We transcribed the interviews and analyzed the data using qualitative description [9]. We applied qualitative methods because our goal is not to quantify users' requirements and expectations, but to understand and describe them. We iteratively coded the interviews to conceptualize the data. We began our analysis with a subset of participants at the low and high ends of the security knowledge and computer expertise spectrum.

Results

The results we report here are based on our initial analysis of 10 interviews from 5 low knowledge (group L: L1..L5) and 5 high knowledge (group H: H1..H5) participants (see Table 3 for demographics).

Knowledge about a Personal Firewall and its protection

None from group L knew how a firewall works or the protection it provides. They did not know the difference between a firewall and an anti-virus; as one said, "firewall always comes automatic and anti-virus I know you have to purchase it online or install it by disk" (L2). All in group H knew how a firewall works. They all had previous experience of configuring a firewall.

Multiple Profiles

We examined participants' perceptions of using multiple profile settings for their security software including personal firewalls. All from group H desired multiple profiles, wanting varied levels of protection for different activities (H1,H2,H4,H5) and different situations (all-H). As H1 said, "I have 2 PC's at home. One runs in Linux and the other in Windows. I want to share files between the two. My firewall on my HP box prevents that communication. I am able to bypass it, but if I want to do something in my home, I don't want to tamper with security settings. I just want it to share my connection to my laptop, but my HP laptop at some point may be taken away to a coffee shop, so I don't need a fixed level of security everywhere." Participants also liked to have the right to choose and control their profile settings (H1,H2,H5). They wanted different levels of protection based on familiarity with the network (all-H), its service provider (H1,H3,H4), its infrastructure (H1,H2,H5), and the people in the network (all-H). They also wanted a higher level of protection for a Wireless connection compared to a LAN (H1,H2,H4,H5). H1 and H3 also wanted profiles based on features, such as host name and IP address.

While the focus of our study was not on Vista firewall, we discussed its use of multiple profiles based on network location. None in group H would choose the network location in Vista based on physical location, "even if I am at home, I put it as a public location so no one can connect and intervene" (H2). However, several (H1,H2,H3) believed that less knowledgeable users might. Indeed, L1 and L5 confirmed that; as L5 said, "I just choose home because it is home, even at a party maybe home; at a coffee shop, public. I do not know why it asks me about the location." Other comments from group L show they lack the basic knowledge to choose the profile based on security needs. L5 did not understand how wireless works: "What is the difference if I am at home or not? It is wireless. It is the same Internet and it is the same wireless. If it was not wireless, I could say at home it is different from school or airport." L4 revealed a misunderstanding of the concept of network location in Vista, stating that she does not think about security when she chooses the network location, "for example I go to some 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 anybody else to use it otherwise I will go over my limit."

All participants thought non-expert users need only one profile, "because [otherwise] you would be getting into complications, and for my little brain, it is just too much" (L3). Three (L1,L4,L5) did not know why they would ever need a lower level of protection, preferring one profile at the highest level. The remainder thought an intermediate level was 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).

Frequent Pop ups

Personal firewalls show pop-up messages to ask users if connections should be allowed or blocked. We probed if users understand the messages and their reaction to them. In line with prior research on phishing warnings [4], our results show even those in group H usually ignore the messages: "If I am installing or removing something, I say Continue, but if in the middle of nowhere it pops up then I will read it. But most of the time the reaction would be Continue" (H2). None from group L understand the messages. Most (L1, L2,L4,L5) ignore the messages because they block 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, just clean it for us" (L2). Prior research recommends that security warnings should interrupt users' primary task to be effective [4]; our results show that interruption is not sufficient to prevent users from discarding the warning to do their primary task. Other participants (H1,L2,L4) noted the high rate of false positives: "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).

Frequent pop ups is one of the reasons participants (all) disliked security software: "I like the fact that I hardly know it's there, and I am not constantly getting all these pop up's, and if there is a pop up, I take it more seriously" (L3). Frequent messages may result in uninstalling the software (H1,H4,L1,L2,L3), switching to another software (H1,L1,L2,L3), or turning it off (all-H,L5), "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 keep it open" (H2).

Automation

Those with high security expertise do not want full automation for security software (all-H), preferring to have some control: "everything automated is an annoyance" (H1), "the software cannot decide on your preferences" (H2). This confirms Edwards et al.'s [3] arguments about the effects of environmental and social contexts on security automation. Some think the software should be intelligent and learn from users' behavior (H2,H4,H3). Participants agree that non-expert users need full automation, stating that they lack the required knowledge and experience to configure their security software (all) and the motivation to learn and understand security (H1,H2,H3, all-L). As L5 said, "you cannot expect normal people to understand those complexities. There is no reason for them to understand the details; it is not their job." Therefore, automation could help reduce the mistakes in configuration of the security software (H1,H3,H5); however, L3 wanted the option to disable automation.

Those participants with low security expertise did not know anything about their current security software and their settings. They (all-L) usually rely on others who, they think, are more knowledgeable in security to choose the software for them and configure it, "he [her boyfriend] knows a lot about computers, so if we need anything he changes and I have no idea. I never go anywhere and never change the security options."

Direction

One feature of personal firewalls is that they can filter both incoming (from the network to the computer) and outgoing (from the computer to the network) traffic. All in group H preferred 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). L2 and L3 also wanted to have protection in both directions, but they mentioned that outgoing protection should be optional, "from the Internet to my computer is more important because I don't usually send anything harmful to the Internet, but worldwide I think it should be both ways because you can't guarantee other people won't." (L2). L1, L4, and L5 thought only incoming traffic should be protected, "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" (L4).

The Black-Box

When the participants with a high level of security knowledge saw the black-box, they asked if it is existing security software, a new type of software, or a combination of them. When we asked what they need, they all said they prefer to have all-in-one security software that combines the existing software; all in group H thought this makes the configuration easier for end users, "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. So one good point is to have as many aspects of security built inside a single solution" (H4). H1 also mentioned that users lack knowledge about the protection provided by security software and so having all-in-one can prevent a false sense of security: "a home user does not know what a firewall is… 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 and he's happy." Comments from participants with low knowledge (all-L) also reveal requirements and expectations from the black-box that can be met only by integrating several types of security software.

Discussion

Our initial results show that participants with low and high levels of security knowledge and experience have differing expectations from security software. Those at the low end of the spectrum lack the knowledge to configure their security software and they do not have the motivation to do so. These participants wanted the firewall included in an all-in-one security package, which works automatically in the background. This confirms the discussion of Dourish et al. [1] that "a technology deployed to solve [just] one problem" may not be appropriate for end-users. They argued that users should answer the question of "is this computer system secure enough for what I want to do now?" Our results show that participants with low security knowledge are unable to answer this question because they do not know what factors affect their security requirements and how. Because they do not know when and where they need a higher or lower level of protection, a single profile setting may be appropriate for them. Alternatively, adjusting the level of protection automatically or basing profiles on *security related factors* that users can understand may be effective. Users with a high level of security knowledge and experience also preferred an all-in-one package, but with the option to control the level of automation and to create different profile settings based on the factors that affect their required level of protection.

Conclusion

Our initial results of an exploratory study describe users' requirements and expectations of security software such as personal firewalls. Our results highlight the differing requirements between those with low and high levels of security knowledge and experience. We are continuing our analysis of the other 16 interviews to examine how the remaining data, which includes participants with a medium level of security knowledge and expertise, impact our initial findings. Our findings will benefit those designing personal firewalls and other security software, as well as complex systems that adapt to changing contexts.

References

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

[2] Downs, J. S., Holbrook, M. B., & Cranor, L. F. Decision strategies and susceptibility to phishing. In *SOUPS '06*, vol. 149 (2006), 79-90.

[3] Edwards, W. K., Poole, E. S., & Stoll, J. Security automation considered harmful? In *NSPW '07* (2007), 33-42.

[4] Egelman, S., Cranor, L. F., & Hong, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *CHI '08* (2008), 1065-1074.

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

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

[7] Johnston, J., Eloff, J.H.P. & Labuschagneb, L. Security and human computer interfaces. *Computers and Security*, 22 (2003), 675–684.

[8] Raja, F., Hawkey, K. & Beznosov, K. Revealing hidden context: improving mental models of personal firewall users. In *SOUPS '09* (2009), 1-12.

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

[10] Stoll, J., Tashman, C.S., Edwards, W.K. & Spafford, K. Sesame: informing user security decisions with system visualization. In *CHI '08* (2008), 1045–1054.

[11] Wack, J.P., Cutler, K., & Pole, J. Guidelines on firewalls and firewall policy: recommendations of the NIST. U.S. Dept. of Commerce, Technology Administration, NIST (2002).