Poster: 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

1. INTRODUCTION

Personal firewalls are recognized as the first line of defense for personal computers. However, the protection they afford depends strongly on their correct configuration [4]. Therefore, their usability is key to their effectiveness. In particular, as users become increasingly mobile, it is important for them to be able to judge whether their computer is secure enough for the usage context at hand [2].

Our prior research [5] revealed that the lack of an accurate mental model about the firewall's system model is one of the root causes of users' errors when configuring the firewall. The results of a laboratory study showed that an improved user interface design that incorporated feedback about the state of the firewall in different network contexts could help users develop more effective mental models of the firewall and improve their understanding of firewall's configuration, resulting in fewer dangerous errors. However, we also learned that a large proportion of users did not see the need for multiple profiles based on context.

In this research, our goal is to better understand users' knowledge, expectations, perceptions, and misconceptions of personal firewalls. We conducted interviews with 30 participants and analyzed the data using qualitative description [7]. The results from 10 interviews are presented in [6]. In this paper we present our aggregated results and examine their implications for the design of personal firewalls.

2. METHODOLOGY

We conducted semi-structured interviews to answer the following research questions: 1) What do users know and what misconceptions do they have about personal firewalls and the protection provided by them? 2) What expectations do users have of an application such as a personal firewall? 3) How do users prefer to interact with an application such as a personal firewall (i.e., the level of automation, feedback)? 4) Do the users need to have different levels of protection for an application such as a personal firewall? Why? and 5) What factors, do the users think, affect their required level of protection from an application such as a personal firewall?

We recruited 30 participants from both the university and general community. They had a wide range of educational levels, backgrounds, and occupations. Almost all (28) used a laptop in a variety of network contexts. We classified their security knowledge and experience into three categories: high (H), medium (M), and low (L) in order to examine their expectations, perceptions, and misconceptions of a personal firewall in relation to their level of security knowledge and expertise. Table 1 shows their demographics.

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

Table 1: Participants' demographics.

3. RESULTS

None in group L knew about the functionality of a firewall. Their comments show their misconceptions about the protection provided by different security software. Most of them did not know whether or not they had a firewall on their computer. All in group H and 6 in group M had previous experience configuring a firewall. Others in group M were not sure about the functionality of a firewall. Some comments from these participants show that they faced problems in configuration of their firewall (e.g., in allowing a printer connection), which resulted in them turning the firewall off.

We examined if participants' required level of protection from their personal firewall varies depending on the context. All in group H and 7 in group M wanted varying levels of protection based on their activity (e.g., online banking vs. multiplayer gaming), the network's characteristics and settings (e.g., wireless vs. wired), and the people in the network (e.g., family vs. people in a coffee shop). Most participants thought non-expert users should have the same protection in all contexts, *"because [otherwise] you would be getting into complications, it is just too much for my little brain"* (L12). Four in group L did not know why they would ever need a lower level of protection, preferring the highest everywhere.

We probed if participants understood the firewall prompts and their reaction to them. Most of them did not make informed decisions in response to prompts. Reasons for this included not understanding the content of the prompts, interference with a primary task, and previous experience *"it's just Allow, Allow, Allow. Because they hit Allow a thousand times and nothing wrong happens" (H1)*. Ignoring firewall prompts can come in different forms: 1) uninstalling the firewall, 2) switching to another firewall, 3) turning the firewall off, and 4) getting habituated to prompts. In general participants dislike the current security alerts.

We asked them how they would rather interact with their firewall. None in group H wanted full automation, preferring to retain some control. On the other hand, participants agree that users with a low level of security knowledge and

experience need full automation, stating that they lack the required knowledge to configure their security software and the motivation to learn and understand security. Some participants thought the software should be intelligent and learn from users' behavior; one specifically talked about automating decisions made in a specific context.

4. DISCUSSION

Many of our participants were unaware of the functionality of a firewall or even its existence on their computers. Lack of awareness of firewall functionality may result in a false sense of protection. A possible solution is to have an all-in-one security solution; that might reduce confusion and misconceptions about the protection provided by specific software. This is in line with the discussion of Dourish et al. [2] that "a technology deployed to solve [just] one problem" may not be appropriate for end-users. We noticed that many of our participants interact with firewalls only when the firewall prompts them to make a security decision. This could be an appropriate "teachable" moment to provide information about the functionality of a firewall in order to communicate a useful mental model of personal firewalls.

Our participants wanted different levels of protection based on several contextual factors. The design of personal firewalls should help users identify the relevant contextual factors and relate those factors to the level of security required. Moreover, they should be able to quickly change the level of security when a relevant contextual factor changes.

Many of our participants preferred to have a firewall which automatically decides whether to allow or block a connection. This decision can be automated based on their prior decisions, expected behavior, or the behavior of other users. If a firewall automates security decisions, it should have a mechanism, such as passive notices, to notify the user about the decision. Such feedback can make the user aware of the security status and also might assist them in dealing with failures in the automated system.

Most of our participants lack the required knowledge to assess the consequences of allowing or blocking a connection. At the same time, since blocking the connection does not allow them to do their primary task, they are not motivated to do so; they may therefore allow a malicious connection. Moreover, as Cranor [1] discusses and our results show, a key factor in users' attitudes and beliefs about warnings is their previous experience. A personal firewall prompts users 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. As discussed before, one solution is to automate the decisions as much as possible. In the case that a decision cannot be made automatically, the firewall can provide 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 [3]. Moreover, visualizations, such as the approaches proposed in our prior work [5] and also by Stoll et al. [8], can be used to help users make more informed decisions. In addition to their immediate function, firewall warnings should be designed in a way that helps users understand the functionality of the firewall. This could help users to be aware of the existence of firewall, and help them in their future decisions.

5. CONCLUSIONS

We presented a study investigating participants' knowledge, requirements, perceptions, and misconceptions of personal firewalls. Our qualitative analysis of 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. We found that context is an important factor in our participants' security decision making and that different contextual factors affect our participants' decisions; however, we also found that most participants lack the knowledge to determine the required level of security based on the contextual factors. When interacting with firewalls, many of our participants had problems making informed decision about allowing or blocking a connection. As a result, they tend to ignore the firewall warnings or even disable or un-install their firewall.

Based on our results, we recommend that personal firewalls be provided as an integrated solution with other security software. Firewalls should have the facility to determine 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 users be afforded with different levels of protection based on their context and also that users are given the information needed 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. Our recommendations will benefit those designing personal firewalls and other security software that needs to adapt to changing contexts or provide warnings to end-users.

6. REFERENCES

[1] Cranor, L. F. A framework for reasoning about the human in the loop. In *UPSEC'08*. 2008, 1–15.

[2] 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.

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

[4] Herzog, A. and Shahmehri, N. Usability and security of personal firewalls. *IFIP'07* (2007), 37–48.

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

[6] Raja, F., Hawkey, K., Beznosov, K., and Booth, K. S. Investigating an appropriate design for personal firewalls. In *CHI EA '10*. 2010, 4123–4128.

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

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