Towards Improving Mental Models of Personal Firewall Users

Fahimeh Raja
University of British Columbia
Vancouver, BC, Canada
fahimehr@ece.ubc.ca

Kirstie Hawkey
University of British Columbia
Vancouver, BC, Canada
hawkey@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
Vancouver, BC, Canada
beznosov@ece.ubc.ca

CHI 2009, April 4 – 9, 2009, Boston, MA, USA
ACM 978-1-60558-246-7/09/04.

Abstract
Windows Vista's personal firewall provides its diverse users with a basic interface that hides many operational details. However, our study of this interface revealed that concealing the impact of network context on the security state of the firewall results in mental models that are unclear about the protection provided by the firewall resulting in an inaccurate understanding of the firewall configuration. We developed a prototype to support more contextually complete mental models through inclusion of network context information. Results from our initial evaluation of the prototype support our approach 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.

Keywords
Usable security, firewall, configuration, mental model

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces-Evaluation/Methodology; D.4.6 Software: Security and Protection-Information flow controls

Introduction
One key to usable security is mitigating the gap between what a system does and the mental models that users have [8, 10]. While an effective mental

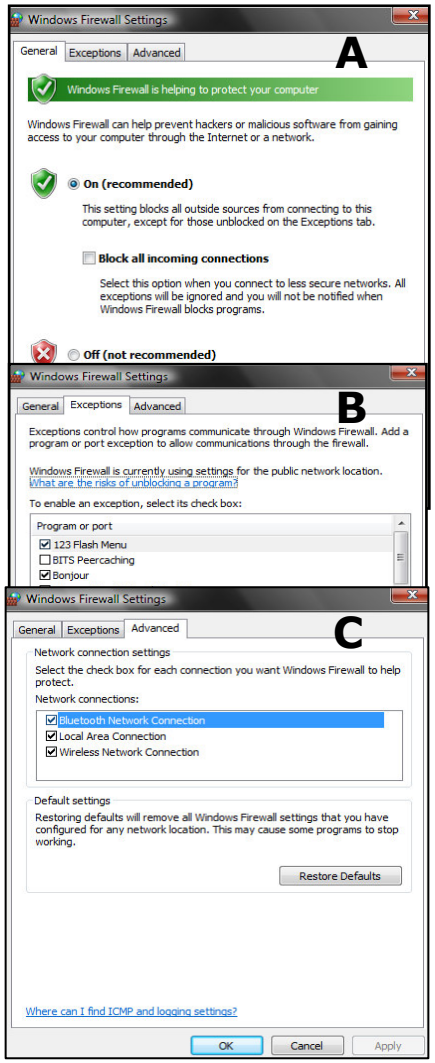

figure 1. Tabs in second window of VF-basic: A. General, B. Exceptions, C. Advanced.

model does not need to include all technical details, it does need to allow users to predict the consequences of their actions [2]. Enough detail must be provided so that users can make informed decisions as they interact with security tools [4]. Prior usable security research has mainly focused on helping users understand their configuration of the *current* security state [2, 7, 10]. However, as users become more mobile, we argue that it is necessary to help them also understand the consequences of their actions on *future* security states (e.g., when in a different network context).

In Windows Vista, Microsoft introduced a personal firewall which provides a basic user interface (VF-basic) for home users of Windows Vista and an advanced one (VF-advanced) for IT professionals. This firewall incorporates the context of network location and connection type. 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 [1]; however, in security applications it may be infeasible to remove the human from the loop [3].

Evaluations of the VF interface during student projects revealed that hiding the effect of network context in VF-basic may result in users developing a poor mental model, which we believed could cause dangerous errors. We designed a prototype that, as suggested by Edwards et al. [5], more explicitly represents the network context and its impact on the firewall's security state. Our study of VF-basic and our prototype provides an initial exploration of mental model development during personal firewall use. Initial results suggest that including contextual information about the network improves the completeness of participants' mental models, resulting in fewer dangerous misconceptions of their firewall configuration. We next describe the underlying functionality of the Vista Firewall, the design of our prototype interface, and our study protocol. We then present our initial findings, discuss the implications of our results for developers of security applications, and conclude with future research plans

Windows Vista Firewall

In Windows Vista, the first time a user connects to a network, he must classify it as *home*, *work*, or *public*. Vista Firewall (VF) has three network locations, which correspond to 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). In each network location, the user can also enable or disable the firewall for three connection types: wireless, local area connection, and Bluetooth, for a total of nine network contexts. When a user configures the firewall through VF-basic, changes will be applied to the current profile and automatically used in future for every network with the same location type [9]. Configuration status is shown as one of three security states (on, off, on for current location; see Fig. 2). A second window with three tabs[1] (Fig.1) is displayed when the "change settings" link in the main window (Fig. 2A) is clicked.

[1] A) General (Fig. 1A): To turn the firewall on or off. When the user turns the firewall on, she has the option to block all incoming connections; B) Exceptions (Fig. 1B): to set exceptions of programs and ports for which inbound connections are allowed; and C) Advanced (Fig. 1C): to enable or disable the firewall for different network connections and restore the default settings of the firewall.

1) The firewall is on (protecting the computer) for all network locations and all network connections; it is using the *recommended settings.*

2) The firewall is off for the current network location.

3) The firewall is on for the current network location, but it is not on for all network locations and connections.

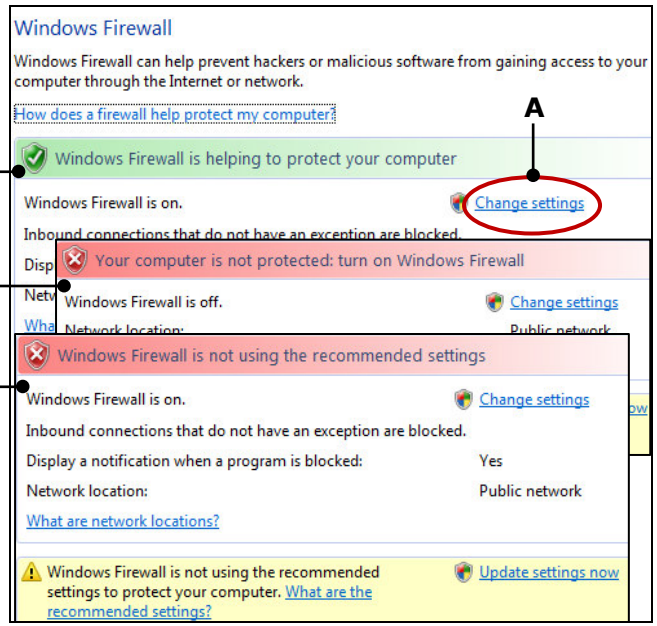

figure 2. Main window of VF-basic, with two inset panels showing different security configurations.

Table 1: Participants' technical experience and expertise.

Technical experience and expertise		N
Vista experience	Yes	15
	No	15
Firewall experience	Yes	15
	No	15
Computer expertise	Basic	21
	Advanced	9
Security expertise	Low	6
	Medium	20
	High	4

Prototype Interface

Our prior course projects evaluating VF-basic and VF-advanced revealed that VF-basic has insufficient contextual information. To evaluate whether an inclusion of contextual information in VF-basic would help users develop richer mental models of VF's functionality, we designed a prototype of an enhanced basic interface (Fig. 3). To isolate the effect of our changes, we imitated Vista's design, using its colors, images, text, and terminology. We used elements from VF-advanced to incorporate contextual information. We iteratively refined our prototype with 13 pilot testers. After applying their feedback, we consulted them again and asked whether the changes made addressed their concerns. Our final prototype provides a *dynamically updated image* (Fig. 3A, modified from one in VF help) to help users visualize network contexts for VF. In this image, each connection is shown with an arrow. A green arrow indicates that the firewall is on for that connection and the connection is protected; a red arrow means that the connection is not protected. Icons from the "Customize Network Settings" of Windows Vista are added to help distinguish different network locations (e.g., a bench for public network location, Fig. 3B). On the recommendation of three of the pilot testers, we added a configuration *table* (Fig. 3C) in the "General" tab of the secondary window. This table 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 the configuration with information about the firewall state is supported by design principles for security systems [7]. In the "Exception" tab, 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 and disable the firewall for different network connections was incorporated throughout our prototype, it no longer required an "Advanced" tab.

Study protocol

We conducted a one-hour lab study with a diverse set of 30 participants (Table 1). After completing a background questionnaire, participants were given picture cutouts of a computer, a firewall, and the Internet cloud and asked to arrange these on a sheet of paper and draw arrows to show how they think VF works. They were then asked to comment on the security state of the firewall based on information visible in VF-basic before undertaking two common firewall tasks: to turn the firewall on and to block a program (Yahoo messenger) through the firewall.

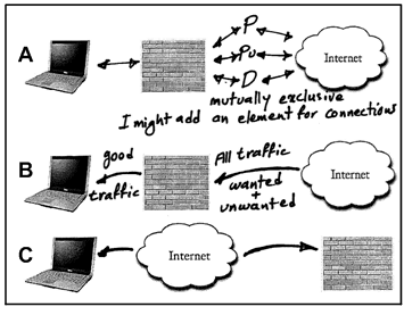

figure 4. Representative drawings reproduced from ones drawn by participants. A. Complete mental model, B. Incomplete mental model, C. Incorrect mental model.

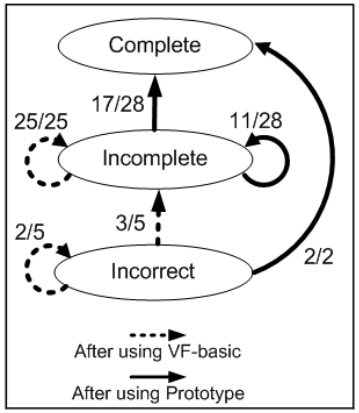

figure 5. Transitions in participants' mental models.

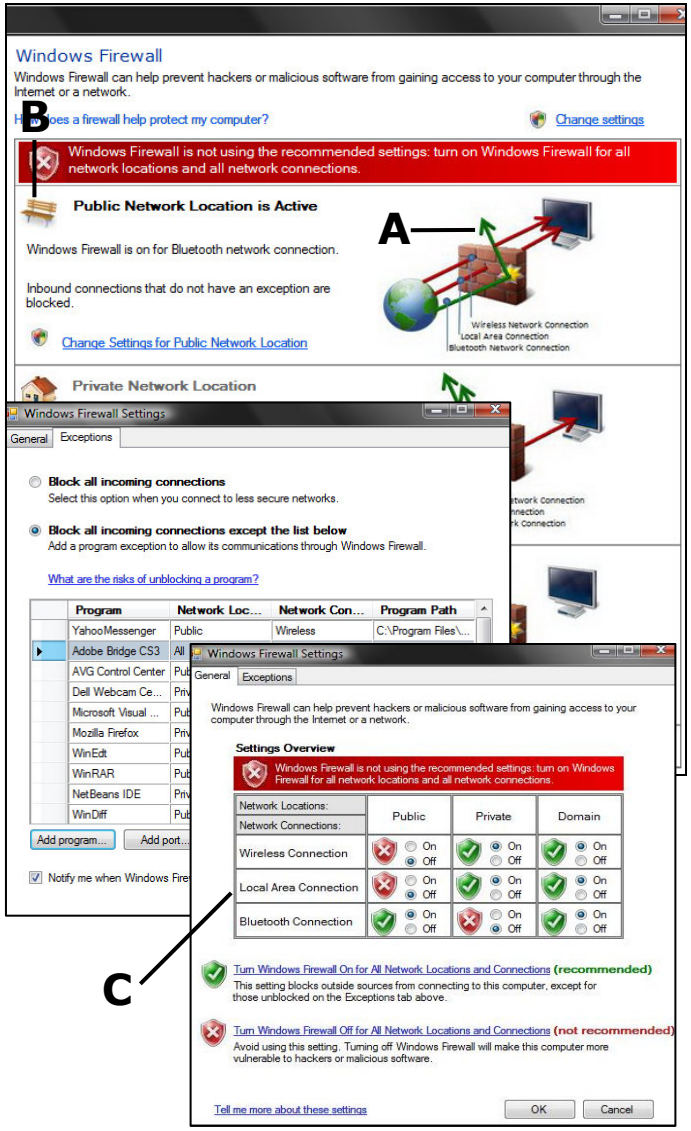

figure 3. Prototype Interface

After the tasks, we briefly interviewed participants about their understanding of the effect of their actions on the security state of the computer. We also asked them to re-draw their mental model and fill out a configuration table indicating whether they thought the firewall was on, off, or they were unsure for each of the nine possible network location/connection contexts. They did this first without looking at VF-basic (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 current and future security states). We repeated the same process for our prototype interface. We are continuing our study with more participants who use the prototype *before* VF-basic to examine whether the presentation order of the interfaces impacts our initial findings.

Results

Mental Models

We categorized participants' drawings of their mental model as *incorrect* (incorrect basic understanding of the inner workings of a firewall), *incomplete* (correct basic understanding of a firewall operation, without network context), or *complete* (correct, with network context) (Fig. 4). We examined their transitions between the categories (Fig. 5). Initially, 5 participants had an incorrect mental model, while 25 had a correct but incomplete one. After using VF-basic, 3/5 moved from the incorrect mental model to an incomplete one; however, none changed to include network context. After using our prototype, 19 participants incorporated complete network context into their mental model. It is possible that participants were primed about the study protocol when using VF-basic and were more careful about the network context when working with our prototype; our continuing study will clarify this.

Table 2. Scores for participants' understanding of VF configuration before and after checking VF-basic.

VF-basic		Mean	SD
Public	Before	1.23	0.898
	After	1.30	1.126
Private	Before	1.32	0.886
	After	1.32	1.030

Table 3. Scores for participants' understanding of VF configuration before and after checking the prototype.

Prototype		Mean	SD
Public	Before	3.00	0.0
	After	3.00	0.0
Private	Before	2.90	0.548
	After	2.90	0.548

Understanding of Firewall Configuration

We now present initial analysis of understanding the effects of the firewall configuration tasks based on participants' completion of the configuration table and their comments. As the domain settings are not within the control of end users, we omit that data and focus on 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. Then, we computed a raw score representing the correctness of understanding of the firewall configuration. Tables 2 and 3 provide the mean and SD of scores, summed for each network location.

Our analysis reveals that after working with VF-basic less than 30% of participants correctly understood their setting for each network context, even when given the opportunity to check the settings through the interface. The low score for private network location indicates that participants were not aware that the firewall settings visible in VF-basic are only for their current network location (public). In contrast, almost all participants were correct in their understanding of the settings after using our prototype.

Dangerous misconception

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 off. It is the second type of error that leaves users in a dangerous state, vulnerable to attacks and malicious software. As one participant said, "you will be more careless because you think you have been protected rather than [if] there is not any firewall." After working with VF-basic there is a relatively high proportion of "incorrect on" responses (fig. 6). Even after checking the interface, 41% of participants had an incorrect belief that they were protected for all network connections at the *current* public network location and 27% had dangerous misconceptions of the firewall being turned on for the *future* private network locations when it was not. After using the prototype, none of the participants were left in this dangerous state.

Discussion

As discussed in [6], "certain user interface constructs" cause human errors. The VF-basic interface does not make it clear how VF reacts to changes in network context; participants exhibited misunderstandings of firewall configuration when working with it. Our initial findings demonstrate that VF-basic does not provide enough contextual information about variables of the system (computing context) that can affect the security state of the VF. This results in inconsistency between their mental model and VF functionality. Revealing the hidden context in our prototype resulted in more effective mental models.

The current design of VF-basic suits a non-changing network context (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. Interestingly, 22/30 participants indicated that they don't necessarily want a correlation between network context and the firewall settings (as was the case for the XP firewall). For those users or for users who are not mobile, one option is to allow them to configure their firewall to only have one profile.

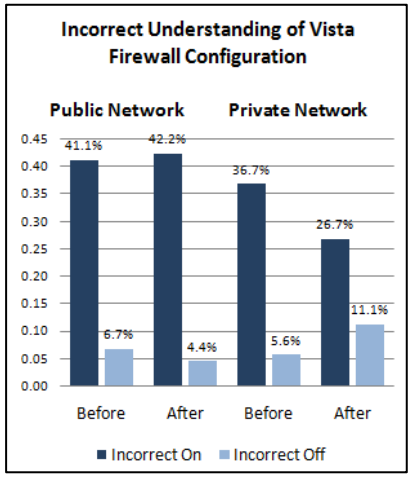

figure 6. Percentage of incorrect responses: "Incorrect On" indicates the incorrect belief that the firewall is on, but it is off. "Incorrect Off" indicates the incorrect belief that the firewall is off, but it is on.

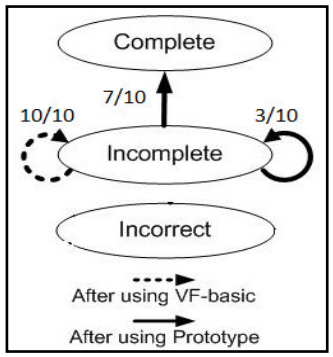

figure 7. Transitions in participants' mental models for those who watched the training video before taking part in the study.

To see if additional training could overcome the limitations of VF, we also ran an additional 10 participants who viewed a training video before beginning the study. This video, which we made with information from VF help, detailed the functionality of VF, including the relationship between the network context and VF profile. As seen in Fig. 7, our training video may have some impact on participants' mental models of firewall as none began with an incorrect model; however, there was no increased inclusion of the contextual nature of the firewall. There was also a decrease in incorrect answers resulting in fewer dangerous misconceptions, i.e., overall 55% fewer "incorrect on" responses.

Based on our initial results, 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.

Conclusion

Supporting users' understanding of the impact of their computing context on security software is particularly crucial as users become more mobile. Hiding system features and operational details can make interfaces more usable; but in the case of security software, complexity must be balanced against security. We presented an initial study of VF-basic which highlights the dangers of hidden complexity. We are continuing our study to further examine whether providing additional information about network context better supports users' mental models and understanding of their configuration. Our findings will benefit those designing personal firewalls, other security software, or complex systems that adapt to changing contexts. Beyond evaluating the effectiveness of our prototype and usability of personal firewalls, we will continue to investigate configuration interfaces, particularly those that are dependent on the underlying system context.

References

[1] Chen, G. and Kotz, D. *A survey of context-aware mobile computing research*. TR2000-381, Dartmouth College (2000).

[2] Chiasson, S., van Oorschot, P. C., and Biddle, R. Even experts deserve usable security: Design guidelines for security management systems. In *USM 2007*, 4 pages.

[3] Cranor, F. L. A framework for reasoning about the human in the loop. In *UPSEC '08* (2008).

[4] De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J., and Filho, R. S. Two experiences designing for effective security. In *SOUPS '05* (2005), 25-34.

[5] Edwards, W. K., Shehan, E., Stoll, J. Security Automation Considered Harmful? In *NSPW '07* (2007).

[6] Maxion, R. A. and Reeder, R. W. Improving user interface dependability through mitigation of human error. *Int. J. Hum.-Comput. Stud.* 63, 1-2 (2005), 25-50.

[7] Rode, J., Johansson, C., DiGioia, P., Filho, S., Nies, K., Nguyen, D. H., Ren, J., Dourish, P., and Redmiles, D. Seeing further: extending visualization as a basis for usable security. In *SOUPS '06* (2006), 145-155.

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

[9] Windows Vista Help: Choosing a network location.

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