It's Too Complicated, So I Turned It Off! Expectations, Perceptions, and Misconceptions of Personal Firewalls

Fahimeh Raja, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, Kellogg S. Booth

University of British Columbia
Vancouver, Canada
{fahimehr,hawkey,pooya,beznosov}@ece.ubc.ca, ksbooth@cs.ubc.ca

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. We conducted semi-structured interviews with a diverse set of participants to gain an understanding of their knowledge, requirements, perceptions, and misconceptions of personal firewalls. Through a qualitative analysis of the data, we found that most of our participants were not aware of the functionality of personal firewalls and their role in protecting computers. Most of our participants required different levels of protection from their personal firewalls in different contexts. The most important factors that affect their requirements are their activity, the network settings, and the people in the network. The requirements and preferences for their interaction with a personal firewall varied based on their levels of security knowledge and expertise. We discuss implications of our results for the design of personal firewalls. We recommend integrating the personal firewall with other security applications, adjusting its behavior based on users' levels of security knowledge, and providing different levels of protection based on context. We also provide implications for automating personal firewall decisions and designing better warnings and notices.

Categories and Subject Descriptors

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

Keywords

Usable security, personal firewall

SafeConfig'10, October 4, 2010, Chicago, Illinois, USA.

1. INTRODUCTION

A personal firewall is security software 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. Intended to be used by non-experts, personal firewalls are becoming commonplace and are recognized as "the first line of defense" for personal computers [22, 19, 31]. However, the protection provided by them depends strongly on their correct configuration [17, 8, 2]. Therefore, the usability of personal firewalls is key to their effectiveness. In particular, as users become increasingly mobile [20], it is important for them to be able to judge whether their computer is secure enough for the usage context at hand [6].

We began studying the usability of personal firewalls by evaluating Microsoft Windows Vista Firewall (VF) [26]. Our study revealed that the lack of an accurate mental model about the VF's system model is one of the root causes of errors when configuring the firewall. We redesigned the user interface of the firewall to more accurately reflect its system model. The results of a laboratory study showed that good user interface design and helpful feedback could assist users to develop more effective mental models of the firewall and improve their understanding of the firewall's configuration, resulting in fewer dangerous errors.

One interesting finding of our prior research [26] was that the majority of participants did not see the need for a 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, perceptions, and misconceptions of personal firewalls. This understanding is required to successfully manage design tradeoffs [14, 24]. 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 [28].

The first contribution of this paper is our analysis, which reveals that participants with different levels of security knowledge have different understandings about the functionality of a personal firewall. While many participants had familiarity and experience with anti-virus software, they were not aware of the existence of a firewall on their computer. Additionally, most participants were not aware of the benefits of personal firewall protection. Our results also show that context is important for participants when making security

decisions. We found different contextual factors that are important to 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. When interacting with personal firewalls, many of our participants had problems understanding and making informed decision about the warnings that ask them about allowing or blocking a connection. As a result, they tend to ignore the firewall warnings or even turn their personal firewall off or completely un-install it. Most of our participants liked the idea of a personal firewall that automatically makes security decisions and provides notifications about such decisions.

Our second contribution is the examination of the implications for the design of personal firewalls that address the issues we found. To have more usable and effective personal firewalls, we recommend providing firewalls in an integrated solution with other security software. We also recommend 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 propose that personal firewalls should provide users with different levels of protection based on their context and also provide the user with information to make informed security decisions in each context. Finally, we provide recommendations for designing effective methods of interaction between the firewall and the user such as providing automation, warnings, and notices.

The remainder of this paper is organized as follows. In Section 2, we provide background and related work on usable firewalls. In Section 3, we describe our methodology for performing the study. In Section 4, we present our findings. We provide implications for the design of usable personal firewalls in Section 5. Finally, we conclude in Section 6 with a summary of our contributions, and a discussion of our future work in this area.

2. BACKGROUND AND RELATED WORK

In 1975 Saltzer and Schroeder [27] introduced "psychological acceptability" as one of the design principles for security mechanisms and applications. However, until the late 1990s, little attention was given to human factors and usability of interfaces in computer and information security. Since then, Usable Security has grown as a distinct field of research [11]. However, even in 2009, prominent researchers in the fields of HCI and security, such as Norman [25] and Lampson [21], argued that users lack a good mental model of security mechanisms and applications.

Security is inherently complex [11, 25, 21]. While users often make security decisions based on their limited security knowledge [31], security mechanisms and applications have usually been designed by experts who are not "good models for typical users" [29, 3]. This may result in unrealistic assumptions being made about end users and their skills when security mechanisms are designed [1], with an outcome of unusable applications. Therefore, it is important to understand users' knowledge and capabilities when designing security applications. Personal firewalls are no exception.

Prior research has considered the usability of personal firewalls. Johnston et al. [19] performed a heuristic evaluation of the Windows XP firewall and proposed improvements for its interface, such as visibility of the system features and status and learnability of the interface. Herzog and Shahmehri [17] defined use and misuse cases for personal firewalls and performed a cognitive walk through of 13 personal firewalls (the most popular personal firewalls for Windows XP at the time[1]) to examine the behavior of the firewalls for those scenarios. They also compared the granularity of rules and the usability of rule configuration for these firewalls. Their results highlight 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. [12] considered the difficulty of understanding and defining firewall rules. They proposed an interactive interface that combines simulation, visualization, and interaction to help system administrators understand and update firewall configurations. Wool [33] critiqued usability problems of direction-based filtering in firewalls that stemmed from a mismatch between the network administrators' global, network-centric view and the firewall's local, device-centric view.

Although these prior studies inform our usability studies of personal firewalls, all of them were based on evaluation by experts. Their findings have not been validated by studies with target users of those firewalls. Hazari [16] performed an exploratory study to investigate users' perceptions of the factors that could affect the selection of a personal firewall in an organization. His Q-sort analysis [30] 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 hands-on firewall experience that included installation, configuration, and use of a commercial personal firewall. His findings may not be generalizable because average users of computers rarely have any security training.

Stoll et al. [31] 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 user study to evaluate the usability of their proposed approach. They found that their participants could make better decisions about allowing or blocking network connections with their tool than with traditional firewalls.

In our earlier work [26], we performed a usability analysis of the 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. The results of our laboratory study suggest that hiding the effect of selecting a Network Location on the security state of the firewall results in dangerous misunderstandings by users of the firewall configuration. It also showed that revealing the hidden network context helps users develop a more complete mental model of the firewall and a better understanding of its configuration. Interestingly, 65% of participants did not see the benefits of maintaining multiple profiles for different contexts of use.

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

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

None of the above work has captured a deep understanding of users' knowledge, expectations, and misconceptions of personal firewalls. The goal of the research presented here is to narrow this gap.

3. 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., the 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 the users think, affect their required level of protection from a personal firewall?

To answer these questions, we conducted semi-structured interviews with a diverse set of participants.

3.1 Participants

To recruit participants, 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 to two online classifieds, Craigslist and Kijiji; and 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.

We recruited 30 participants from both the university and general community. They had a wide range of educational levels (from high school to Ph.D.) and backgrounds (e.g., mining, business, computer science, art, pharmacy), 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 the operating system). Almost all (28/30) used a laptop in a variety of networks.

Based on participants' responses to our background questionnaire (see Section 3.2 for more details about the questionnaire), we classified participants' security knowledge and experience into three categories: high, medium, and low. The categorization was done to understand users' requirements, 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 interrater reliability analysis using the Kappa statistic was performed to determine consistency between the raters. The reliability was found to be Kappa = 0.897 ($p<0.001$). 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. Table 1 shows the demographics of the participants in each group.

It should be noted that 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.

3.2 Study Protocol

We conducted a one-hour, audio-recorded, semi-structured interview with the participants. We chose interviews because they are useful for investigating events that occur infrequently and irregularly [13], which is the case for users' interaction with personal firewalls. For the same reason, 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 investigation 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 [10, 7, 15].

In the study, participants first completed a consent form and background questionnaire. This included an assessment of their security knowledge and experience with the following six tasks taken from the "Security Center" of Windows Vista [32]: (1) installing updates; (2) scanning for viruses, spyware, and other potentially unwanted software; (3) changing security settings of web browsers; (4) deleting browsing history and cookies; (5) setting different security controls for different users; and (6) managing browser plugins. 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 participants to describe what they knew about the tasks and their importance, and to specify how often they performed those tasks.

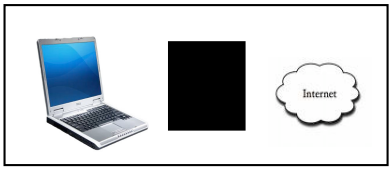

Figure 1: The black-box figure used to assess participants' perceptions and requirements of a security application such as a personal firewall.

To assess participants' perceptions and requirements 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 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 participants questions about their knowledge of and experience with personal firewalls to determine if they knew what a 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 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 this software?
- How do you want to interact with them? (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 their reasoning behind the responses. We also 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 [23]. 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.

3.3 Data Analysis

We transcribed the audio records of the interviews and analyzed the data using Qualitative Description [28]. 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 we 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" [18, p. 283]. An effective strategy for increasing the validity of the analysis is to use multiple investigators in interpreting the data [18]. 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.

4. RESULTS

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

4.1 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 configuration easier for end users; as H26[2] 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. So one good point is to have as many aspects of security built inside a single solution."* 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*

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

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 and make it be able to do some kind of intelligent decision. If I had to add it on top of the current ones then I don't need it. I think 5 is enough, I do not really want the 6th one."*

Comments from participants with lower level of security knowledge and experience also reveal 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).

4.2 Knowledge about Personal Firewall

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 one said, *"firewall always comes automatic, and anti-virus... I know you have to purchase it online or install it by disk"* (L3). The comments from 6 participants in group L show 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. Although they did not know its exact functionality, they all 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 6 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 multi-player gaming (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 a printer 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 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 they mentioned that it prevents malicious applications from sending private information of the user to unknown sources (H22, M4).

4.3 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 7 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, its service provider, and 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. Then the organization that provides the connection."* (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. For example 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 Windows Vista firewall, we discussed its use of multiple profiles to provide the user with different levels of protection based on network. 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 on the firewall settings. None in group H and M would choose the Network Location based on 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 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 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." (L17)*

4.4 Interaction

Personal firewalls usually prompt users to ask whether a connection should be allowed or blocked. We probed if participants understood the firewall prompts and their reaction to them. While most of the participants read the prompts, many of them did not make informed decisions in response to them. There were three different reasons for the lack of an informed decision:

- **Not understanding the content of the prompts**: All participants in group L and 3 in group M did not understand the messages. Some of the participants 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 prompts 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 have affect on users' decision making about firewall prompts: *"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: *"No. But as long as many friends have it [the game] installed, I would install it."*

Ignoring firewall prompts 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 do not use that firewall anymore. It is too sensitive. I got alerts all the time. It always beeps so I do not like it. This one [the new firewall] 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 prompts** (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 trade off. I can not pay attention to each and every pop-up" (M10).

All of the participants except H26 and M28 thought frequent prompts 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 keeps reminding me and it's kind of annoying"* (L14). We asked them how they would rather interact with their firewall. Our results show 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 prompts, the software should provide them with the 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 4 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."*

5. 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.

5.1 Knowledge about Personal Firewall

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. [6] that "a technology deployed to solve [just] one problem" may not be appropriate for end-users.

The second approach is to design firewall prompts 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 these warnings may be a good method for communicating a useful mental model of personal firewalls.

5.2 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 affects their security requirements. However, to be effective, it should be possible for users to switch between different levels of security when required. Further research is required for a concrete implementation of this approach and its formal evaluation.

5.3 Interaction

Considering Cranor's classification of security communications [4], firewall prompts 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 [4], 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 prompts is the human receiver, "the human who receives the security communication and whose actions will impact system security" [4, 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 [4] 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 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) user's prior decisions, (2) user's expected behavior, or (3) other user behavior. DiGioia et al. [5] also show that relying on a community consensus can be effective for users without the required expertise to make an appropriate decision. However, there should be an option for disabling the automation; because our findings show that users with higher than normal security expertise are interested in making security decisions themselves.

If a personal firewall automates security decisions, it should have a mechanism for providing awareness to the user 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 in the automated system. Passive notices would be one way to provide the user with such awareness. These notices should be designed to be understandable, with short, unambiguous, and jargon-free descriptions [4]. If a decision about a connection attempt cannot be made automatically, the firewall should provide the user with active warnings. However, unlike current firewall prompts that only ask the user to allow or block the connection, the prompt 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 [9, 7, 4]. Moreover, visualizations, such as the approaches proposed in our prior work [26] and those by Stoll et al. [31], 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.

5.4 Summary of Design Recommendations

To aid the reader, we summarize our recommendations for improving the design of personal firewalls based on our findings.

- ***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.

6. CONCLUSION

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. Many of our participants had problems making informed decisions when they receive warnings from their firewalls, which results in them ignoring these warnings. Most of our participants wanted a firewall that automatically makes security decisions and provides notifications about such decisions. 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.

Acknowledgments

This research is funded by the Natural Sciences and Engineering Research Council (NSERC) of Canada under the Strategic Networks and Discovery Grants programs. We thank all the participants of our user study and also LERSSE and IDRG members for their helpful feedback on the project. Research by the first, second, and fourth authors have been partially supported by the Canadian NSERC ISSNet Internetworked Systems Security Network Program.

7. REFERENCES

[1] Anderson, R. Psychology and security resource page. http://www.cl.cam.ac.uk/ rja14/psysec.html (2009).

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

[3] Brostoff, S., Sasse, M. A., Chadwick, D., Cunningham, J., Mbanaso, U., and Otenko, S. R-What?: Development of a role-based access control policy-writing tool for e-Scientists. *Software Practice and Experience*, *35*, 9 (2005), 835–856.

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

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

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

[7] Downs, J. S., Holbrook, M. B., and Cranor, L. F. Decision strategies and susceptibility to phishing. In *SOUPS '06*. ACM, New York, NY, USA, 2006, 79–90.

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

[9] Egelman, S., Cranor, L. F., and Hong, J. 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*. ACM, New York, NY, USA, 2008, 1065–1074.

[10] Friedman, B., Hurley, D., Howe, D. C., Nissenbaum, H., and Felten, E. 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*. ACM, New York, NY, USA, 2002, 614–615.

[11] Garfinkel, S. L. *Design principles and patterns for computer systems that are simultaneously secure and usable*. Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, USA (2005). Adviser-David D. Clark and Adviser-Robert C. Miller.

[12] Geng, W., Flinn, S., and DeDourek, J. Usable firewall configuration. In *PST*. 2005, 11 pages.

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

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

[15] Gross, J. B. and Rosson, M. B. 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*. ACM, New York, NY, USA, 2007, 10.

[16] 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.

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

[18] Johnson, R. Examining the validity structure of qualitative research. *Education*, *118*, 2.

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

[20] Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D. "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*. ACM, New York, NY, USA, 2009, 1993–2002.

[21] Lampson, B. Privacy and security usable security: how to get it. *Commun. ACM*, *52*, 11 (2009), 25–27.

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

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

[24] Nielsen, J. *Usability Engineering*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1993.

[25] Norman, D. A. When security gets in the way. http://www.jnd.org/dn.mss/when_security_gets_in_the_way.html (2009).

[26] Raja, F., Hawkey, K., and Beznosov, K. Revealing hidden context: improving mental models of personal firewall users. In *SOUPS '09*. ACM, New York, NY, USA, 2009, 1–12.

[27] Saltzer, J. and Schroeder, M. The protection of information in computer systems. *Proceedings of the IEEE*, *63*, 9 (1975), 1278–1308.

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

[29] Smetters, D. Usable security: Oxymoron or challenge? http://www.nae.edu/nae/naefoe.nsf/weblinks/GBAN-79EJLA/$FILE/smetters_presentation.pdf?OpenElement (2007).

[30] Stephenson, W. *The study of behavior: Q-technique and its methodology*. University of Chicago Press, 1953.

[31] Stoll, J., Tashman, C. S., Edwards, W. K., and Spafford, K. Sesame: informing user security decisions

with system visualization. In *CHI*. ACM, New York, NY, USA, 2008, 1045–1054.

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

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