Revealing Hidden Context: Improving Mental Models of Personal Firewall Users

Fahimeh Raja, Kirstie Hawkey, Konstantin Beznosov
University of British Columbia, Vancouver, Canada
{fahimehr,hawkey,beznosov}@ece.ubc.ca

ABSTRACT

The Windows Vista personal firewall provides its diverse users with a basic interface that hides many operational details. 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. We present a study of participants' mental models of Vista Firewall (VF). We investigated changes to those mental models and their understanding of the firewall's settings after working with both the VF basic interface and our prototype. Our prototype was designed to support development of a more contextually complete mental model through inclusion of network location and connection information. We found that participants produced richer mental models after using the prototype than when working with the VF basic interface; they were also significantly more accurate in their understanding of the configuration of the firewall. Based on our results, we discuss methods of improving user understanding of underlying system states by revealing hidden context, while considering the tension between complexity of the interface and security of the system.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*Evaluation/Methodology*; D.4.6 [**Software**]: Security and Protection—*Information flow controls*

General Terms

Design, Human Factors, Security

Keywords

Usable security, firewall, configuration, mental model

1. INTRODUCTION

Mobile computing is increasingly commonplace [30]; even in a single location, there may be different network connection options. In Windows Vista (with 180 million licenses as of August, 2008 [24]), Microsoft introduced a built-in personal firewall which provides a basic user interface (which we call VF-Basic) for home users of Windows Vista and an advanced one (VF-Advanced) for IT professionals to configure firewall and Internet protocol security settings [25]. This firewall incorporates the context of network location (a change from the XP firewall) and connection types. In VF-Advanced, a user can configure the firewall for each network location; 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 [3]. However, full automation with no user intervention is difficult to achieve; it is often infeasible to completely remove the human from the loop [7, 10, 29].

A mental model has been defined as the model of the system that the user holds in his mind [18]. One key to usable security is mitigating the gap between what a system actually does and the mental model that users have of its functionality [28, 35]. 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 a user and the system's security features [16]. While an effective mental model does not need to include all the technical system details, it does need to be functional and allow users to predict both observable system behaviours and the consequences of the users' actions [4]. Concealing system details as a means of reducing complexity may leave users unable to respond to unexpected system events [9]; enough technical details must be provided so that users can make informed decisions as they interact with security tools [8]. We cannot hide the inner complexity for the sake of interface simplicity, if the user is then left with an ineffective mental models for those times they must interact. This is particularly important for security user interfaces in order to avoid dangerous errors.

In this paper, we present a study which examines participants' mental model of firewalls, as well as how VF-Basic and our prototype support those mental models and their understanding of the effects of their firewall configuration. Our prototype interface provides a more explicit representation of the network context and its impact on the firewall's security state both in current and future network contexts. We found that including this contextual information improved participants' mental models and understanding of configuration, resulting in fewer dangerous errors about the security state of the firewall. Based on our results, we discuss the impact of mobile computing on usable security

Symposium On Usable Privacy and Security (SOUPS) 2009, July 15-17, 2009, Mountainview, CA, USA.

interfaces, how to better support users' mental models of underlying system state, and how to balance security and complexity in the interface. Our study makes an important contribution as it highlights the dangers of hidden complexity and provides an initial exploration of developing more effective mental models through feedback about both the current security state of the system and the security state in future computing contexts. Our findings may be relevant to other configuration interfaces for context aware end-user security tools. We first present related work in the areas of usable security and firewall usability, and provide background information about VF and its usability.

2. RELATED WORK

2.1 Usable Security

The issue of overly complex interfaces impacts security and non-security applications alike. One approach is to present different configuration options and information 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 [21]. Whitten and Tygar [32] introduced the concept of safe staging for security interfaces to safely reduce immediate complexity for novice users. Cranor [6] 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 [34] secure interaction design guidelines. Chiasson et al.'s [4] principles for designing security applications for administrators include providing feedback to accurately determine the current state of the system and the consequences of actions. 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 [27].

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 action [3]. Prior usable security and privacy research has focused on the social and environmental settings of users' context [5, 14], rather than the computing context (i.e., current network connection).

2.2 Usable Firewalls

Prior research has considered the usability of firewalls for administrators and organizations. Geng et al. [11] considered the difficulty of understanding and defining firewall rules. They propose an interactive interface that combines simulation, visualization, and interaction to help system administrators understand and update firewall configurations. Wool [33] critiques usability problems of enterprise firewalls that stemmed from a mismatch between users' global network perspective and the firewall's local device-centric perspective. For personal firewalls, our perspective is that usability problems may exist when there is a mismatch between users' computer-centric perspective of their security and the firewall's security state which changes according to the context of network location and connection.

Another body of work has investigated the usability of personal firewalls that are intended for use by non-experts. Johnston et al. [16] performed a heuristic evaluation of the Windows XP personal firewall and proposed improvements for its interface based on HCI-security criteria they developed, such as visibility of the system status, conveying features, and learnability. They emphasized that in security applications the user should trust the system. Herzog and Shahmehri [12] performed a usability study of 13 personal firewalls by comparing the granularity of rules and usability of rule setup. They defined use cases and misuse cases and performed a cognitive walk through to examine the behavior of the firewalls for these scenarios. They highlight the need of conveying firewall design to users. Finally, Herzog and Shahmehri [13] present techniques for presenting help-related content to the users in order to increase the usability of personal firewalls.

We are not the first to propose providing personal firewall users with more information about the security state of their firewall. Stoll et al. [29] used a spatial extension of the desktop metaphor to visually show system level information. Their goal was to present technical information in an understandable way so that non-expert users can make informed decisions. Our approach is similar to theirs in that we provide visual information to make the security state visible; however, our emphasis is on providing information on the network context that effects the functionality of the firewall, not the functionality of the firewall itself.

In summary, prior usable security research has mainly focused on helping users understand the consequences of their configuration on the security state of their system for the *current* context of use. However, as users become more mobile, it is increasingly necessary to help them understand the consequences of their actions on security state for their *future* contexts of use as well (e.g., when in a different network context). We propose that if the security of the application changes as a result of underlying context, the changes must be revealed to users. Otherwise the hidden context can leave them with dangerous misunderstandings of security state.

3. WINDOWS VISTA FIREWALL

3.1 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 [22]. The VF interface has three network locations which 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). Which profile is *automatically* applied depends on which network location was detected. In each location, the user can also enable or disable the firewall for three types of connections: wireless, local area connection, and bluetooth; this results in 9 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 location type (as long as the firewall is enabled for that connection type).

The main window of VF-Basic has three links to change its settings (A, B, C in Figure 1) and help links about how the firewall works (Figure 1D) and what network locations are (Figure 1E). It also provides the current network location (Figure 1F) and the security state of the firewall. There are three possible security states: 1) the firewall is on (protecting the computer) for all network locations and all network

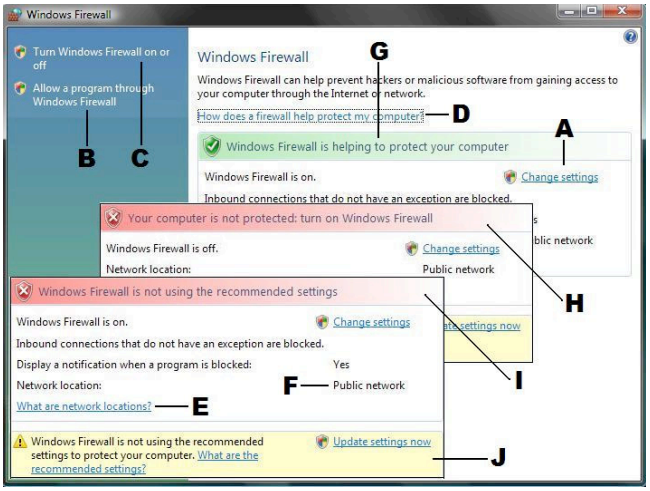

Figure 1: Main window of VF-Basic, with two inset panels showing different security configurations.

connections, it is using the *recommended settings* (Figure 1G); 2) the firewall is off for the current network location, (e.g., public in Figure 1H); and 3) the firewall is on for the current network location, but it is not on for all network locations and connections (Figure 1I). In the last two cases a yellow bar is displayed (Figure 1J), which says the firewall is not using the recommended settings and gives an"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). In the "General" tab (Figure 2A), the user can turn the firewall on or off. When she turns the firewall on, she also has the option to block all incoming connections. In the "Exceptions" tab (Figure 2B), the user can set exceptions of programs and ports for which inbound connections are allowed. In the "Advanced" tab (Figure 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 VF-Advanced).

3.2 Analysis of Vista Firewall Usability Issues

The research we present in this paper builds upon three projects which investigated the usability of VF. A heuristic evaluation, a survey, and a lab experiment (12 participants) identified several usability problems [1, 15]; 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 evaluated a medium fidelity prototype for VF in which a link was provided between the two interfaces [2]. 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

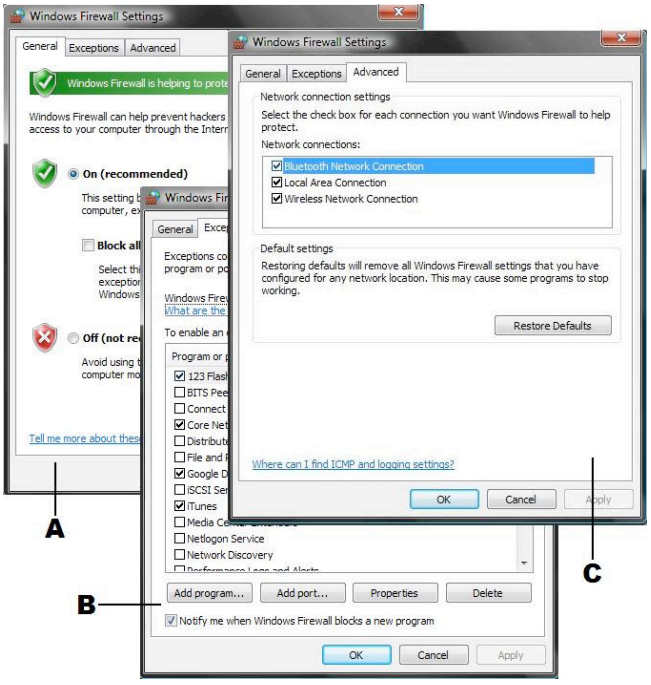

Figure 2: Tabs in second window of VF-Basic: A. General, B. Exceptions, C. Advanced.

it does support. For example, in VF-Advanced a user can configure the firewall for each network location; however, in VF-Basic, configuration changes are only applied to current network location and this is not obvious.

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

4. PROTOTYPE INTERFACE DESIGN

To evaluate whether inclusion of contextual information in VF-Basic can help users develop a richer mental model of the VF's underlying functionality, we designed a prototype for an enhanced basic interface. To isolate the effect of our changes, we designed the prototype 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 network context information and did not include all the functionalities of VF-Advanced, such as IPSec configuration and monitoring security associations.

Our prototype provides visualization of two context parameters that have an effect on the security state of the firewall: network location and connection. We also provide 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 possible network contexts without having to leave the basic interface.

We iteratively refined our prototype with 13 pilot testers (students) who performed the study tasks. As we applied their feedback to our design, we consulted them to ensure

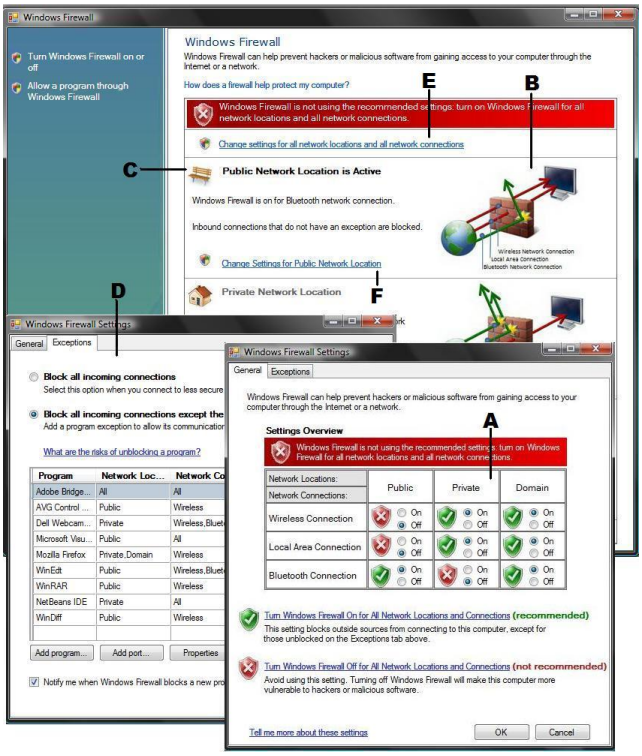

Figure 3: Prototype interface. Main window with dynamic configuration image (B) and enhanced context (C). Secondary window: General tab with configuration table (A), Exception tab with enhanced context (D).

that the changes made addressed their concerns. Our final prototype provides the configuration table (Figure 3A) recommended by three early pilot testers and a *dynamically updated image* (Figure 3B, modified from one in VF help [23]) to help users visualize different contexts for VF and the security state of the firewall in each context. This image includes the security state of 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 3C) to help 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 3A) mentioned above. This reveals all possible combinations of 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 [27, 26, 29]. In the Exceptions tab (Figure 3D), we included information about network location and connection. We gave the user the option to choose the network location and connection through a wizard similar to the one used in VF-advanced. As the ability to enable/disable the firewall for different network connections was incorporated throughout our prototype, we no longer required an "Advanced" tab.

5. METHODOLOGY

Preliminary studies [1, 15, 2] demonstrated that VF has usability issues that go beyond the surface presentation. Our prototype 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 in all future network contexts. We conducted a lab study with a diverse set of participants to examine the mental models that users have of VF and how VF-Basic and our prototype support users' mental model of firewall functionality and their understanding of the effects of their configurations.

5.1 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 participants used VF-Basic before our prototype (order1). However, there were concerns that this may have introduced a practice effect, priming 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 before VF-Basic (order2).

5.2 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 (not only users of Windows Vista) 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 VF was off for public and private network locations (enabled for bluetooth only), and on for domain locations (enabled for all network locations). Screen and voice recording software was installed on the laptop and used to record the session to augment researcher 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 participants' mental model of the firewall more accurately. As Jonassen and Cho [17] 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 VF works and how its settings will be applied to their computer. Figure 4C shows representative drawings reproduced from ones drawn by 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.

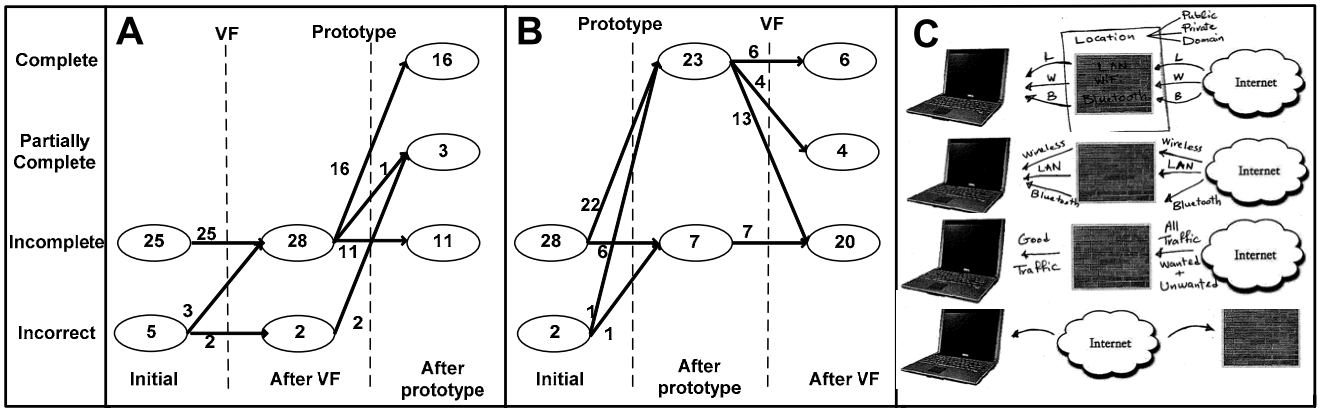

Figure 4: Transitions in participants' mental models (A: order1, B: order2) and representative drawings for each category of mental models (C).

After performing the tasks with each interface, we asked them to re-draw their mental model and briefly interviewed participants about their general understanding of the effect of their actions on the security state of the computer. We then had them fill out a configuration table indicating whether they think the firewall was on, off, or they were unsure for each of the 9 possible network location/connection contexts. They did this first without looking at interface (to see if they were aware of the effect 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, 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.

5.3 Participants

Since VF-Basic is designed for normal users of Windows Vista [25], for order1 we recruited 30 participants from both the university and general community. To ensure diversity, we screened interested participants by email. We asked their age, gender, degree and major, occupation, whether or not they were 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 the second group (order2) to reduce individual differences which could affect the development of the mental models. All participants were paid $10 for their participation.

The average age of participants in order1 was 29.6 (20-58) and order2 was 28.2 (19-56). Each group had roughly equal ratios of males/females, students/non-students, and those with/without prior experience with Windows Vista and personal firewalls. Participants 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., configuring the operating system). Almost all (order1: 28/30; order2: 26/30) used a laptop, with the majority using a desktop computer as well (order1: 20/30; order2: 21/30). Most (order1: 26/30; order2: 23/30) used their computers in a variety of network contexts (network locations and connections). We assessed participants' security experience by having them indicate how often they perform 6 computer security tasks (taken from the security center of Windows Vista). We categorized participants' security experience as low (order1: 6/30; order2: 4/30), medium (order1: 20/30; order2: 18/30), or high (order1: 4/30; order2: 8/30).

6. RESULTS

We now present key results. These include participants' mental models of how VF works, how well they understood the effects of their configuration tasks, and qualitative feedback about both VF-Basic and our prototype. It is important to note that the underlying operation of the firewall did not change between VF-Basic and the prototype; the prototype merely explicitly revealed the effect of network location and connection context on the firewall settings.

6.1 Mental Models

We categorized participants' drawings of VF functionality as an *incorrect* (incorrect basic understanding of the inner workings of a firewall), *incomplete* (correct basic understanding of the firewall operation, without context of network location and connection), *partially complete* (correct basic understanding of the firewall operation, with either the context of network location or connection), or *complete* (correct, with context of both network location and connection) mental model (see Figure 4C for representative drawings of each category). We examined participants' transitions between these categories of mental models (Figure 4A,B).

In order1, before working with the interfaces, 5 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 complete one which includes the relationship between VF settings and network location and connection. After using our prototype, 2/5 participants moved from the incorrect mental model to a mental model which includes network location

		Order1								Order2							
		VF-Basic				Prototype				Prototype				VF-Basic			
		Public		Private		Public		Private		Public		Private		Public		Private	
		B4	After	B4	After	B4	After	B4	After	B4	After	B4	After	B4	After	B4	After
CP1	μ	.85	1.06	.89	1.30	3.00	3.00	2.73	2.73	2.72	3.00	2.61	3.00	2.16	2.56	1.87	1.60
	σ	.438	1.004	.398	.938	0	0	.904	.904	0.188	0	.200	0	.226	.162	.183	.182
CP2	μ	2.50	2.07	2.71	1.36	3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	2.18	2.77	1.73	.96
	σ	.866	1.239	.488	1.376	0	0	0	0	0	0	0	0	.255	.156	.319	.228
T	μ	1.23	1.30	1.32	1.32	3.00	3.00	2.90	2.90	2.92	3.00	2.88	3.00	2.17	2.63	1.82	1.37
	σ	.898	1.126	.886	1.030	0	0	.548	.548	.324	0	.364	0	.922	.642	.886	.830

Table 1: Participants' scores for configuration understanding before (B4) and After checking each interface. Scores reported by configuration path (VF-Basic: did not apply (CP1) or applied recommended settings (CP2); Prototype: changed settings for each (CP1) or all (CP2) network context) and in total (T).

(partially complete) as did one of those with an incomplete mental model, while 16/28 with an incomplete mental model incorporated the full context of network location and connection into their mental model (complete). However, 11 still drew a contextually incomplete mental model.

In order2, before working with the firewall interfaces, 2 participants had an incorrect mental model of firewalls, while 28 participants had a correct but contextually incomplete mental model (incomplete). After using our prototype, one participant with an incorrect mental model moved to an incomplete one and the other moved to the complete mental model; and 22/28 participants with an incomplete mental model incorporated the complete context of network location and connection. Interestingly, after using VF-Basic, only 6/23 of participants with a complete mental model kept that mental model; 4/28 moved to a partially complete mental model which included only network connection context (visible in the advanced tab of VF-Basic (Figure 2C)). The rest (13/23) downgraded to an incomplete mental model.

These results contrast how our prototype and VF-basic affected participants' mental model of the firewall functionality. Several comments from participants as they drew their mental models illustrate their changing understanding. One from order1, whose first two mental models were classified as *incomplete*, described her *complete* mental model drawn after working with the prototype, "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, 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 (order1), whose mental models transitioned from *incorrect* to *complete* after using the prototype, said "I learned that you can customize it for different locations and connections". One participant (order2) described her mental model of both VF-Basic and our prototype through an example. She compared VF-Basic to a light switch at the entrance of house which controls the light for the house as a whole, but said that the prototype gives you the ability to turn the light on or off for each room.

6.2 Configuration Paths

Not all participants took the same path through the interface as they configured the firewall. We briefly describe their configuration paths for each prototype, as these impact the actual configuration achieved during the study.

When participants turned on the firewall in VF-Basic, it was turned on for the the current network location (public). Participants 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 (order1: 23; order2: 19) did not respond to this warning, in which case only public-bluetooth was on as bluetooth was the only enabled network connection (CP1 in Table 1). The remainder (order1: 7; order2: 11) applied the recommended settings ("Update settings now" (Figure 1J) or "Restore defaults"(Figure 2C)), resulting in the firewall being turned on for all network locations and connections (CP2 in Table 1).

With the prototype, participants could turn the firewall on for each network location (Figure 3F, CP1 in Table 1) or for all network locations and connections with the change settings link (Figure 3E, CP2 in Table 1). For those who used CP1 (order1: 11, order2: 9), three participants (order1: 1; order2: 2) turned the firewall on only for public network location; the rest turned it on for all network locations and connections. All participants who used CP2 (order1: 19; order2: 21) turned on the firewall for all network locations and connections.

6.3 Understanding of Firewall Configuration

We now present analysis 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 6 network contexts: 3 network connections (wireless, local area connection, bluetooth) within 2 network locations (public, private). We assigned a value of 0 for an incorrect response, 0.5 for unsure, and 1 for correct 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 1 provides the mean and SD 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.

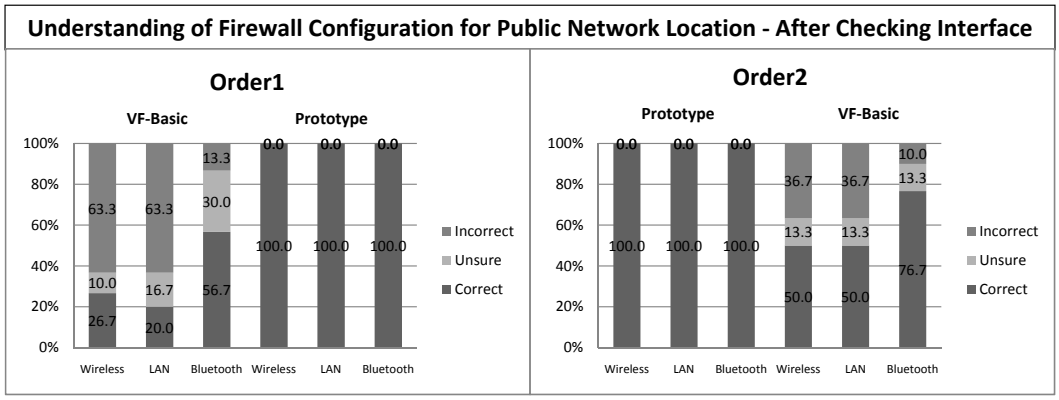

Figure 5: The average percentage of correct, incorrect and unsure answers in public network location after checking the interface for both order1 and order2.

6.3.1 Overall Understanding of Configuration

A fully repeated measures 2x2x2x2 mixed ANOVA, with one between subjects factor (order of interface presentation) and three within subject factors (interface, checking interface, network location) shows a significant main effect for interface (p=0.000, Partial Eta Squared=0.815); users' understanding of our prototype settings (μ=11.800 (out of 12, 6 for before/after checking the interface), σ=.8982) was significantly better than for VF-Basic (μ=6.575, σ=2.8371). Further analysis revealed that users' understanding of VF-Basic settings in order2 (μ=7.983, σ=2.0021) was significantly (t(58)=-4.404,p=0.000) increased in contrast to order1 (μ=5.167, σ=2.8748). This suggests that the mental models developed while using our prototype not only helped participants to understand its configuration, but 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 order1 reveals no significant difference for checking the interface or for the context of network location. It also does not reveal any significant interactions between factors. Whether or not participants' checked the interface to confirm their answers or considered the public or private network location, working with the prototype improved participants' understanding of their firewall security state in order1. After working with VF-Basic, less than 30% of participants in order1 correctly understood their setting 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 5 shows public location results).

A similar within subjects analysis of order2 shows a significant main effect of network location (F(1,29)=35.578, p=0.000). A fully repeated measures 2 (location) x 2 (checking) ANOVA, shows network location and checking do not have a significant effect on the prototype configuration understanding; however, we found a significant effect of network location (F(1,29)=38.184, p=0.000) and a significant interaction between checking and network location for VF-Basic. 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 1F).

Since VF-Basic only shows the firewall settings (on/off) for the user's current network location and our prototype showed all the settings, we also compared their responses with what we expected them to answer based on the information visible in the interface. For the private network location (raw score of 0 to 6), it is correct to be unsure as only the public security state is visible. A fully repeated measures 2 (interface) x 2 (checking) ANOVA, revealed a significant main effect for interface (order1: F(1,29)=64.51,P=0.000; order2: F(1,29)=5.009,P=0.033) indicating that overall correctness of understanding after using the prototype (order1: μ=5.80, σ=1.0954; order2: μ=5.883, σ=0.3640) was still higher than for VF-Basic (order1: μ=1.97, σ=2.282; order2: 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, these results show that for the private network location participants had more unsure answers in order2 than in order1; this demonstrates the learning effect of our prototype. After using the prototype, participants were more aware of 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 order2 describes, "for the private, I am just sure about the unsure one."

6.3.2 Pseudo Understanding of Configuration

Regardless of which configuration path participants used with the prototype, they understood the firewall security state in both order1 and order2 (Table 1). During post hoc analysis based on participants' configuration paths through VF-Basic, we found that in order1 those 7 participants who applied the recommended settings, had a higher percentage of correct responses than participants that did not. A fully repeated measures 2x2x2 mixed ANOVA, with one between subjects factor (applied/did not apply recommended settings) and two within subject factors (checking interface and network location) shows that this difference is significant (p=.000, partial Eta squared = 0.460). However, when comparing the results for 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=0.004)(Figure 6).

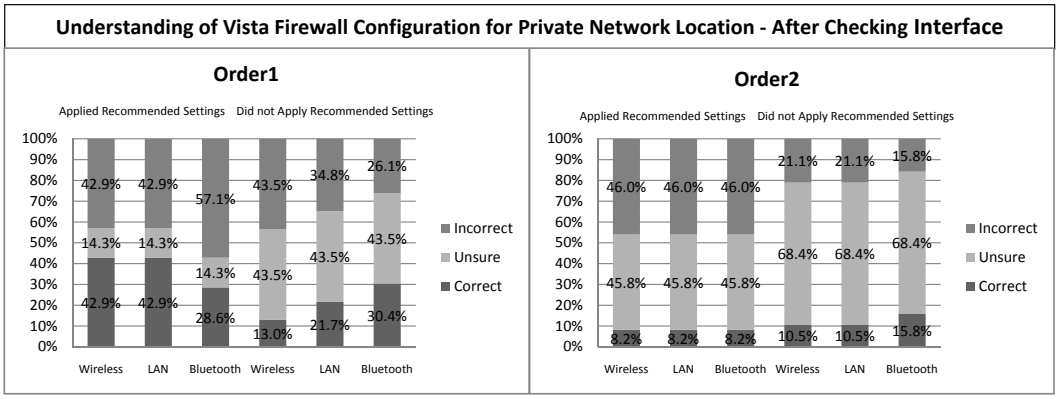

Figure 6: The average percentage of participants with correct, incorrect and unsure answers for the Firewall settings in private network location after checking VF-Basic.

This suggests that their apparent understanding of the VF configuration was shallow at best.

Upon inspection, participants appear unaware that the recommended settings had been applied to the private network location as well as their current public network location. Participants' comments confirmed their pseudo understanding of the settings after clicking "Update settings now" (Figure 1J) in response to the warning message. Before the six 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 Windows updates, or block all incoming connections. After clicking the link, the warning disappeared as the firewall was now turned on for all 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, participants were either still left with their misconceptions about what they had accomplished or were surprised that the warning was removed. Even the participant who had appeared to understand that it would enable the recommended security settings, discussed how the firewall would now be more efficient, so it is unclear exactly which recommended settings he thought were applied.

In order2 we did not find any significant difference for those who did or did not apply the recommended settings. In general, we had a larger percentage of unsure answers in order2 both for those who did and who did not apply the recommended settings than in order1. But, as can be seen in Figure 6, for order2 there were more incorrect answers for participants who applied the recommended settings. 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 before VF-Basic; our prototype made participants aware of different network contexts, and since they could not see any information about the private location in the VF-basic they may have thought that it is only on for public network location. Their comments about the "Update settings now" (Figure 1J) are similar to those made in order1, none in order2 understood that this link would apply the recommended settings (i.e., turn the firewall on for all network locations).

6.3.3 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." A recent study of WiFi use [19] reported that use of a firewall provides users with a sense of security that may extend beyond its actual protection. None of the participants were left in this dangerous state after using the prototype interface for both order1 and order2.

After working with VF-Basic, there is a relatively high proportion of incorrect responses for both order1 and order2 (Figure 7). Even after checking the interface, 42.2% of responses from order1 and 24.4% from order2 are incorrect for the current network location (public); these participants have an incorrect belief that they are protected for all network connections at the current network location. This is because VF-Basic's main window shows the current network location (Figure 1F), but does not indicate if it is turned on for 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 responses of order1 and 12.2% from order2 indicate dangerous misconceptions of the firewall being turned on for future private network locations when it is not.

As can be seen, participants in order2 had fewer dangerous misconceptions than those in order1. This could be the effect of presenting the prototype before VF-Basic which increased participants' awareness of network contexts, resulting in more unsure answers than dangerous misconceptions. As one participant from order2 mentioned, "the experience from previous firewall [prototype] helped me to understand the state."

6.4 Qualitative Feedback on Interface

6.4.1 Vista Firewall: Recommended Settings Unclear

During the experiment, VF-Basic showed a warning that

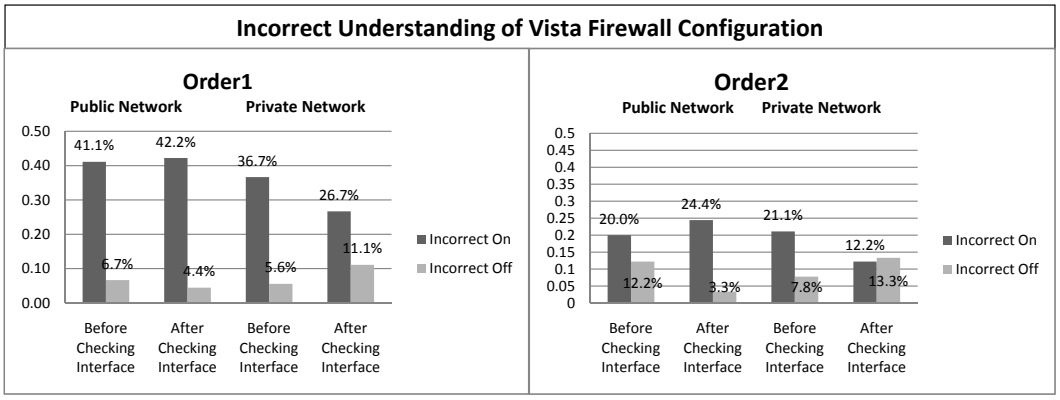

Figure 7: The percentage of incorrect responses after checking VF-Basic, . "Incorrect On" indicates the incorrect belief that the firewall is on, but it is off. "Incorrect Off" indicates the incorrect belief that the firewall is off, but it is on.

indicated that the recommended settings were not in place because the firewall was not on for all network locations and connections. As discussed above, VF was only turned on for the bluetooth connection in the public network location unless the recommended settings were applied. All 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 1I). As one participant from order1 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." P1 from order2 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 participants what they thought the security state of VF was given the feedback that it was turned on, but having feedback that it was not using the recommended settings. Almost all participants (56/60) were confused about why the firewall was not using the recommended settings: 31 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); 6 thought that the firewall should be updated, as one said after clicking on "Update settings" link, "Now it is on and uses its latest version"; 4 thought that it was because the public network was not a secure location and after reading the help files, thought that they should change it to private; 3 thought that the update feature of Windows should be turned on; and 1 thought that the firewall protection is weak. Only four participants recognized that it had to be turned on for all network connections (3 after following the help link provided in the warning, 1 after checking wireless and local area connection under the "Advanced" tab and restoring default settings). Furthermore, several participants had difficulty in understanding what to do with the information. As one from order1 stated, "I do not know much about firewalls, I prefer to use the recommended settings, but I cannot find it." Another participant from order2 went to change settings again after clicking on "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." As discussed before, 7 participants from order1 and 11 from order2 did end up applying the recommended/default settings.

These results show that our participants did not know what the recommended settings are, why the computer did not use the recommended settings, and how they could apply the recommended settings. VF-Basic does not provide feedback about the necessary contextual information or the functionality to set the firewall for all network contexts.

6.4.2 *Prototype Interface: Portrayal of Firewall State*

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 they preferred the prototype to VF-Basic. They liked the increased information about network context that was provided in both the state diagram and the configuration table. As one (order1) said, "The way that the second [prototype] interface presents the information about location and connection is a lot more obvious". They also appreciated the interaction abilities afforded within the interface. One (order1) explained, "The second [prototype] interface 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 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 turned off. Two participants in order1 and three in order2 commented that the picture should be modified with respect to the way that the incoming connections are portrayed, providing more detail 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.

6.4.3 *Underlying Functionality: Multiple Firewall Profiles*

Participants were asked how they would prefer firewall set-

tings to be applied to their computer. The majority (39/60) indicated they would like to have changes applied to all network locations and connections. This was thought to make the firewall easier to use as they would not have to worry about context, "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." For these participants, the multiple firewall profiles that are applied according to the context of the network locations and connections 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 Vista Firewall currently offers: 13 wanted the flexibility of having more control in specific locations; 4 wanted the settings applied to their current location; 3 wanted to have them applied to all, but have the ability to exclude some; 1 participant wanted flexibility to turn it on/off for connections, but not locations. One participant had the interesting notion of having changes that increased security applied to all connections/locations, but changes that would make things less secure applied only to a specific location.

7. DISCUSSION

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

7.1 Responding to Shifting Contexts

As is common [19], our diverse set of participants used their laptop computers in different network computing contexts. As our results show, participants often exhibited misunderstandings of their actual firewall configuration when working with VF-Basic. As discussed by Maxion et al. [20], "certain user interface constructs" cause human errors. VF-Basic does not make it clear to users how the firewall reacts to changes in network context, and the user is not always aware of the underlying 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 their system is secure for all 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 [21], 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 [35]. However, Vista Firewalls's underlying model has to be more clearly portrayed to the user so that they can develop an effective mental model of configuration changes.

7.2 Supporting Users' Mental Models of System State

Our results suggest that the inconsistency between users' mental model and VF functionality is due to insufficient information about variables of the system (computing context) that can affect the state of the firewall. The incomplete knowledge likely resulted in their increased uncertainty about the system state [34].

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 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 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 VF 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. Users must be made aware of the current and future consequences of their actions so that they can develop a correct mental model of the application functionality and avoid dangerous errors.

7.3 Balancing Complexity and Security

One of the main usability problems with VF is that its basic and advanced interfaces are designed at the two extreme ends of the complexity versus simplicity spectrum [2]. 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 VF and security applications in general. We found no obvious differences in the results attributable to participants' computer experience and security knowledge; regardless of their backgrounds, most participants struggled with understanding their configurations with VF-Basic. Further research is required to find which user attributes are important when evaluating usable security, particularly when considering multiple interfaces for basic and advanced users.

If separate interfaces are indeed necessary, how can devel-

opers 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 [21]. 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.

7.4 Role of Education

A common thread in usable security research is educating users [31]. 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 order2.

After the first 30 participants in order1, we did run an additional 10 participants who first viewed a simple training video (created from VF help) before beginning the study. We wanted to examine if the additional training would help participants to understand the security state of the firewll when working with VF-Basic. This video detailed the functionality of VF, including the correlation between the network context and the firewall profile and the crucial fact that changes made in VF-Basic would only be applied to the current network context.

Our simple training video may have had some impact on users' mental model of how the firewall works as none began with an incorrect mental model and there was also a decrease in incorrect answers resulting in fewer dangerous misconceptions (i.e., overall 55% fewer "incorrect on" than for order1); however, the video did not further promote inclusion of the contextual nature of the firewall in the users' mental model. As one participant said when asked why his mental model did not change when he watched the video, but did after using our prototype, "when it is interactive, when you do it yourself, it better remains in your mind." This is inline with our results of order2 which show interaction with our prototype had some effect on users' mental of model of underlying functionality of VF-Basic. It is 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 order2 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 the 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 [31]. 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.

8. CONCLUSION AND FUTURE WORK

Supporting users' understanding of the impact of their computing context on security software is particularly crucial as users become more mobile. We presented a study investigating how VF-Basic supports mental models of its operation and whether the addition of information about network context could better support the mental models and participants' understanding of its configuration. Our prototype interface for the firewall helped participants to develop a correct and contextual mental model of the firewall and dramatically increased their understanding of the effects of their firewall configuration. After using the contextually augmented prototype, no users had dangerous misunderstandings about their security state. Although hiding system features and operational details can make interfaces more usable, in the case of security software complexity must be balanced against security. Our findings will benefit those designing personal firewalls, other security software, or complex systems that adapt to changing contexts.

We intend to modify our prototype based on our findings. In particular, we will incorporate an interactive tutorial for novice users of the firewall to help them develop their mental models of its contextual functionality and make suggested modifications to the configuration table and dynamic image of the firewall state. We will also incorporate changes based on prior research [2] into the Vista Firewall usability, such as improving the link between the basic and advanced user interfaces and refining some of the terminology used. Beyond the usability of personal firewalls, we will continue to investigate the appropriateness of multiple interface design for security and configuration interfaces, particularly those that are dependent on the underlying system context.

9. ACKNOWLEDGMENTS

This research is funded by the Natural Sciences and Engineering Research Council of Canada. We thank all the participants of our user study and also LERSSE and IDRG members for their helpful feedback on the project.

10. REFERENCES

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

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

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

[4] S. Chiasson, P. C. van Oorschot, and R. Biddle. 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, July 2007.

[5] J. Coutaz, J. L. Crowley, S. Dobson, and D. Garlan. Context is key. *Commun. ACM*, 48(3):49–53, 2005.

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

[7] L. F. Cranor. 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, 2008. USENIX Association.

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

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

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

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

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

[13] A. Herzog and N. Shahmehri. User help techniques for usable security. In *CHIMIT '07: Proceedings of the 2007 symposium on Computer Human Interaction for the Management of Information Technology*, pages 93–102, Cambridge, Massachusetts, 2007. ACM.

[14] S. Hohn. Bringing the user back into control: A new paradigm for usability in highly dynamic systems. *Lecture notes in computer science*, pages 114–122, 2006.

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

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

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

[18] W. Karwowski. *International Encyclopedia of Ergonomics and Human Factors, Second Edition - 3 Volume Set*. CRC Press, Inc., Boca Raton, FL, USA, 2006.

[19] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. "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, 2009. ACM.

[20] R. A. Maxion and R. W. Reeder. Improving user-interface dependability through mitigation of human error. *International Journal of Human-Computer Studies*, 63:25–50, 2005.

[21] J. McGrenere, R. M. Baecker, and K. S. Booth. 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, 2002. ACM.

[22] Microsoft. Windows Vista Help: Choosing a network location.

[23] Microsoft. Windows Vista Help: What is a firewall.

[24] Microsoft. Microsoft's annual revenue reaches $60 billion. http://www.microsoft.com, 2008.

[25] Microsoft. Windows firewall with advanced security - content roadmap. http://technet.microsoft.com, 2008.

[26] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. Expandable grids for visualizing and authoring computer security policies. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, pages 1473–1482, New York, NY, USA, 2008. ACM.

[27] J. Rode, C. Johansson, P. DiGioia, R. S. Filho, K. Nies, D. H. Nguyen, J. Ren, P. Dourish, and D. Redmiles. 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, 2006. ACM.

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

[29] J. Stoll, C. S. Tashman, W. K. Edwards, and K. Spafford. 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, 2008. ACM.

[30] M. Tungare and M. Pérez-Quinones. Thinking outside the (beige) box: Personal information management beyond the desktop. In *Proceedings of the 3rd Invitational Workshop on Personal Information Management*, page 8 pages, 2008.

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

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

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

[34] K.-P. Yee. 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, 2002. Springer-Verlag.

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