



Revealing Hidden Context

Improving Users' Mental Models of Personal Firewall

Fahimeh Raja

In SOUPS '09: Proceedings of the 5th symposium on Usable privacy and security

Shifting complexity and actions to the system

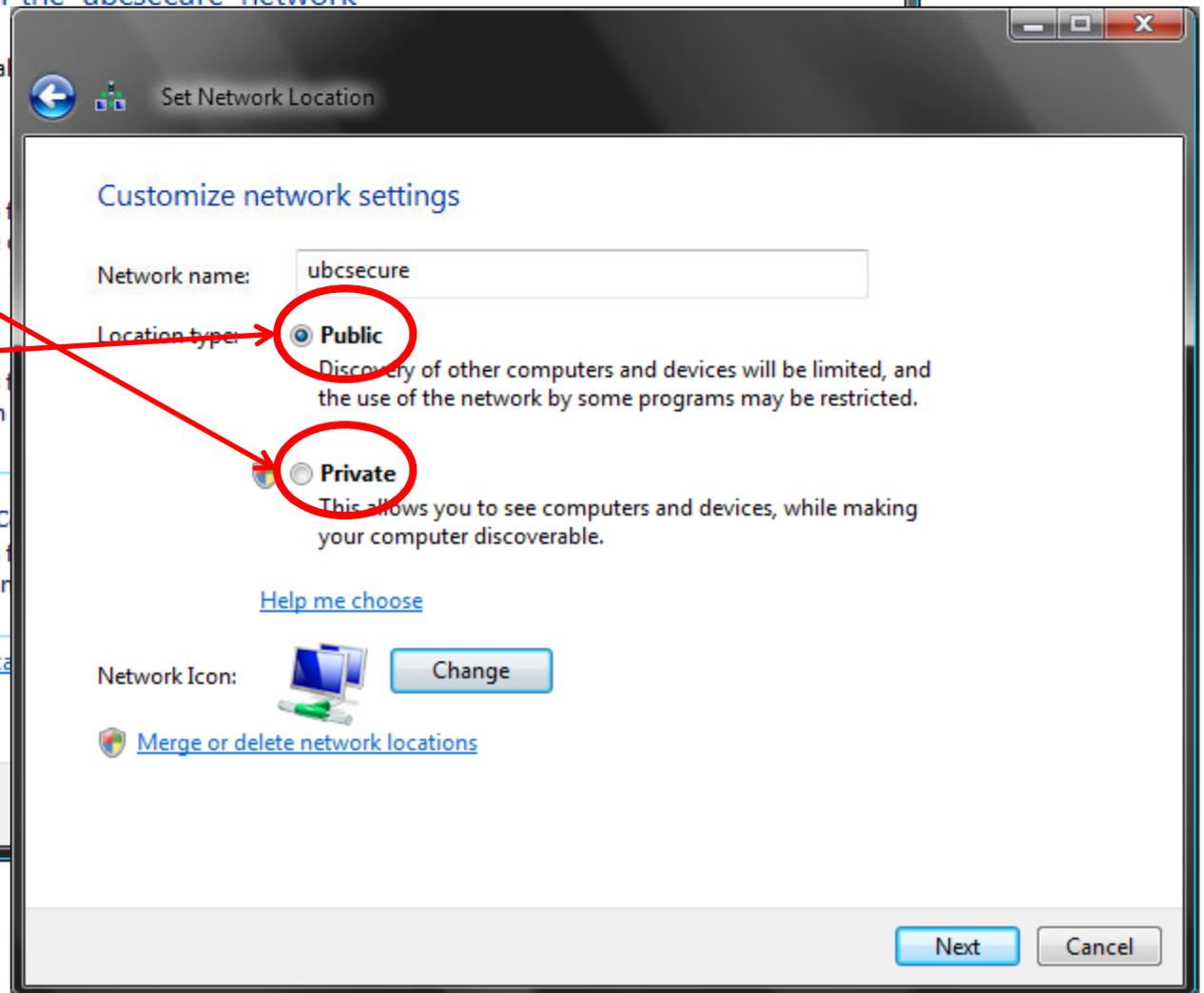
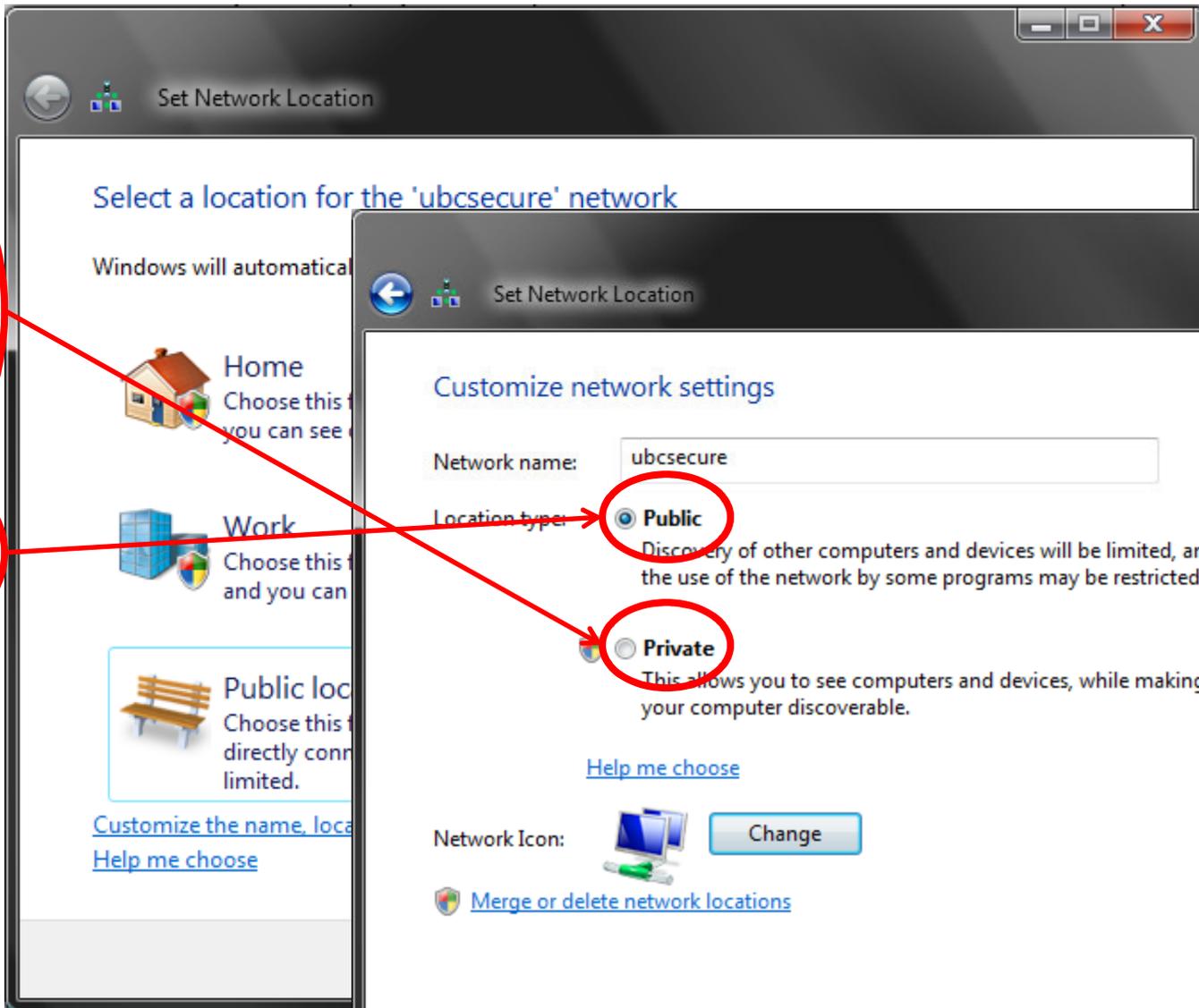
BUT

Concealing system details as a means of reducing complexity may leave users 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)

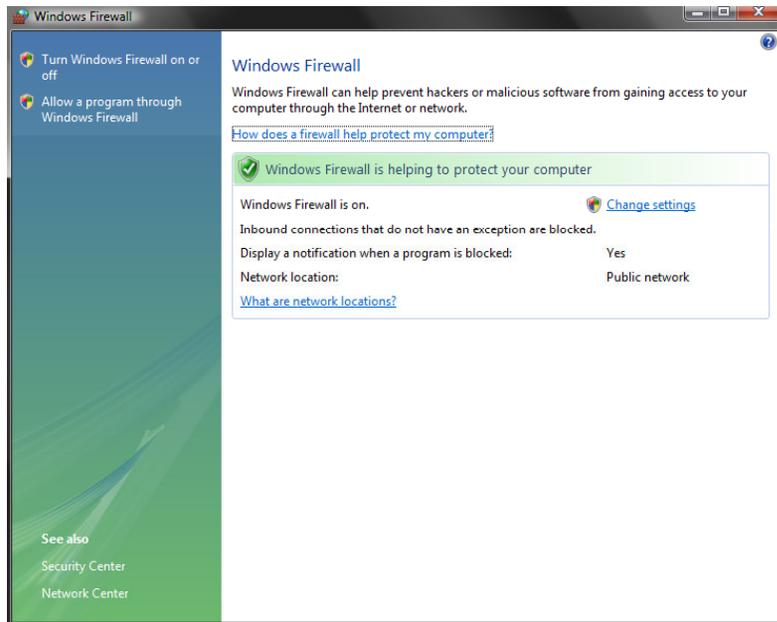


Domain (controlled by network admin)

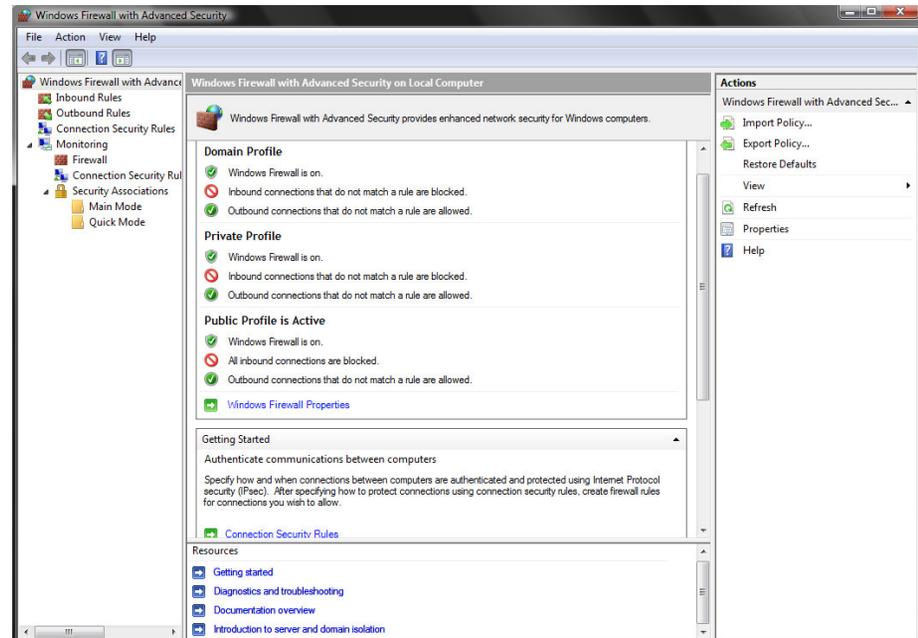


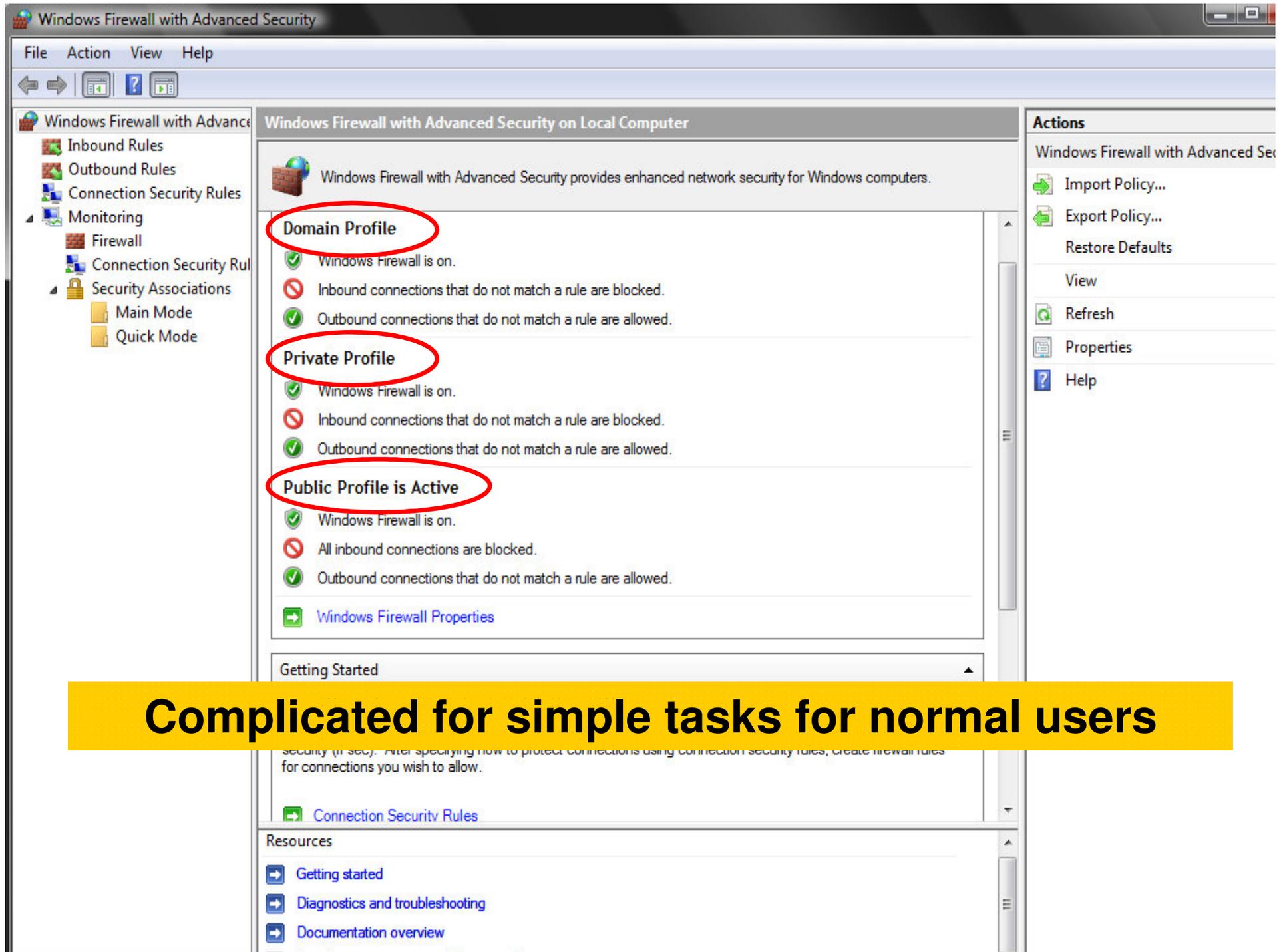
Interface

Basic

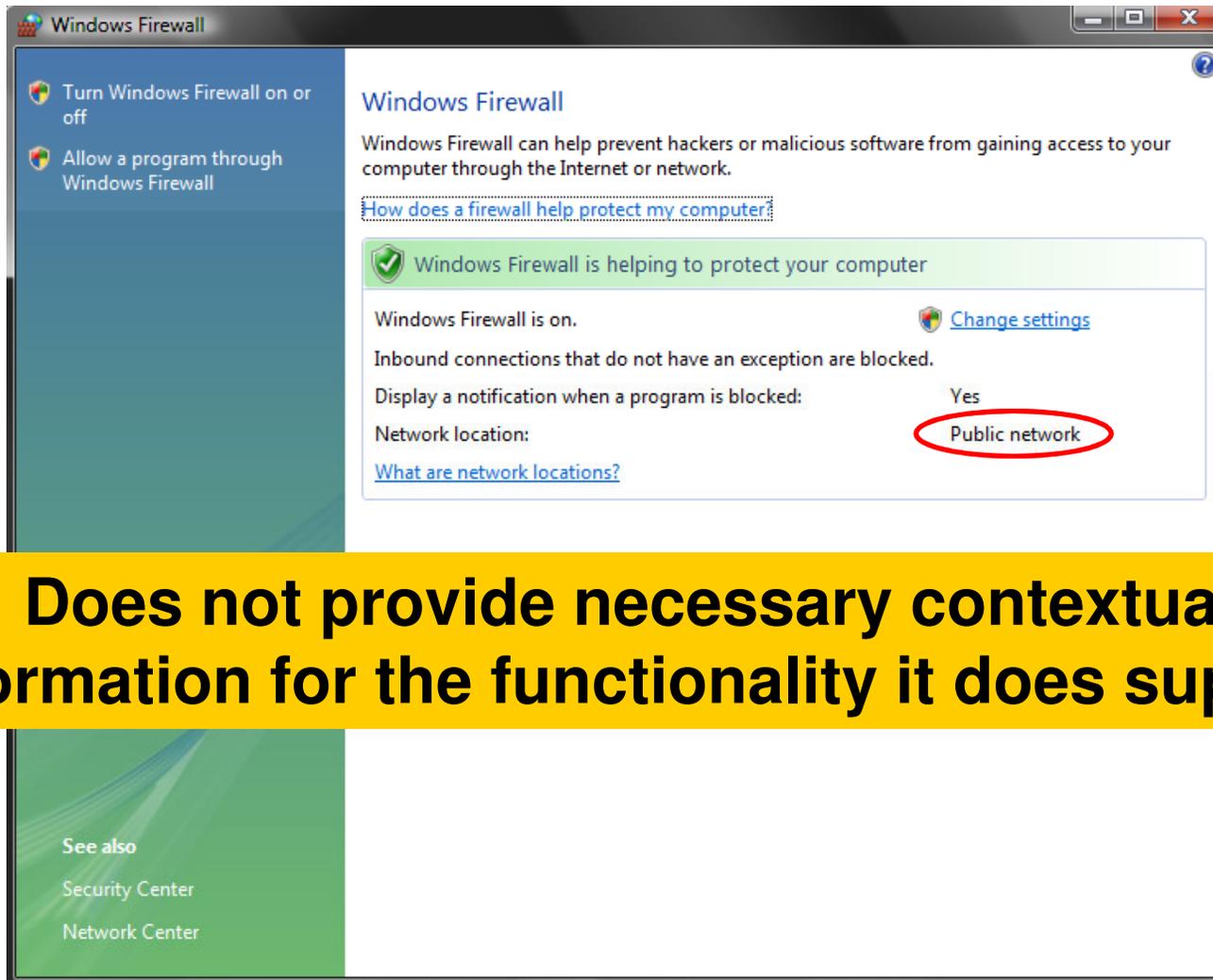


Advanced



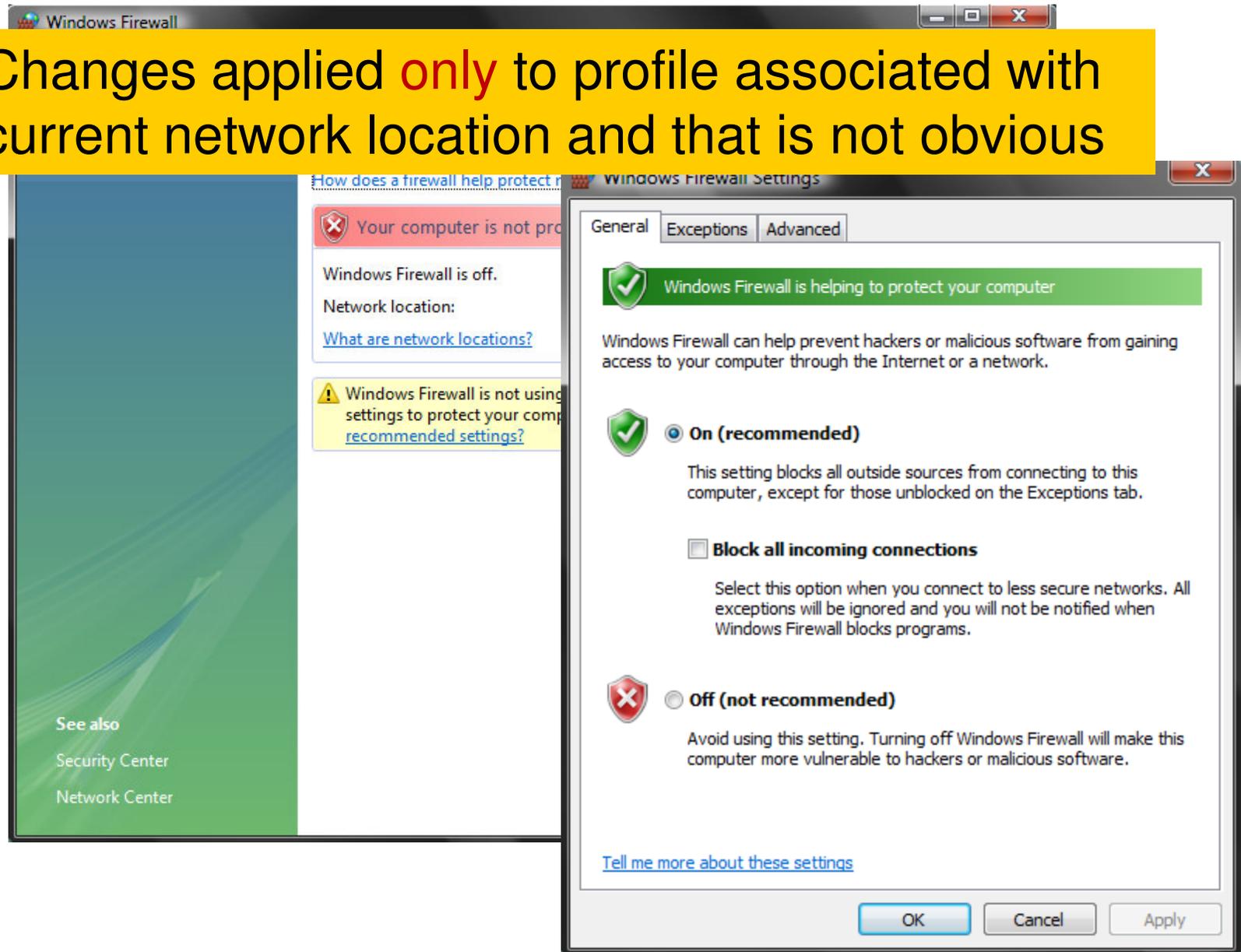


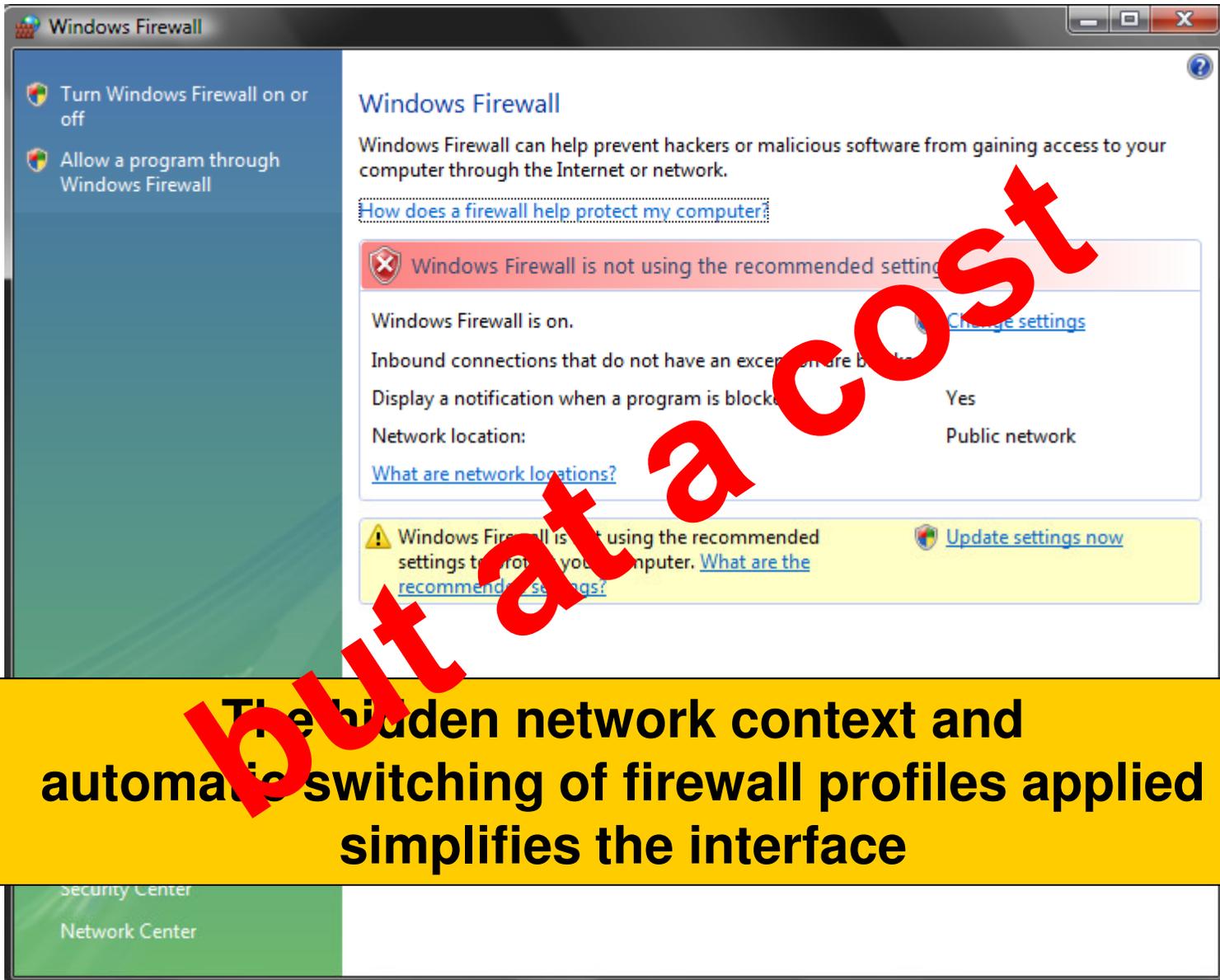
Limited functionality and simplified interface to hide complexity from user



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





The hidden network context and automatic switching of firewall profiles applied simplifies the interface

The cost?

- Users can be left in a dangerous situation, believing that they are protected in their current and all future network contexts
- If a similar change is wanted for future networks (different location profile), user must remember to replicate the change

**Proposed alternative interface
reveals the hidden context**

- Turn Windows Firewall on or off
- Allow a program through Windows Firewall

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?

Windows Firewall network locations

[Change settings for Public Network](#)

Public Network

Windows Firewall is on for this network location.

Inbound connections that are blocked:

[Change Settings for Public Network](#)

Private Network

Windows Firewall is on for this network location.

Inbound connections that are blocked:

[Change Settings for Private Network](#)

Domain Network

Windows Firewall is on for this network location.

Inbound connections that are blocked:

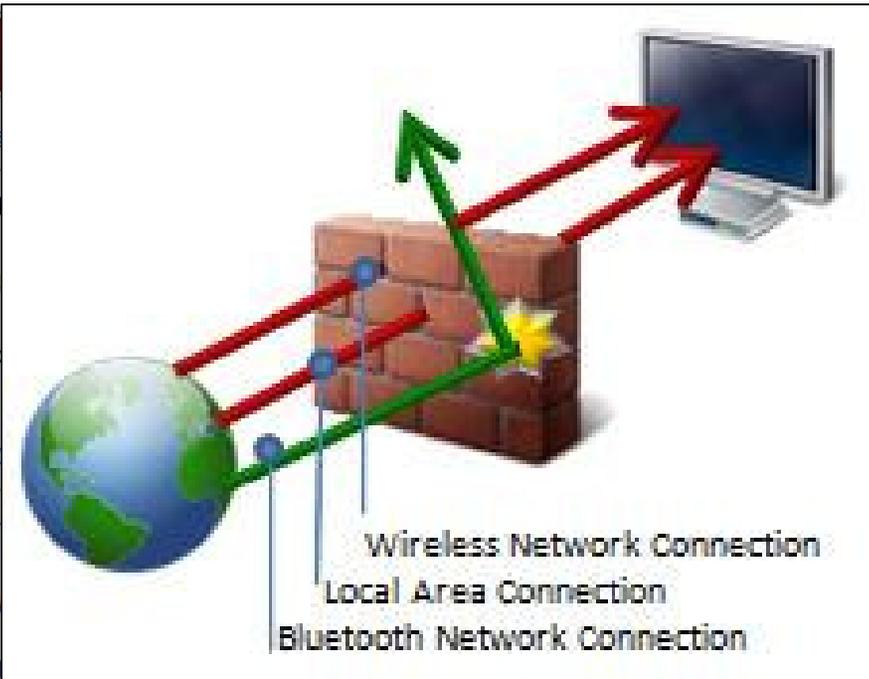
[Change Settings for Domain Network](#)

[What are network locations?](#)

See also

Security Center

Network Center



Bluetooth Connection	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
----------------------	--	--	--

- [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](#)

OK Cancel

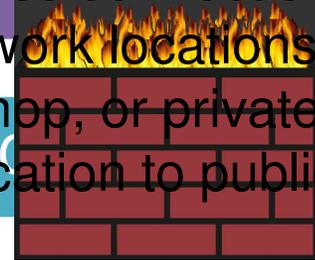
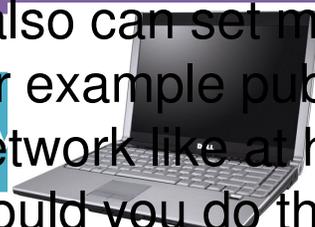
User Study

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?



	Public Network Location	Private Network Location	Domain Network Location
Wireless Network Connection			
Local Area Connection			
Bluetooth Network Connection			

Participants

- 13 pilot testers
- ✓ 60 actual study
- 10 training at the beginning

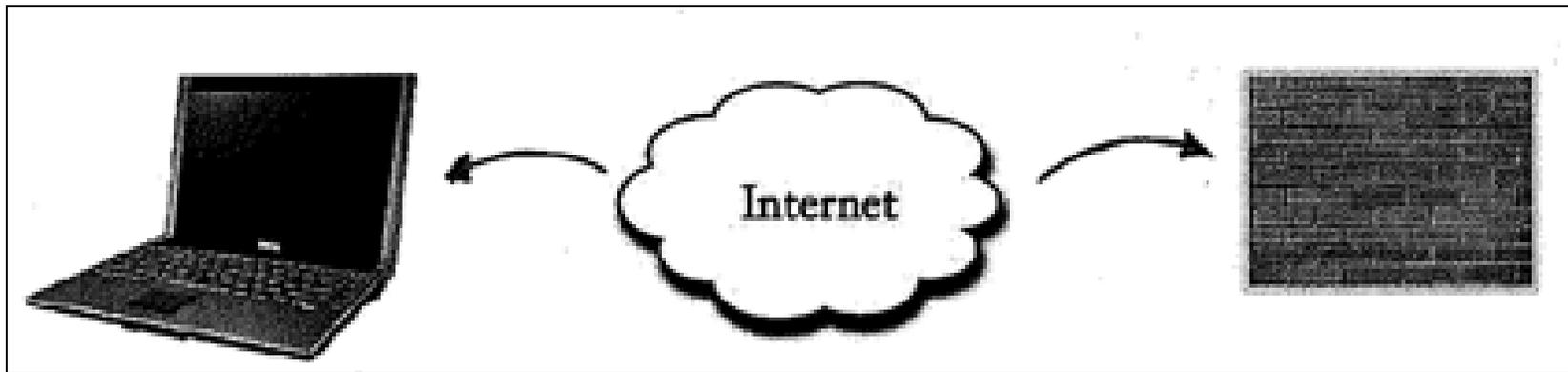
Results

Mental Models

- Incorrect
- Incomplete
- Partially complete
- Complete

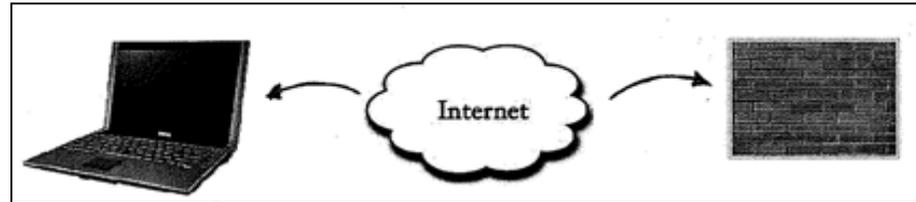
Mental Models

➤ Incorrect

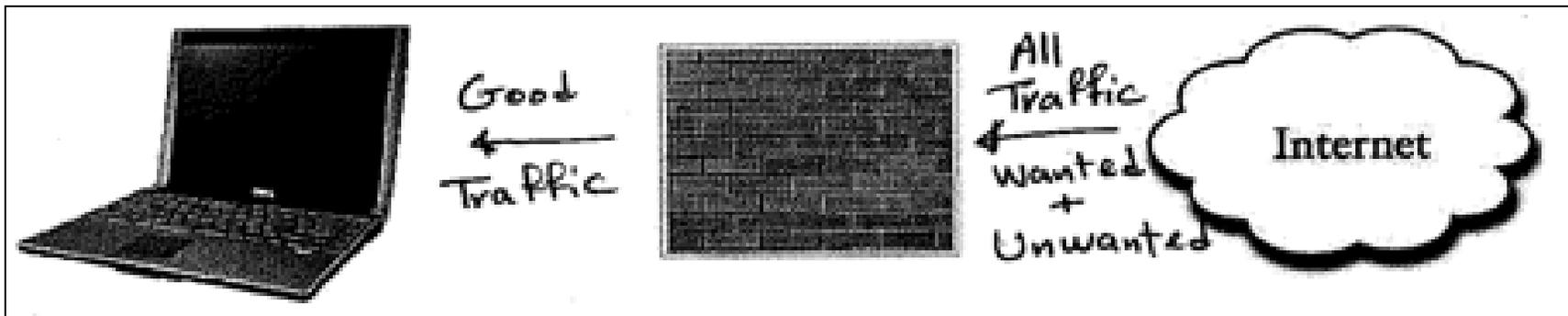


Mental Models

- Incorrect

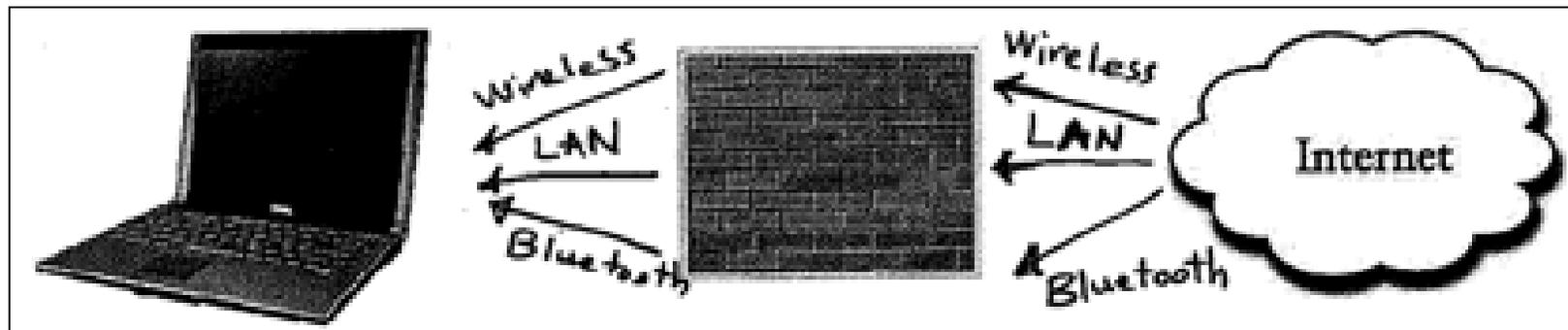
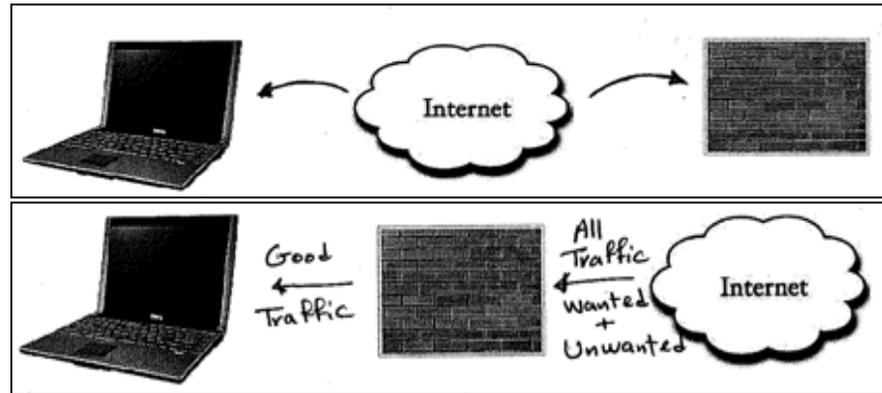


- Incomplete



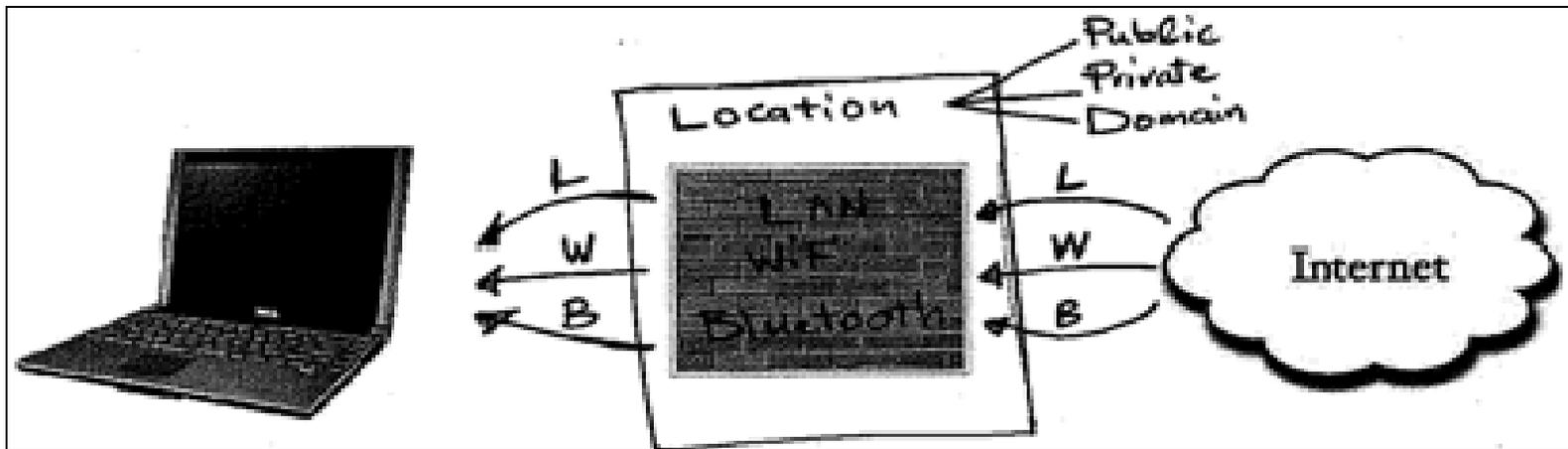
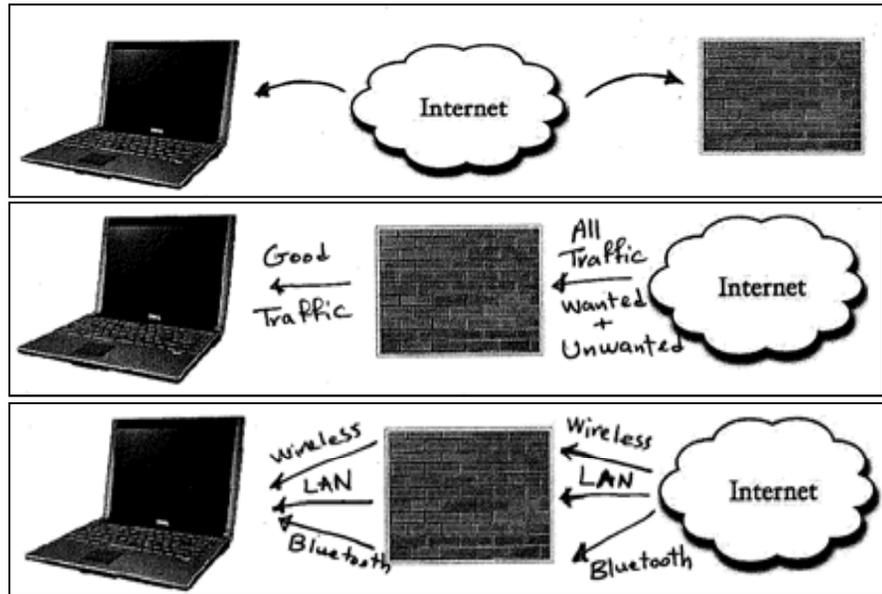
Mental Models

- Incorrect
- Incomplete
- Partially complete

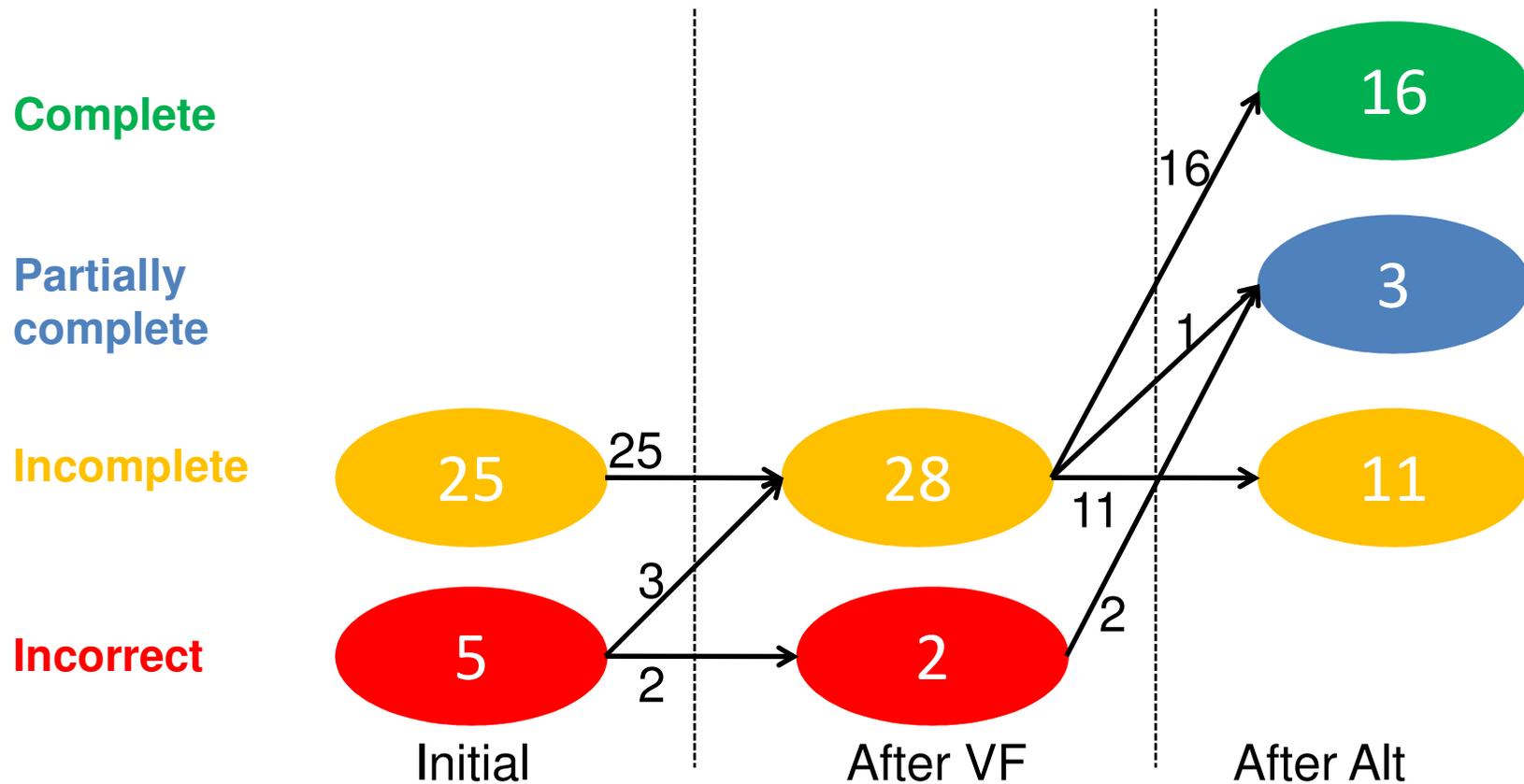


Mental Models

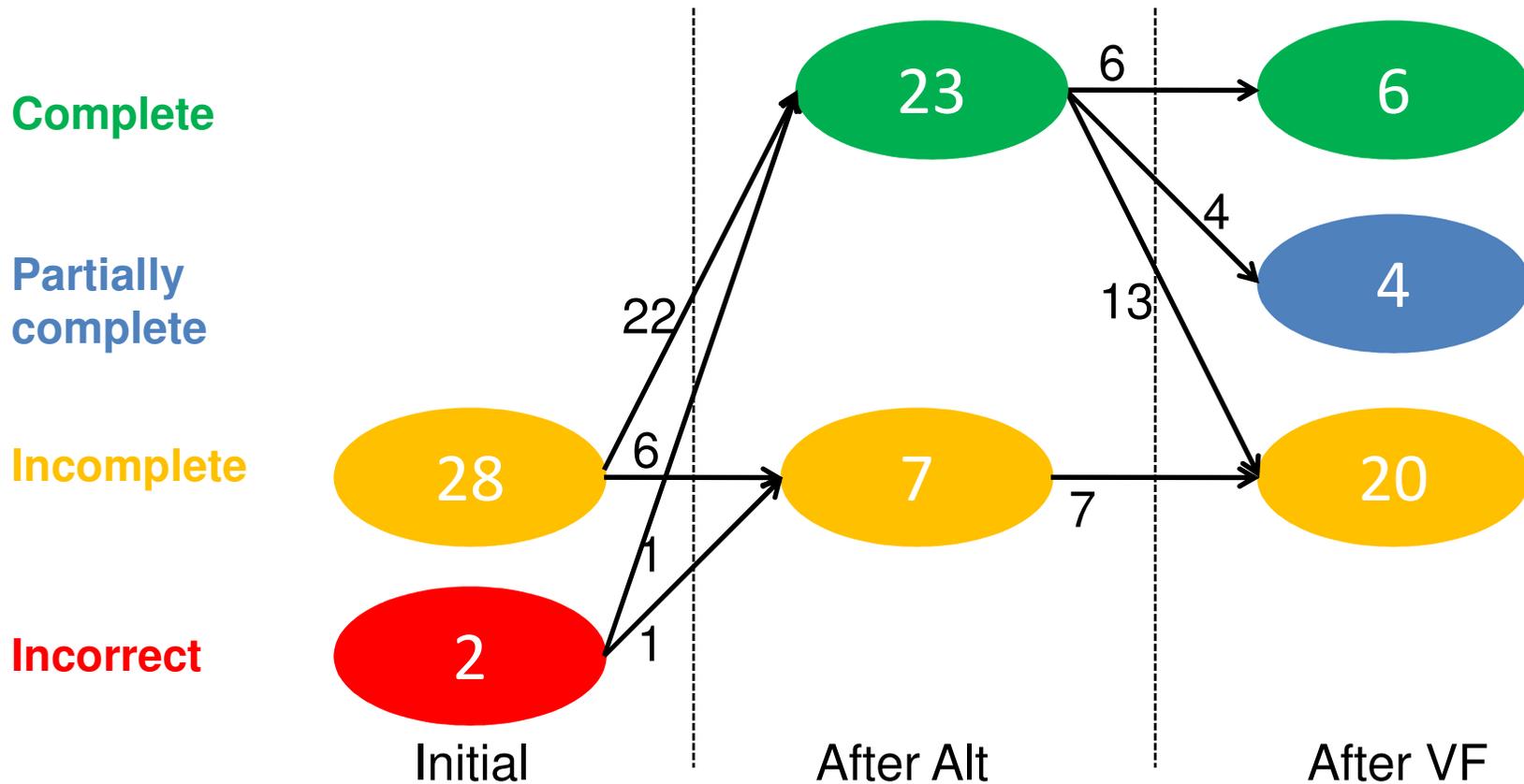
- Incorrect
- Incomplete
- Partially complete
- Complete



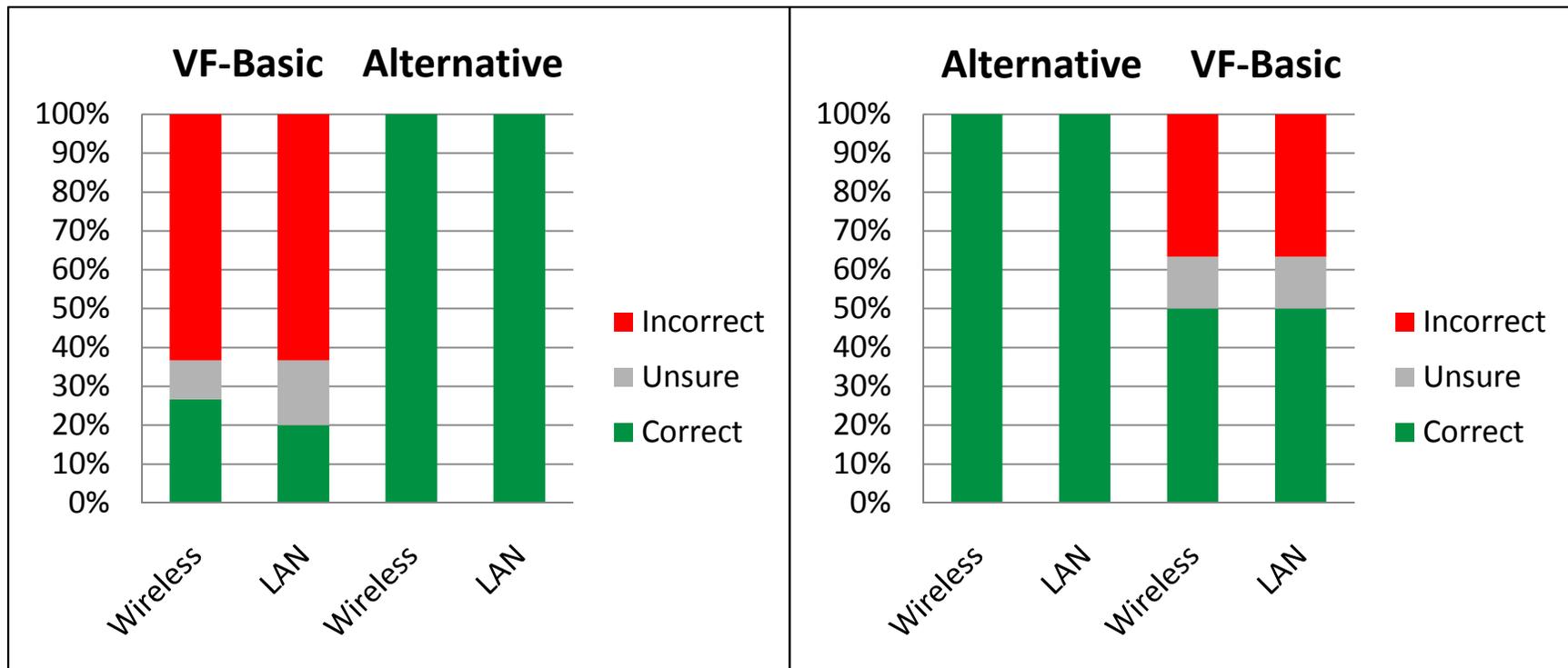
Vista Firewall – Alternative



Alternative – Vista Firewall



Understanding of configuration



Vista-basic: large % of incorrect
Alternative interface: Understood config. (100% correct)

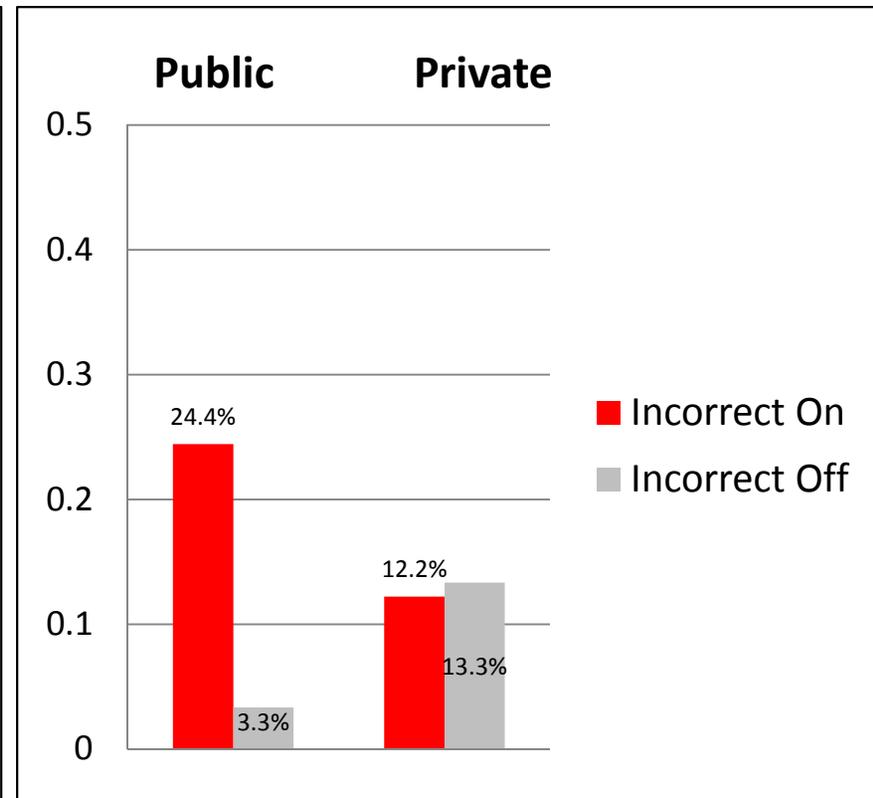
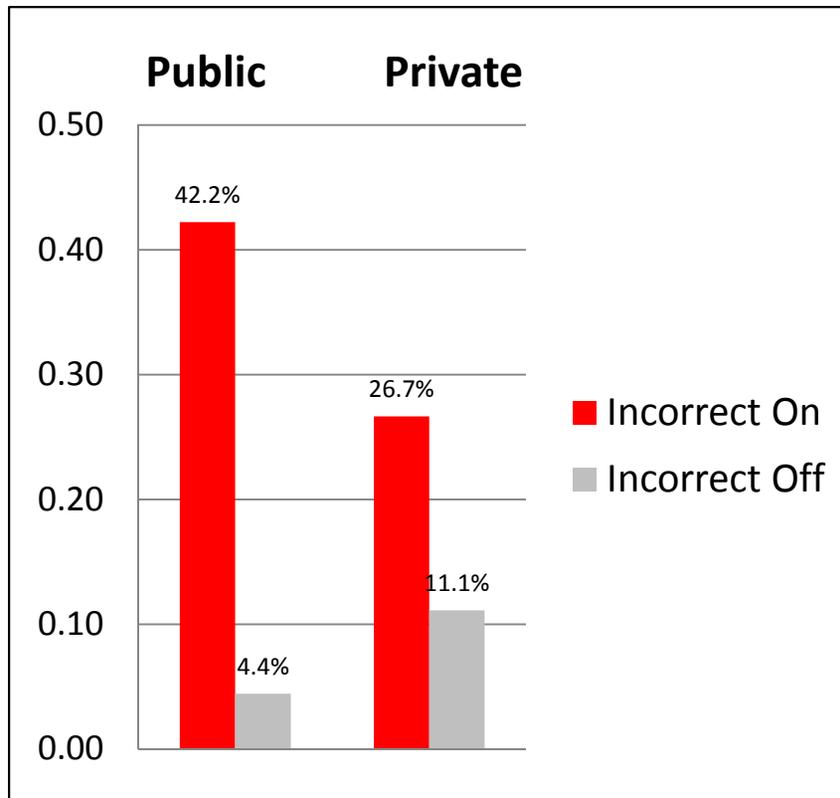
Dangerous misconceptions

- Incorrect answers:
 - Incorrect belief that firewall is off, but it is on
 - incorrect belief that firewall is on, but it is off
- No dangerous state after using prototype

Incorrect understanding of Vista Firewall configuration

(Vista – Alt)

(Alt - Vista)



Conclusion

- Design of Vista basic ok for desktop users, but not 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
 - Education can help, but training video not enough

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
- Not related but need feedback:
 - Access control on collaborative settings
 - Privacy and security on shared large screens

For more information:

Fahimeh Raja, fahimehr@ece.ubc.ca

Kirstie Hawkey, hawkey@ece.ubc.ca

Kosta Beznosov, beznosov@ece.ubc.ca

QUESTIONS?