Revealing Hidden Context
Improving Users’ Mental Models of Personal Firewalls

Fahimeh Raja
Kirstie Hawkey and Konstantin Beznosov
Outline

• Background
• Windows Vista firewall - usability issues
• Prototype: revealing hidden context
• User study
• Results
• Conclusions
Initial Motivation
Users Need to Understand the Effect of Configuration on the System’s Security State

• Any active actors and authority relationships that affect security state should be visible to the user.

• Users should be able to assess security state for their immediate needs.
  – Visualizing system activity
  – Integrating configuration and action

• Users should be able to determine current security state.
  – Sufficient feedback
Our Study

As users become more mobile, it is increasingly important to understand the security state for both current and future contexts of use.

***

The changes must be revealed, if security state changes based on the underlying context

Otherwise

The hidden context can leave user in dangerous situations.
Network Location
in
Windows Vista
Personal Firewall
in
Windows Vista
Context Dependent Functionality

Settings *automatically* applied depending on network context detected

- **Public** (public networks)
- **Private** (home / work networks)
- **Domain** (controlled by Windows domain admin)
## Network Context in Vista Firewall

<table>
<thead>
<tr>
<th>Network Context</th>
<th>Public Network Location</th>
<th>Private Network Location</th>
<th>Domain Network Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Connection</td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Local Area Connection</td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Bluetooth Network Connection</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
2 User Interfaces:
Basic and Advanced
- not intended for average users
- complex
Limited functionality and simplified interface to hide complexity from user

Does not provide necessary contextual information for the functionality it does support
Changes applied **only** to profile associated with current network location and that is not obvious.
Simplified interface:

• Hidden network context
• Automatic switching of firewall profiles

But at a cost!
What is the Cost?

- Users can be left in a **dangerous situation**
  - Only protected in the current network context
  - But, believing to be protected for future network contexts

- Must remember to replicate the change, if a similar change is wanted for future networks
Proposed Alternative Interface:
Reveals the Hidden Context
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

- **Public Network**: Windows Firewall is on for Bluetooth and wireless connections. Inbound connections that don't have exceptions are blocked.

- **Private Network**: Windows Firewall is on for all network connections. Inbound connections that don't have exceptions are blocked.

- **Domain Network**: Windows Firewall is on for all network locations and connections. This setting blocks outside sources from connecting to this computer, except for those unblocked on the Exceptions tab above.

- **Turn Windows Firewall On for All Network Locations and Connections (recommended)**: This setting blocks outside sources from connecting to this computer, except for those unblocked on the Exceptions tab above.

- **Turn Windows Firewall Off for All Network Locations and Connections (not recommended)**: Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings
User Study
Goal

To investigate the impact of addition of contextual information to Vista Firewall basic interface on:

- Users’ mental model of Vista Firewall functionality
- Users’ understanding of Vista Firewall configuration
Study Design

• Within-subjects lab study

• Screen and voice recorded

• Recruitment:
  – Online classifieds: Craigslist, Kijiji
  – University email lists
  – Flyers: posted and handed out
    • University
    • Vancouver public places

• Participants:
  – 13 pilot testers
  – 60 actual study
    ✔ 30 first Vista firewall basic interface, then our interface
    ✔ 30 first our interface, then Vista firewall basic interface
  – 10 training at the beginning
Gender Balance

30  30
All Daily Computer Users

Windows
Vista
Windows XP
Linux
Mac OS
Windows 2000
Context of Use

![Pie chart showing the distribution of user contexts: Desktop users, Laptop users, Laptop and Desktop users, One network context, Variable network context.]

- Desktop users
- Laptop users
- Laptop and Desktop users
- One network context
- Variable network context
Study Protocol

Introduction to the Context

Mental Model

As you know we can use different network connections to connect to the Internet, like wireless or a cable. For this experiment, I set the laptop to use a wireless connection. I also can set my network for different network locations, for example public network like a coffee shop, or private network like at home. First, let’s set the location to public. Could you do that?

<table>
<thead>
<tr>
<th>Network Connection</th>
<th>Public Network Location</th>
<th>Private Network Location</th>
<th>Domain Network Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Area Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth Network Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Results
Mental Models

• Incorrect
• Incomplete
• Partially complete
• Complete
Mental Models

- Incorrect: incorrect basic understanding of firewall operation
Mental Models

• Incorrect

- Incomplete: correct basic understanding of firewall operation, without context of network location and connection
Mental Models

- Incorrect
- Incomplete

Partially complete: correct basic understanding of firewall operation, with either context of network location or connection
Mental Models

• Incorrect
• Incomplete
• Partially complete

Complete: correct basic understanding of firewall operation, with both context of network location and connection
First Vista Firewall Basic, then Alternative

Complete

Partially complete

Incomplete

Incorrect

Initial

After VF

After Alt

Complete

Partially complete

Incomplete

Incorrect
First Alternative, then Vista Firewall Basic

Complete
Partially complete
Incomplete
Incorrect

Initial  After Alt  After VF
# Understanding Firewall Configuration

<table>
<thead>
<tr>
<th>Network Connection</th>
<th>Public Network Location</th>
<th>Private Network Location</th>
<th>Domain Network Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Connection</td>
<td>On ×</td>
<td>On ×</td>
<td>Unsure</td>
</tr>
<tr>
<td>Local Area Connection</td>
<td>On ×</td>
<td>Off ×</td>
<td>Unsure</td>
</tr>
<tr>
<td>Bluetooth Network Connection</td>
<td>On ✓</td>
<td>Unsure</td>
<td>Unsure</td>
</tr>
</tbody>
</table>
Understanding Firewall Configuration
Public Network

Vista-basic: large % of incorrect
Alternative interface: Understood config.
Incorrect Understanding of **Vista** Firewall Configuration

Incorrect off: Incorrectly believe that firewall is off, when it is on

Incorrect on: Incorrectly believe that firewall is on, when it is off
Feedback on Vista Firewall Basic Interface

“For some reason it is not on, the first thing that I am looking at is this red. This states to me is 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.”

Personal trainer-Laptop user with medium level of security experience
Feedback on Alternative Interface

• 56 (93%) participants liked images, fine-grained control

“The second interface is much better. The pictures are very instructive. I have more control on it and that is nice.”

Librarian-Both laptop and desktop user

• Some confusion about firewall state diagram

“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.”

Grad Student in Electrical Eng.-Both laptop and desktop user
Multiple Firewall Profiles

• 39 (65%) participants preferred to have only one profile
  – Easier to use as they would not have to worry about context
  – Would avoid confusion
  – The multiple firewall profiles adds overhead without a perceived benefit

“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.”

Undergrad Student in Biology-Laptop user
Conclusions

• Design of Vista Firewall basic interface does not provide enough context for mobile users
  – If unaware that configuration changes only applied to current network location, may be left with dangerous misconceptions

• The users’ mental models can be supported by revealing the hidden context
  – Possible to balance complexity with security
Summary

• **Study:**
  – Mental models of Vista Firewall
  – How VF-Basic and our interface support users’ mental model of Vista Firewall functionality
  – Understanding of the effect of Vista Firewall configuration

• **Contributions:**
  – Highlight the dangers of hidden context
  – Provide an initial exploration of developing more effective mental models
    • Through feedback about security state in both current and future computing contexts
Revealing Hidden Context
Improving Users’ Mental Models of Personal Firewall

Fahimeh Raja             Kirstie Hawkey           Kosta Beznosov

Education and Research in Secure Systems Engineering

Laboratory
Windows 7 Firewall

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?
What are network locations?

- **Home or work (private) networks**
  - On
  - Block all connections to programs that are not on the list of allowed programs
  - None
  - Notify me when Windows Firewall blocks a new program

- **Public networks**
  - On
  - Block all connections to programs that are not on the list of allowed programs
  - Network
  - Notify me when Windows Firewall blocks a new program

Timeline:

- **1st phase**
  - May 08
- **CHI**
  - Sept. 08
- **2nd phase SOUPS**
  - Jan. 09
  - Feb. 09
- **CHI poster**
  - Apr. 09
  - May 09
  - Jun. 09
- **Presentation**
  - Jul. 09
- **Public Beta show**
- **Release candidate available**
Possible states

Your computer is not protected: turn on Windows Firewall

Windows Firewall is off.
Network location: [Public network]

What are network locations?

Windows Firewall is not using the recommended settings

Windows Firewall is on.
Inbound connections that do not have an exception are blocked.
Display a notification when a program is blocked: Yes
Network location: [Public network]

What are network locations?

Windows Firewall is not using the recommended settings to protect your computer. [What are the recommended settings?]

Update settings now

Windows Firewall is helping to protect your computer

Windows Firewall is on.
Inbound connections that do not have an exception are blocked.
Display a notification when a program is blocked: Yes
Network location: [Public network]

What are network locations?
Incorrect Understanding of **Vista** Firewall Configuration

Incorrect off: Incorrectly believe that firewall is off, when it is on
Incorrect on: Incorrectly believe that firewall is on, when it is off

Vista - Alt

<table>
<thead>
<tr>
<th></th>
<th>Incorrect On</th>
<th>Incorrect Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>42.2%</td>
<td>4.4%</td>
</tr>
<tr>
<td>Private</td>
<td>24.4%</td>
<td>11.1%</td>
</tr>
</tbody>
</table>

Alt - Vista

<table>
<thead>
<tr>
<th></th>
<th>Incorrect On</th>
<th>Incorrect Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>3.3%</td>
<td>13.3%</td>
</tr>
<tr>
<td>Private</td>
<td>12.2%</td>
<td>11.1%</td>
</tr>
</tbody>
</table>
Understanding of Configuration
Public network- after checking interface

Vista-basic: large % of incorrect
Alternative interface: Understood config. (100% correct)
Shifting complexity and actions to the system


BUT

Concealing system details as a means of reducing complexity may leave users in dangerous situations.
Future work

• Filed study examining what users know about or expects from a personal firewall

• How it would affect design and usability of personal firewalls
Understanding Firewall Configuration
Public Network- Before Checking Interface

Vista-basic: large % of incorrect
Alternative interface: Understood config.
Security Experience

How do you assess your experience of computer security?

- Install updates
  - regularly
  - rarely
  - never

- Scan for spyware and other potentially unwanted software
  - regularly
  - rarely
  - never

- Change security settings of Internet browser
  - regularly
  - rarely
  - never

- Delete browsing history and cookies
  - regularly
  - rarely
  - never

- Set different security controls for different users
  - regularly
  - rarely
  - never

- Manage browser add-ons
  - regularly
  - rarely
  - never