University of British Columbia

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.**

  K.-P. Yee. User interaction design for secure systems. International Conference on Information and Communications Security, 2002.

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

  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. Symposium on Usable Privacy and Security, 2006.

- **Users should be able to determine current security state.**
  - **Sufficient feedback**

  S. Chiasson, P.C. van Oorschot, and R. Biddle. A Usability Study and Critique of Two Password Managers. USENIX Security Symposium, 2006.

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

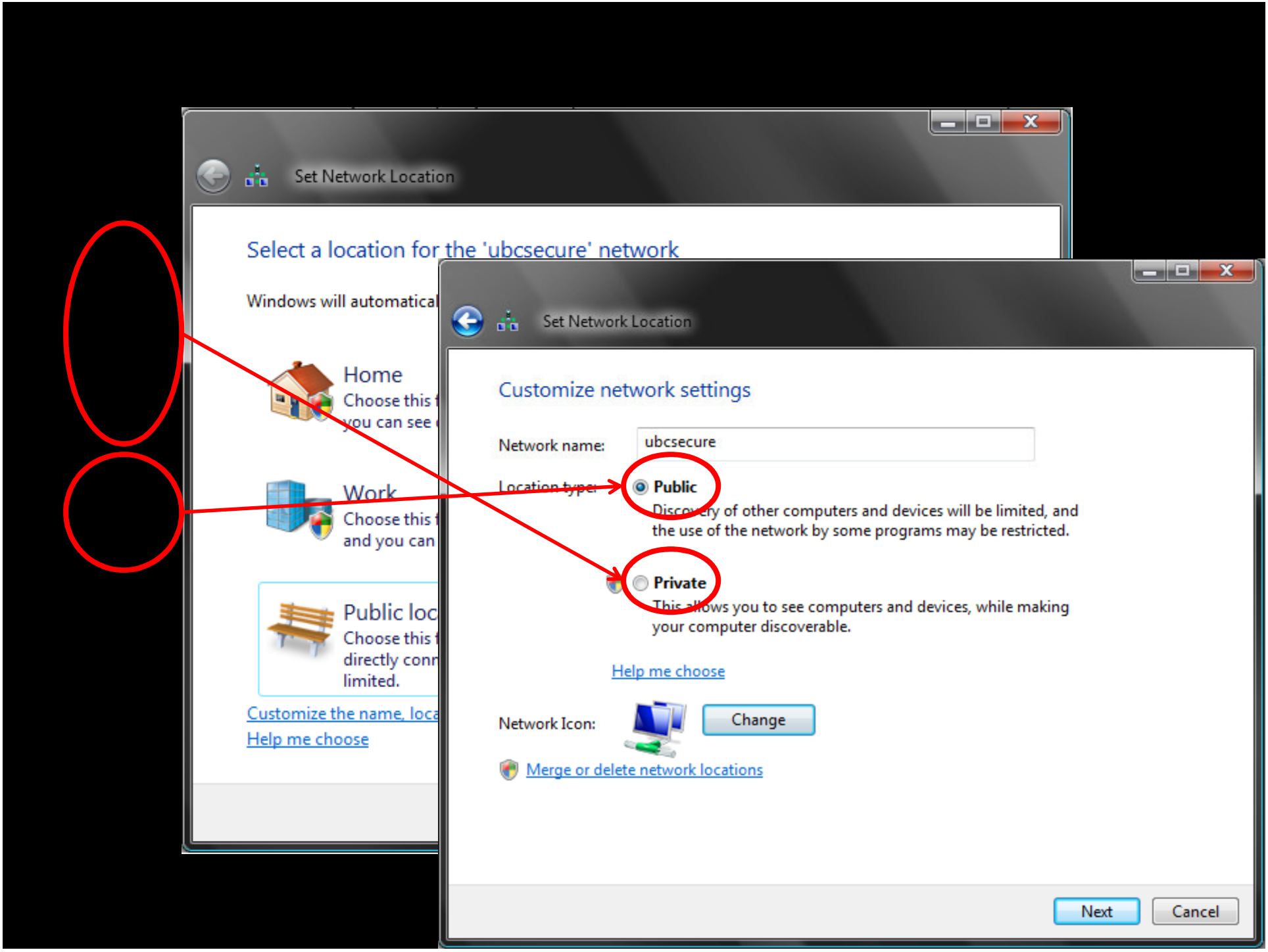
Otherwise

The hidden context can leave user in dangerous situations.

Network Location

in

Windows Vista


Set Network Location
Select a location for the 'ubcsecure' network
Windows will automatical
Home
Choose this
you can see
Work
Choose this
and you can
Public loc
Choose this
directly conn
limited.
Customize the name, loca
Help me choose
Set Network Location
Customize network settings
Network name:
ubcsecure
Location type:
Public
Discovery of other computers and devices will be limited, and the use of the network by some programs may be restricted.
Private
This allows you to see computers and devices, while making your computer discoverable.
Help me choose
Network Icon:
Change
Merge or delete network locations
Next
Cancel

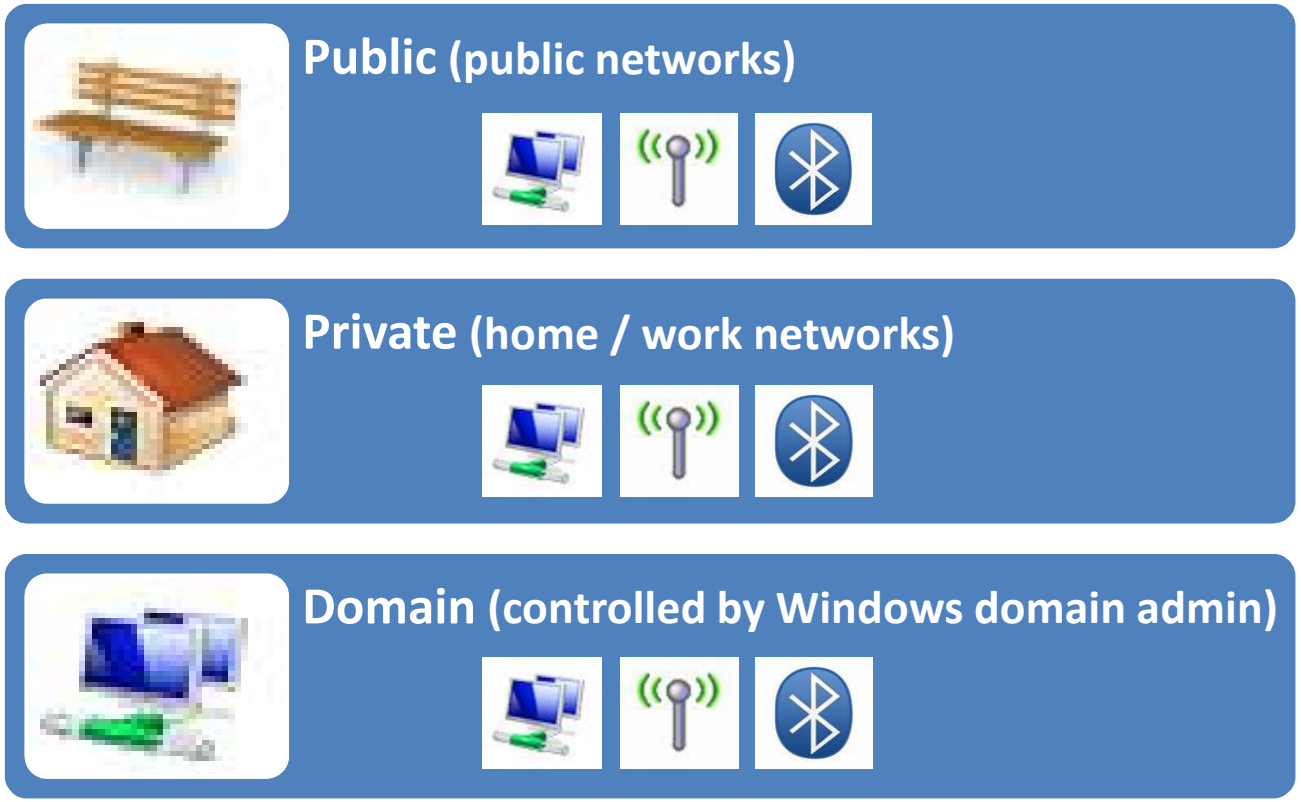
Personal Firewall

in

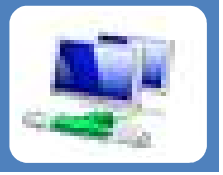
Windows Vista

Context Dependent Functionality

Settings *automatically* applied depending on network context detected

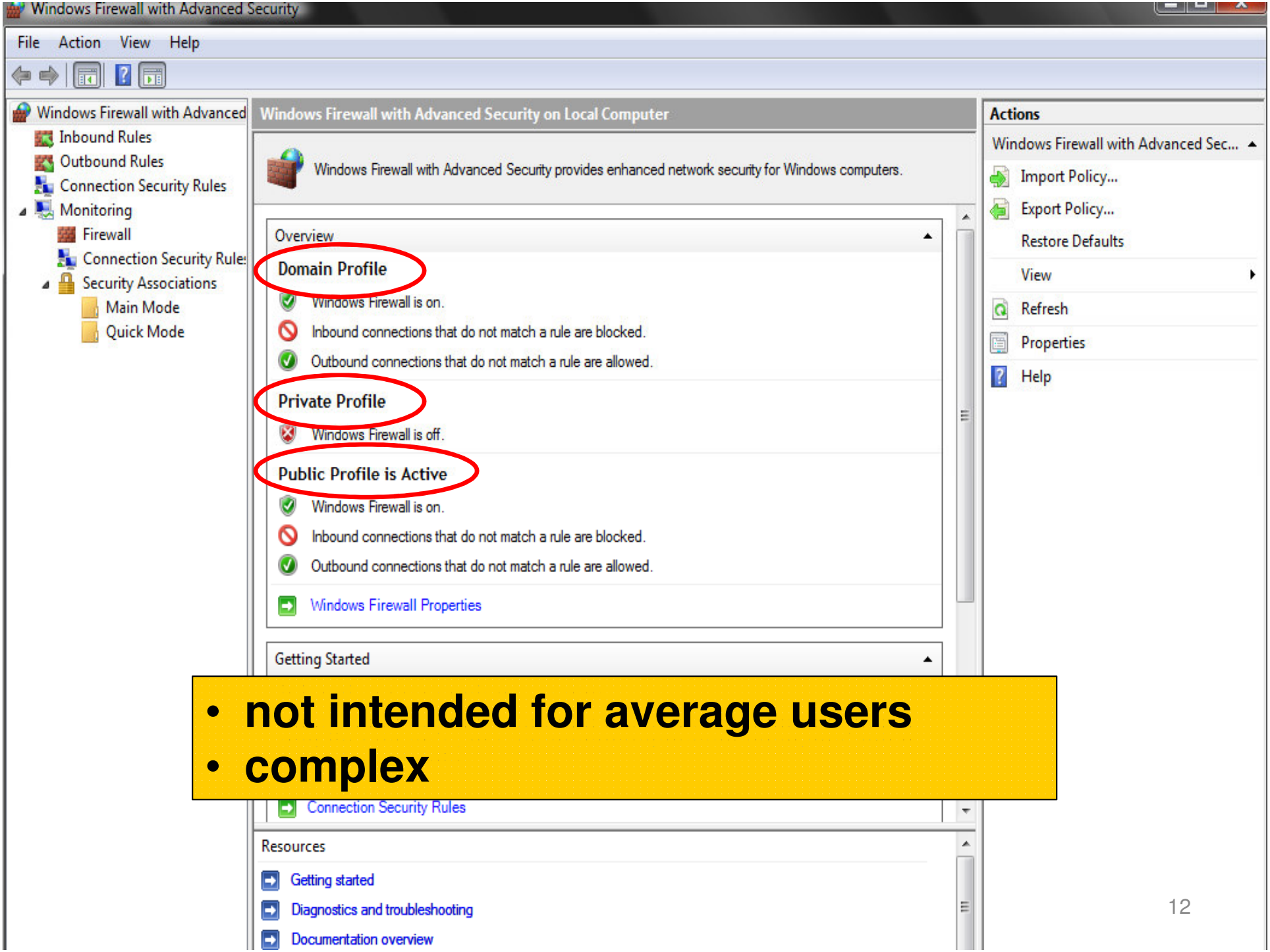


Network Context in Vista Firewall

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

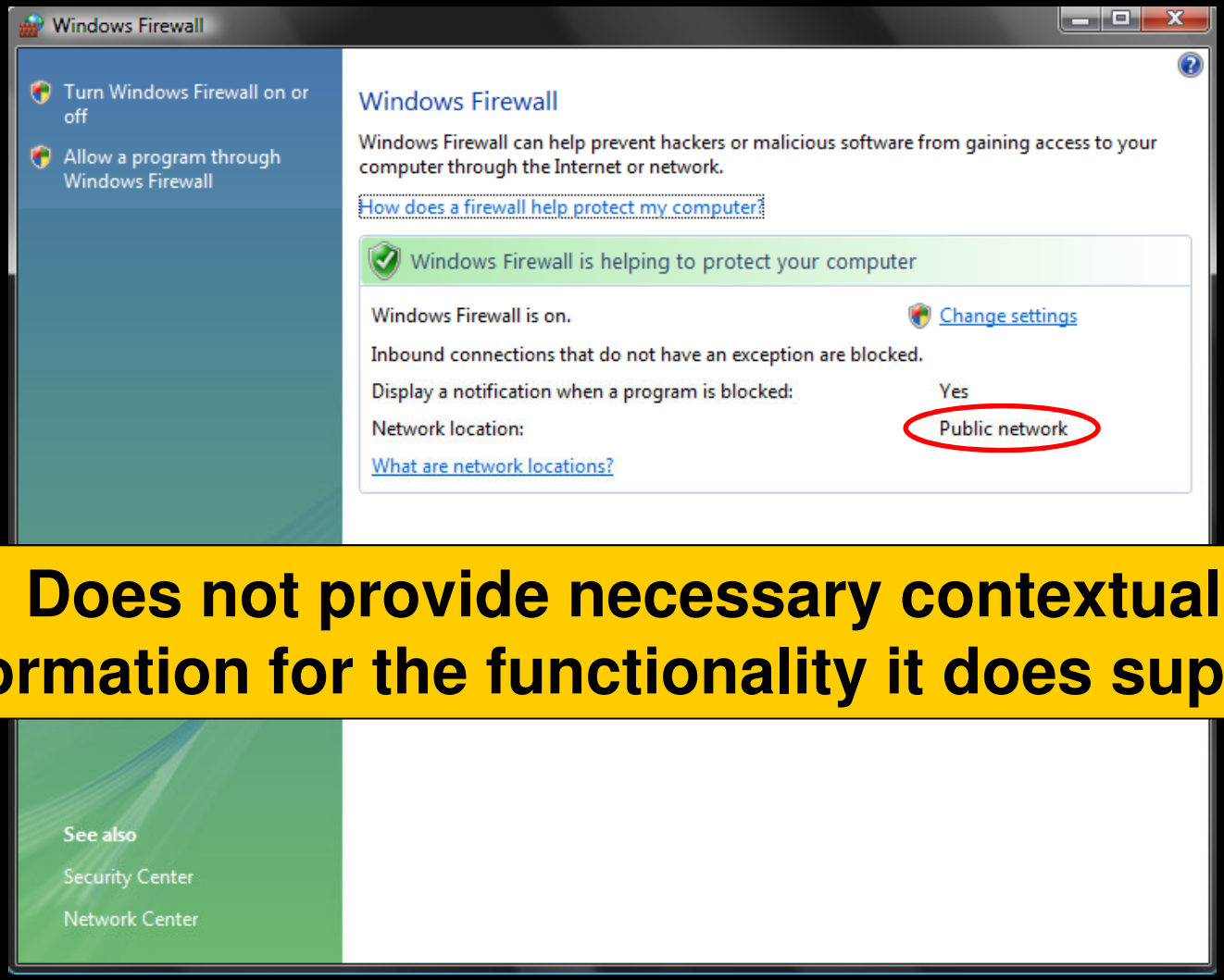
2 User Interfaces:

Basic and Advanced



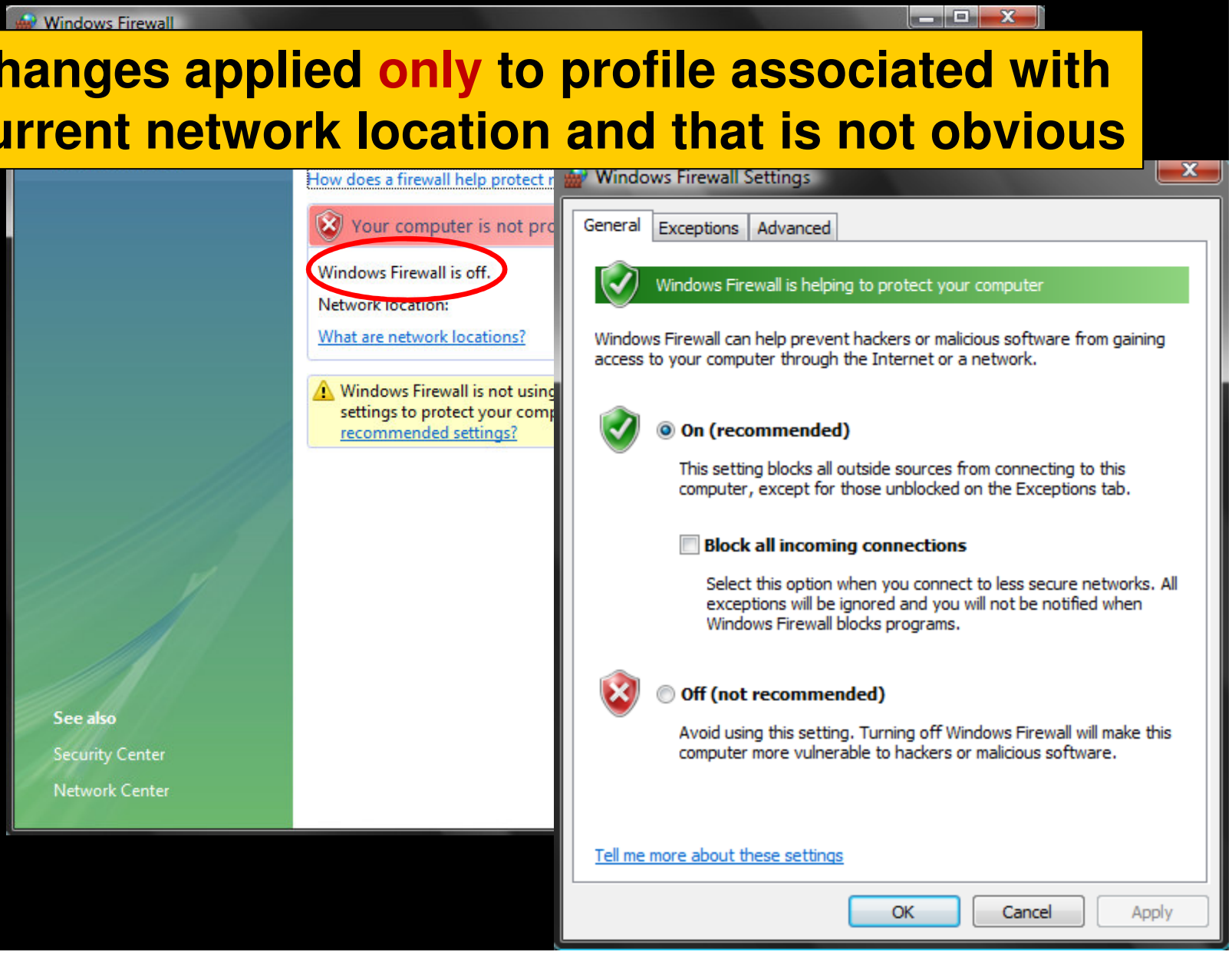
- **not intended for average users**
- **complex**

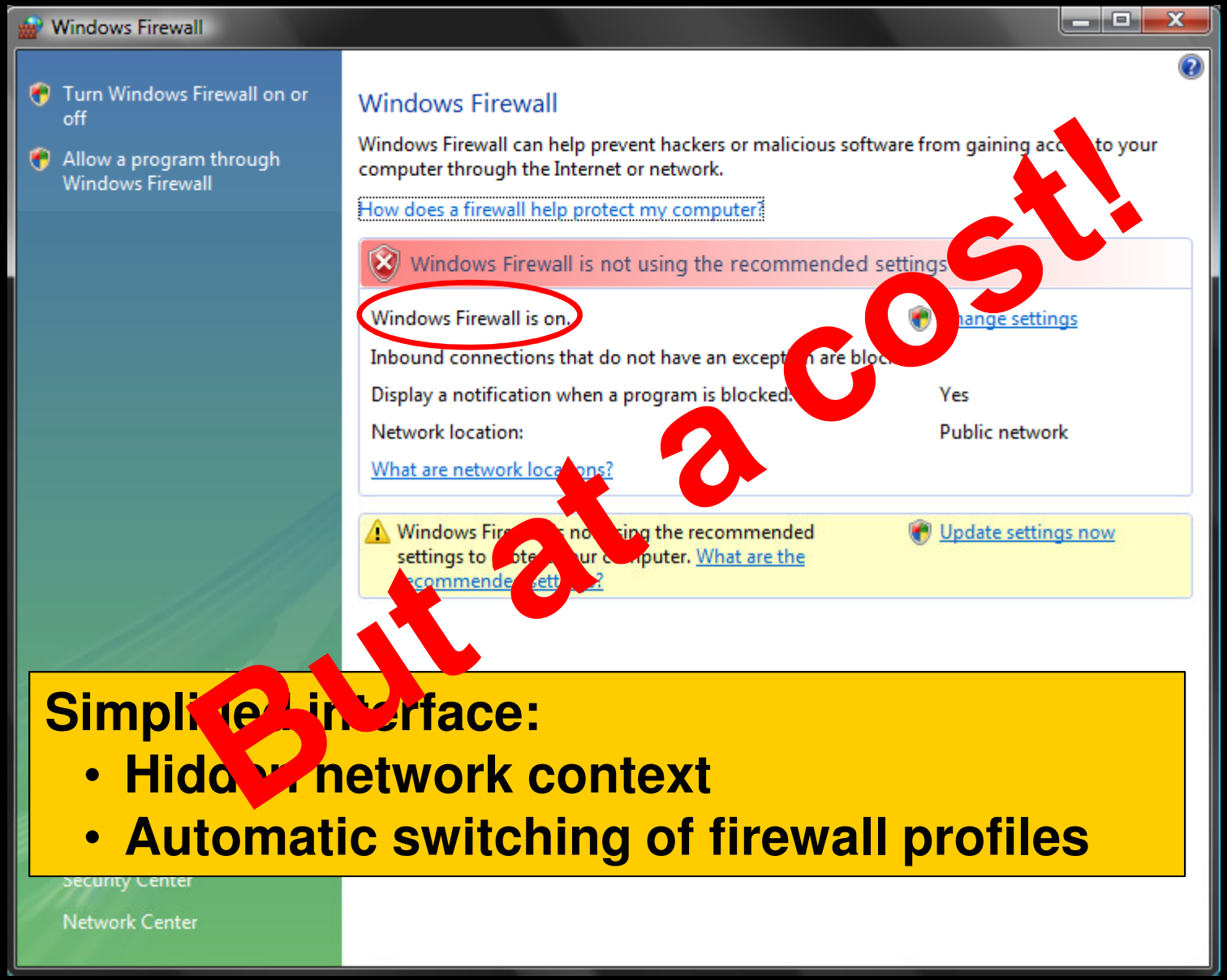
Limited functionality and simplified interface to hide complexity from user



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





But at a cost!

Simpli ed interface:

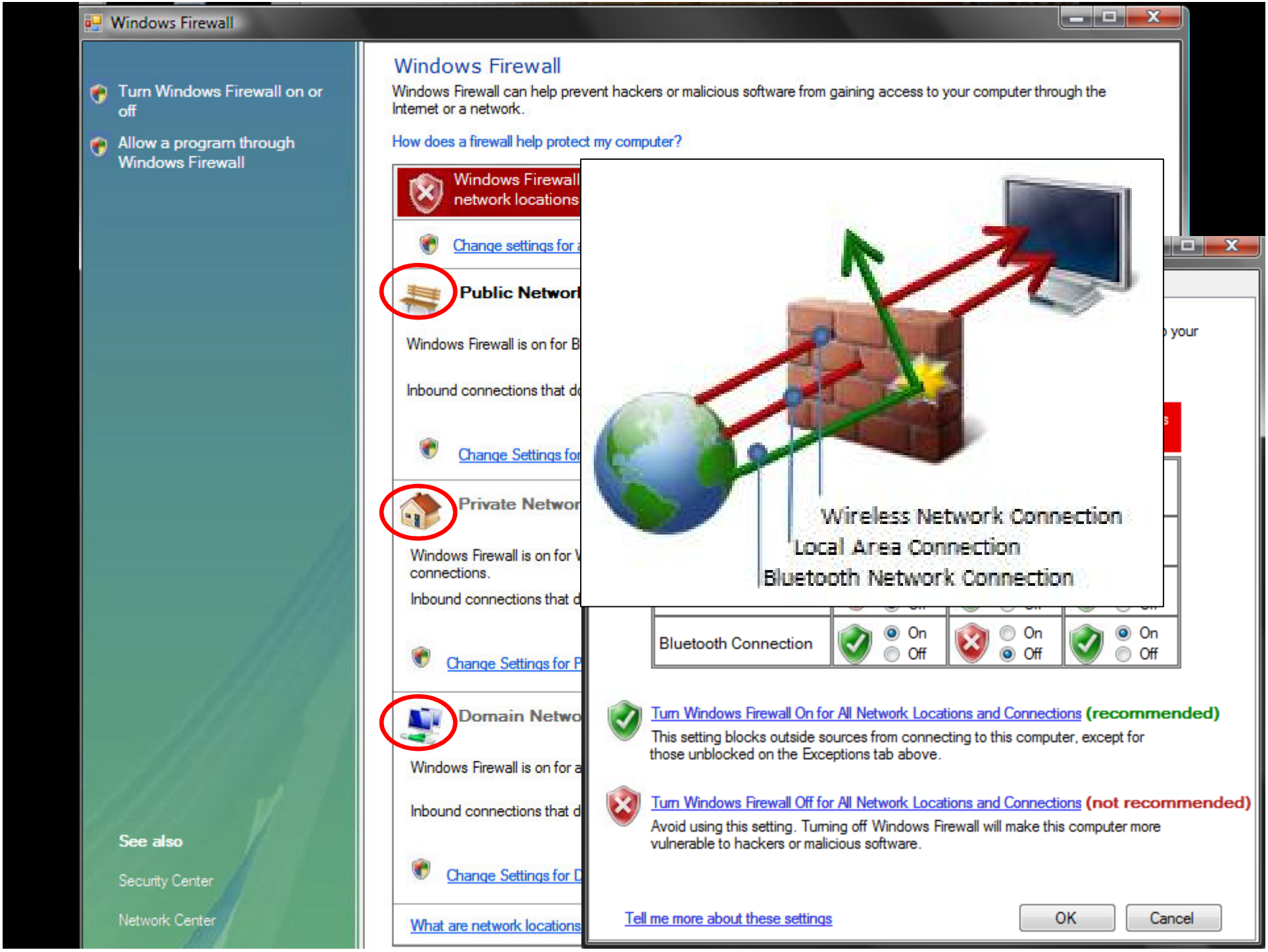
- **Hidd n network context**
- **Automatic switching of firewall profiles**

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
Turn Windows Firewall on or off
Allow a program through Windows Firewall
See also
Security Center
Network Center
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 Networ
Windows Firewall is on for B
Inbound connections that d
Change Settings for
Private Networ
Windows Firewall is on for
connections.
Inbound connections that d
Change Settings for P
Domain Netwo
Windows Firewall is on for a
Inbound connections that d
Change Settings for D
What are network locations
Wireless Network Connection
Local Area Connection
Bluetooth Network Connection
Bluetooth Connection
On
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

Goal

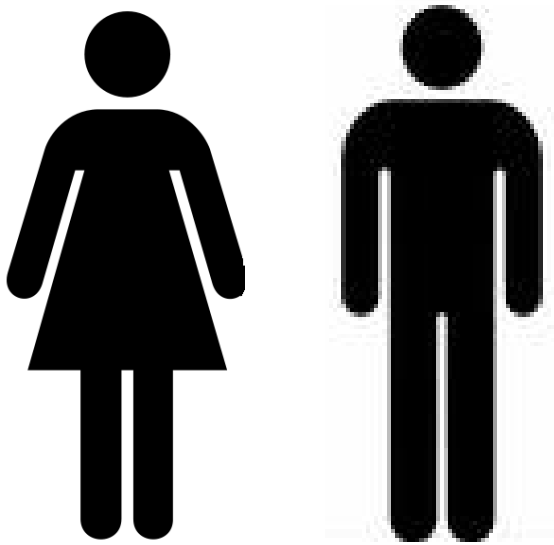
To investigate the impact of addition of contextual information to Vista Firewall basic interface on:

- Users' mental model of Vista Firewall functionality
- Users' understanding of Vista Firewall configuration

Study Design

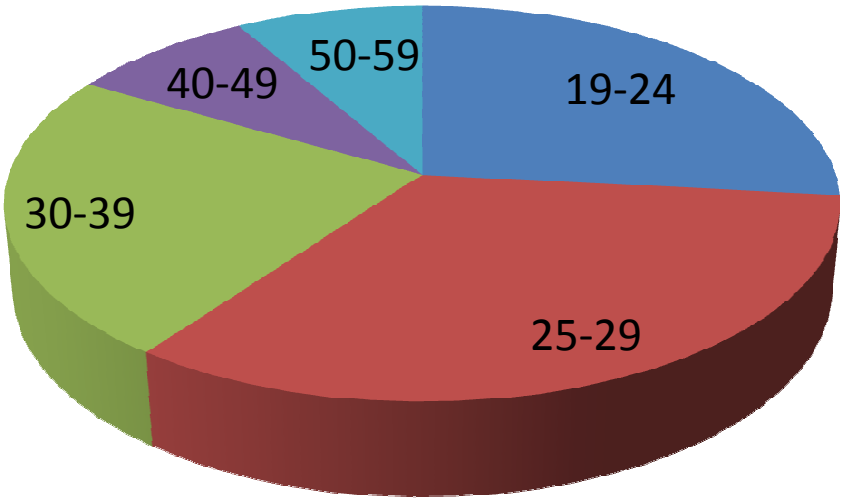
- Within-subjects lab study
- Screen and voice recorded
- Recruitment:
  - Online classifieds: Craigslist, Kijiji
  - University email lists
  - Flyers: posted and handed out
    - University
    - Vancouver public places
- Participants:
  - 13 pilot testers
  - ✓ 60 actual study
    - ✓ 30 first Vista firewall basic interface, then our interface
    - ✓ 30 first our interface, then Vista firewall basic interface
  - 10 training at the beginning

Gender Balance

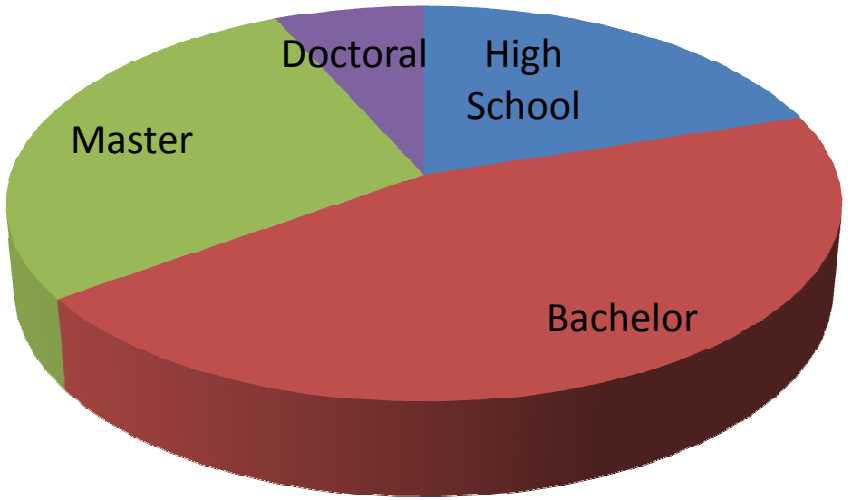


30 **30**

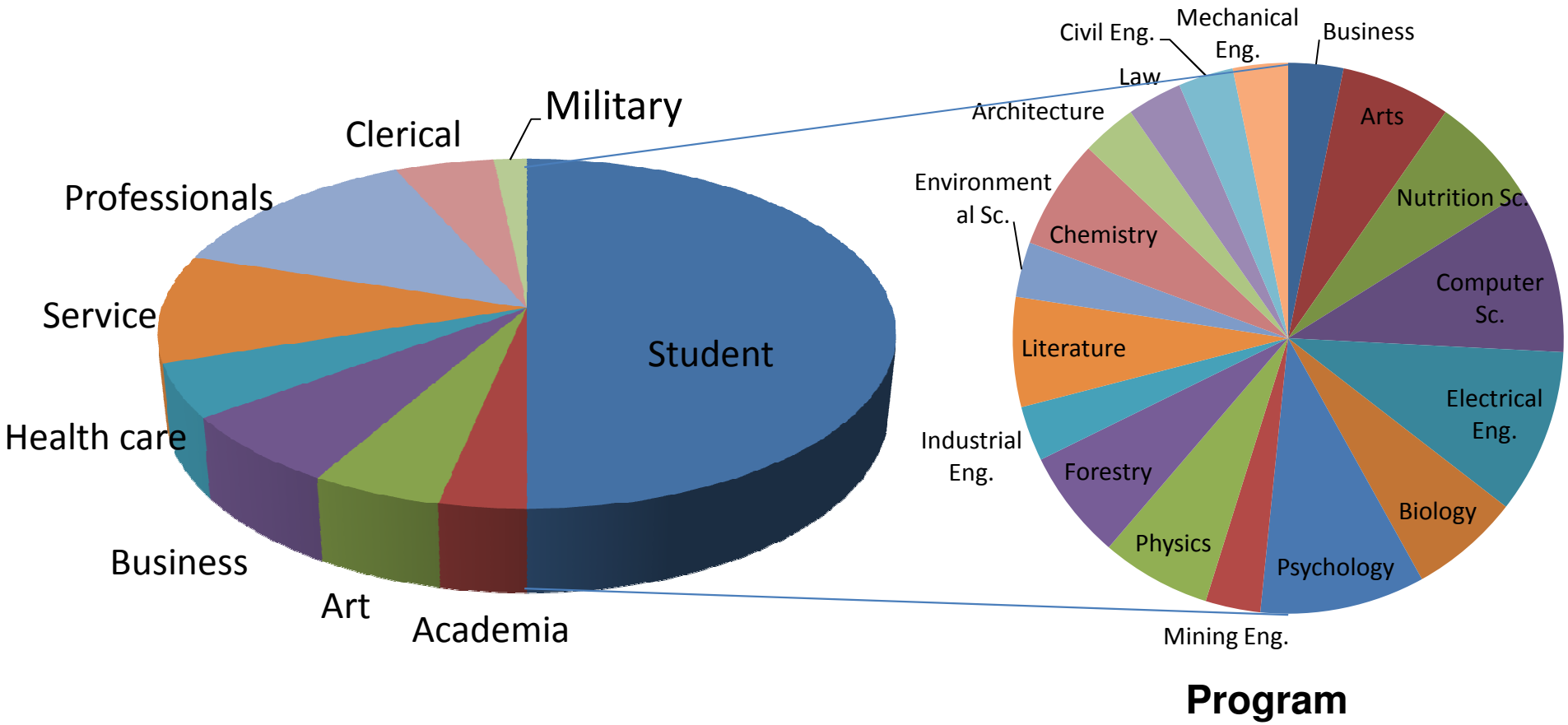
Age



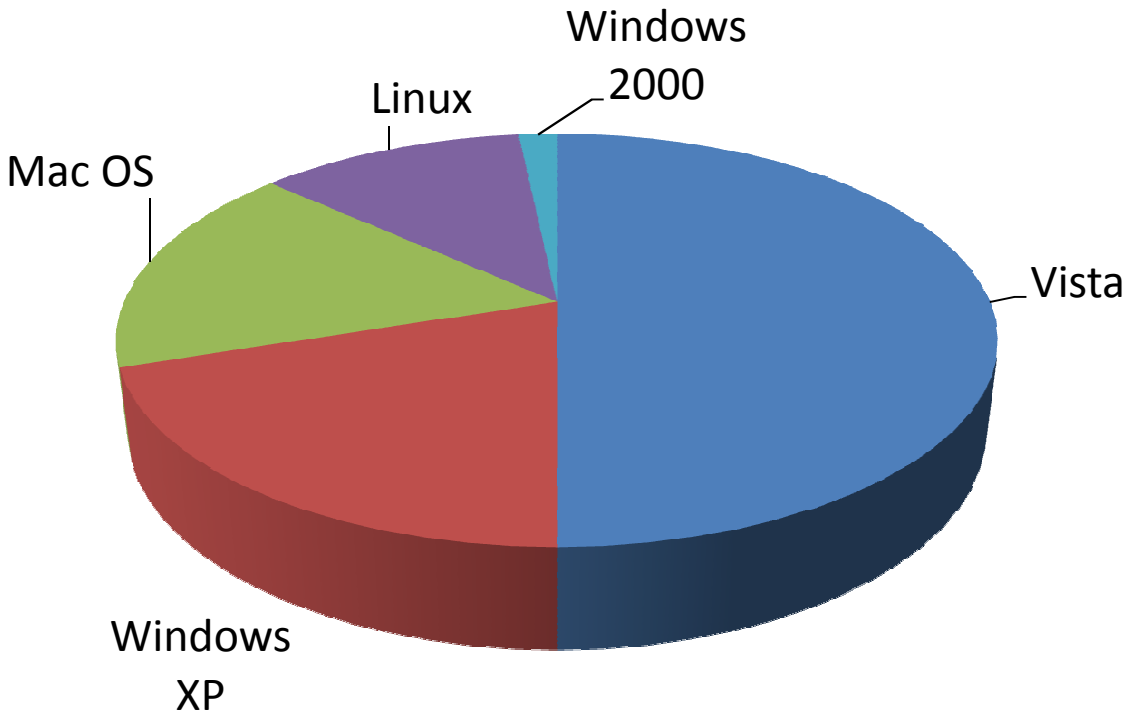
Completed Education



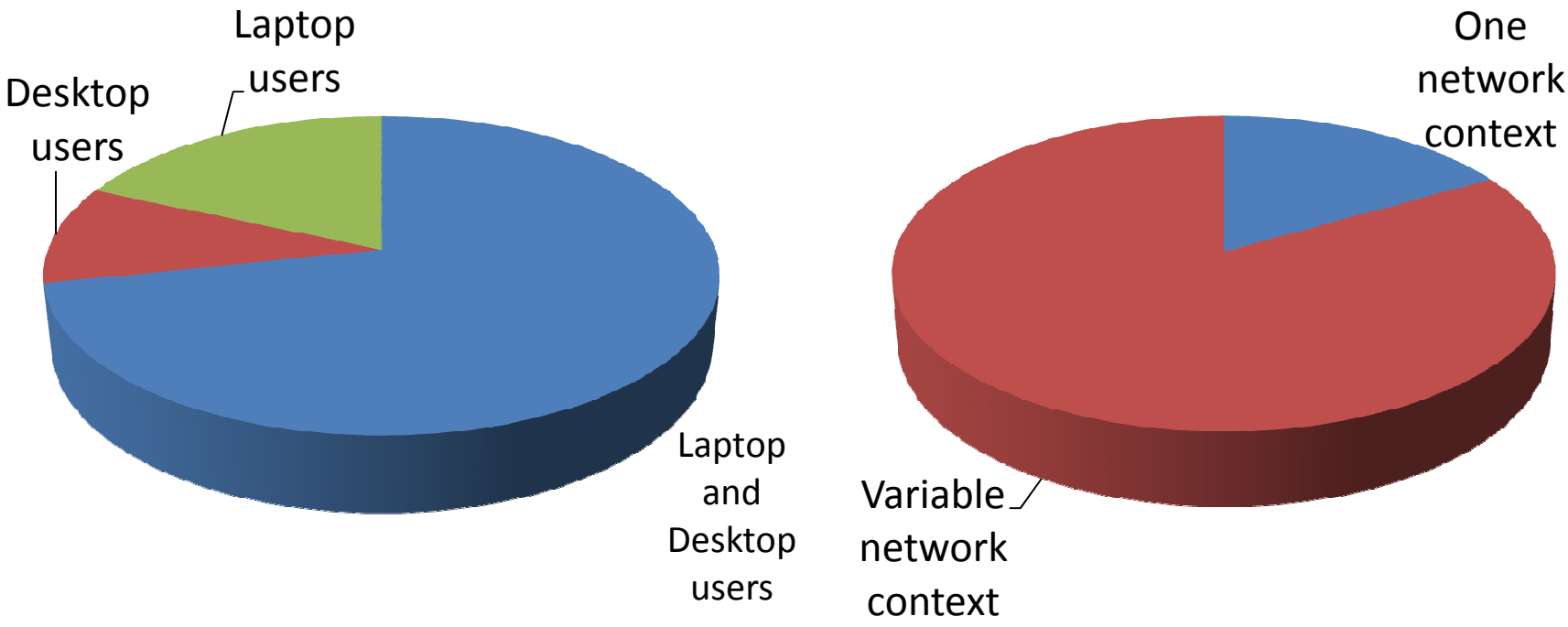
Occupation


Military
Clerical
Professionals
Service
Health care
Business
Art
Academia
Student
Civil Eng.
Mechanical Eng.
Business
Law
Architecture
Arts
Environment al Sc.
Nutrition Sc.
Chemistry
Computer Sc.
Literature
Electrical Eng.
Industrial Eng.
Forestry
Biology
Physics
Psychology
Mining Eng.
Program

All Daily Computer Users



Context of Use



Study Protocol

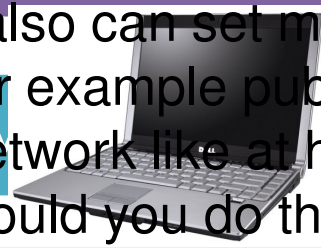
Introduction to the Context

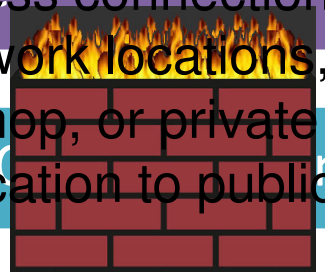
Mental Model

Tasks on the 1st Interface

N… l and Understanding of C… n

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			

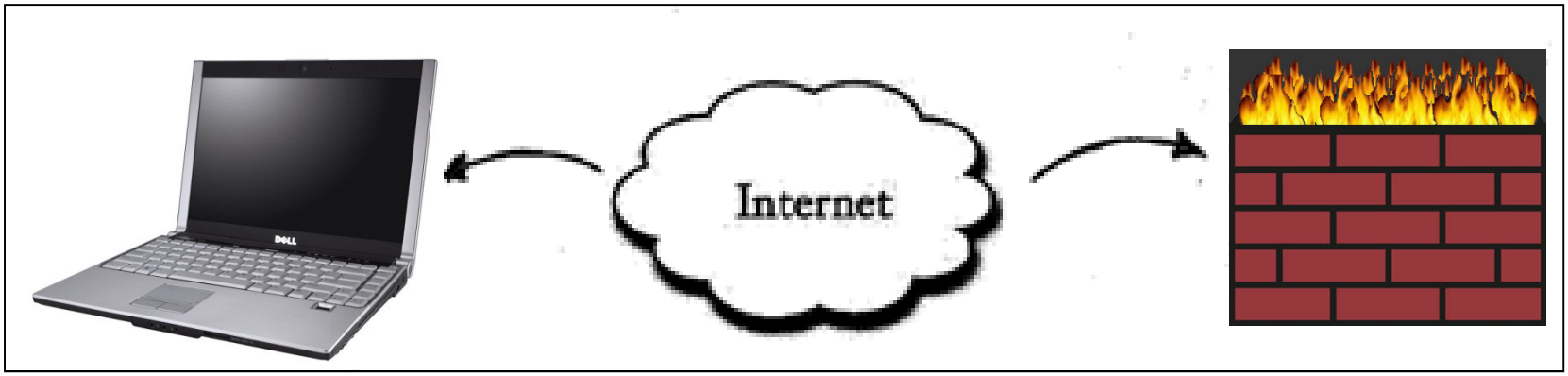
Results

Mental Models

- Incorrect
- Incomplete
- Partially complete
- Complete

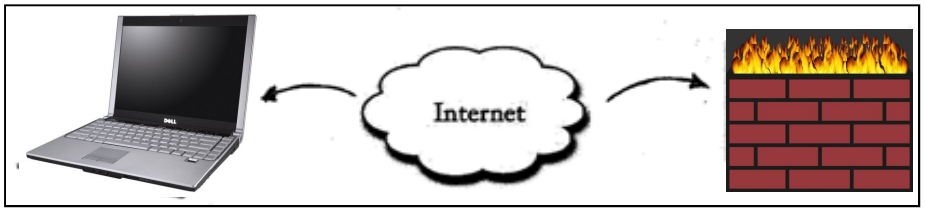
Mental Models

- **Incorrect:** incorrect basic understanding of firewall operation

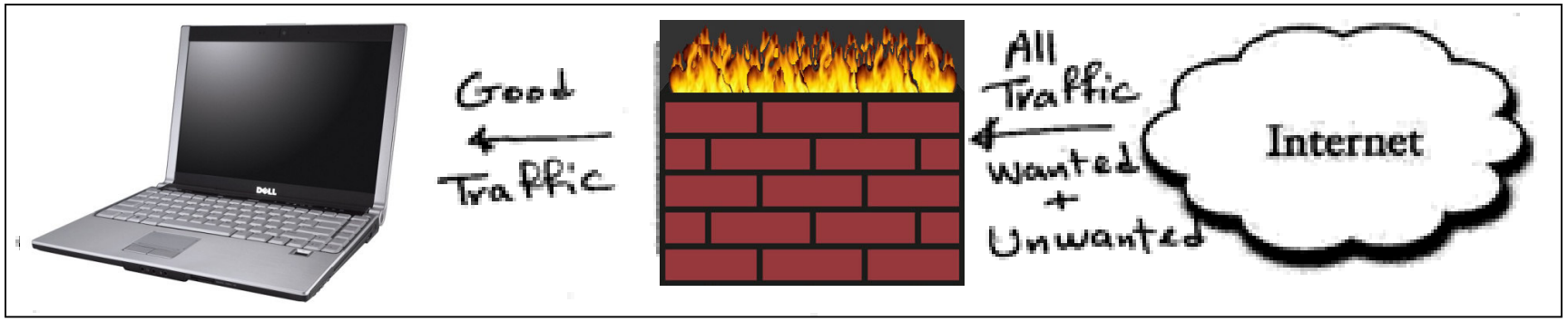


Mental Models

- Incorrect

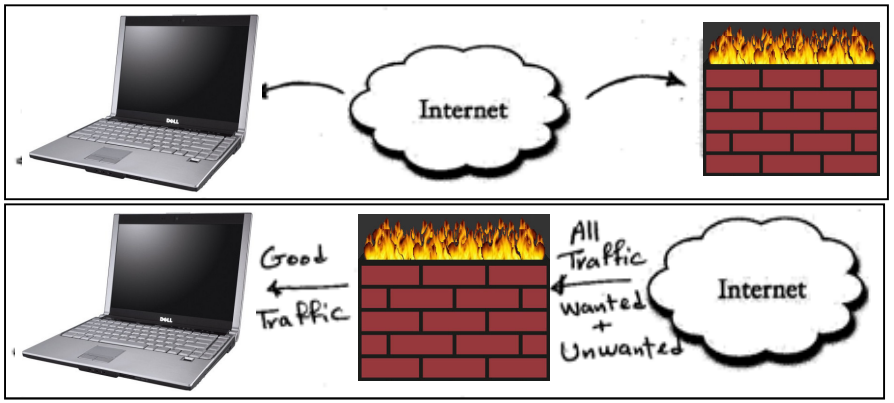


➢ Incomplete: correct basic understanding of firewall operation, without context of network location and connection

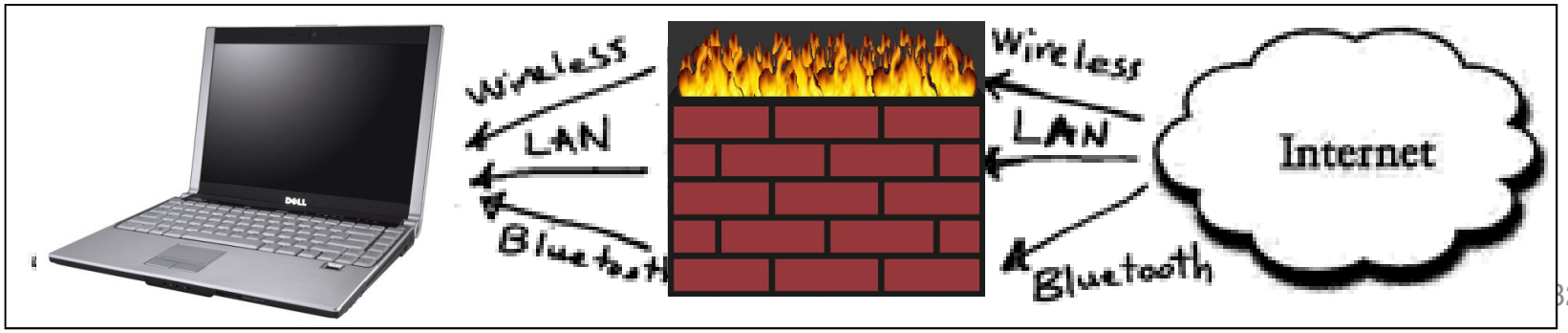


Mental Models

- Incorrect
- Incomplete

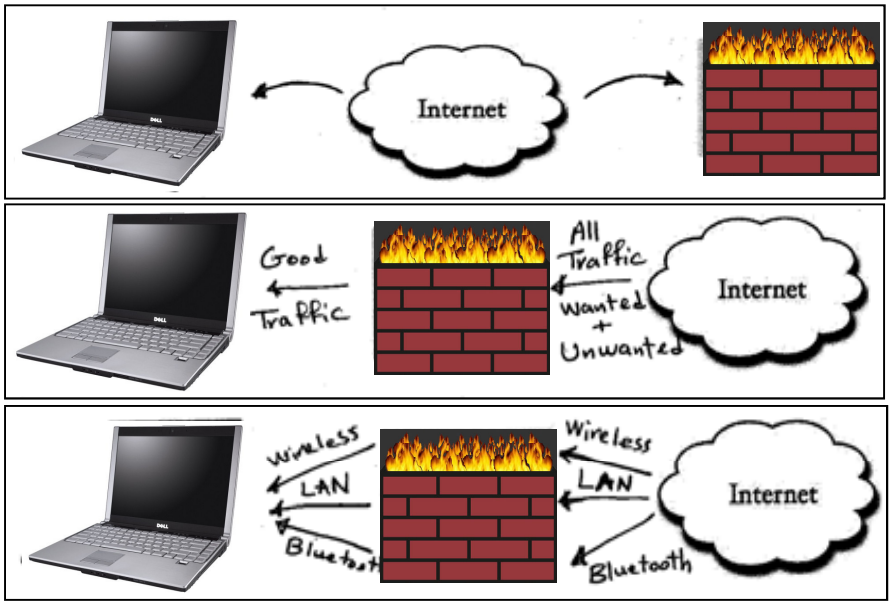


➢ Partially complete: correct basic understanding of firewall operation, with either context of network location or connection

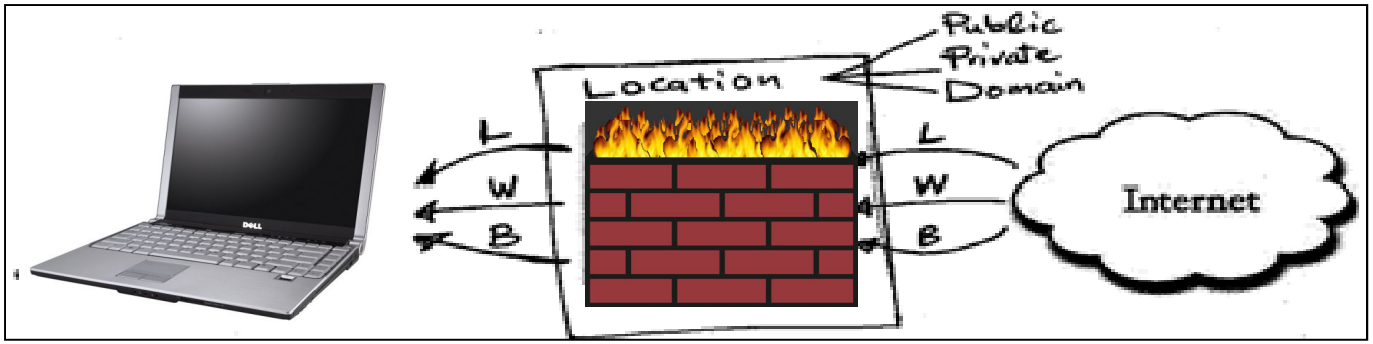


Mental Models

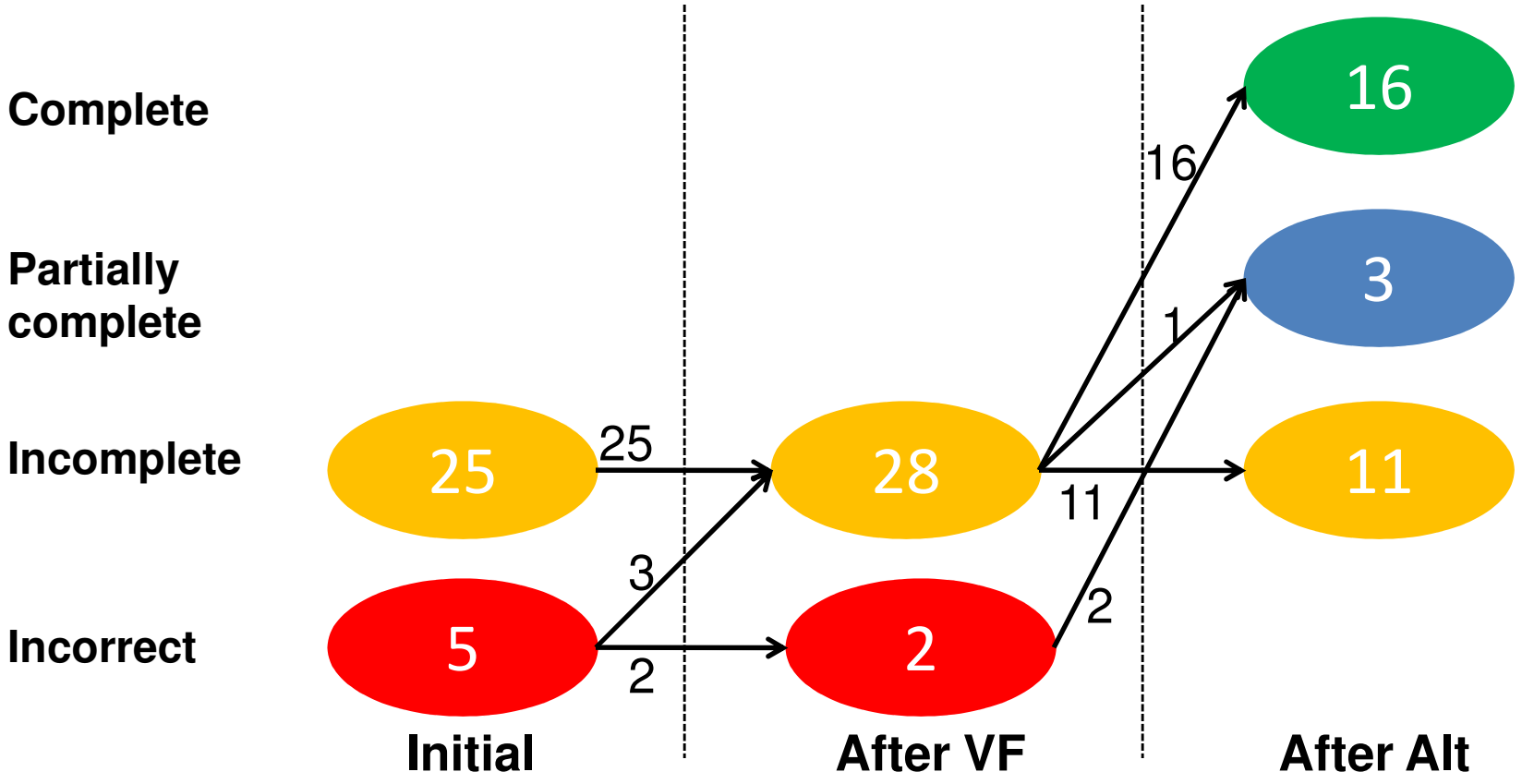
- Incorrect
- Incomplete
- Partially complete



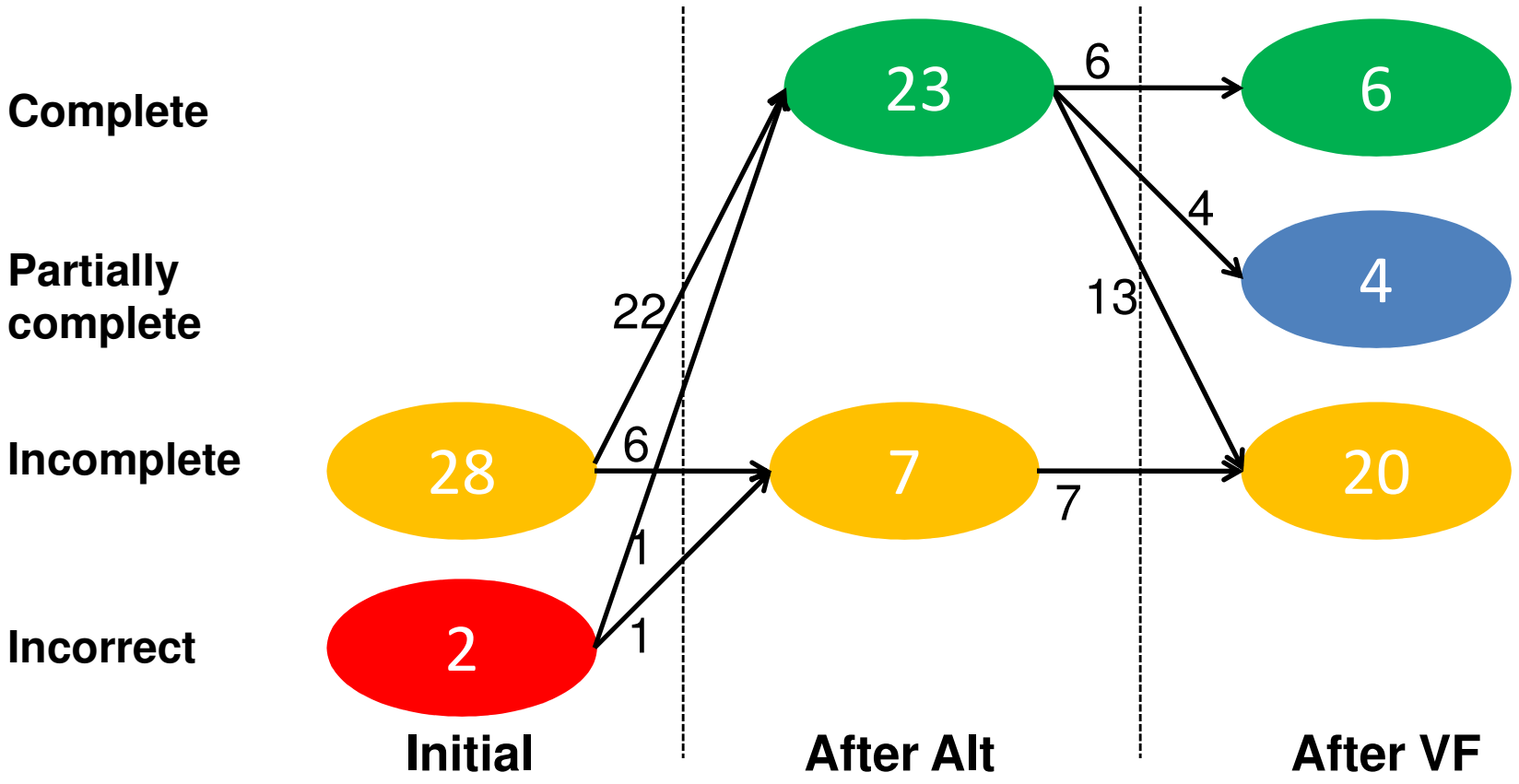
➢ Complete: correct basic understanding of firewall operation, with both context of network location and connection



First Vista Firewall Basic, then Alternative



First Alternative, then Vista Firewall Basic

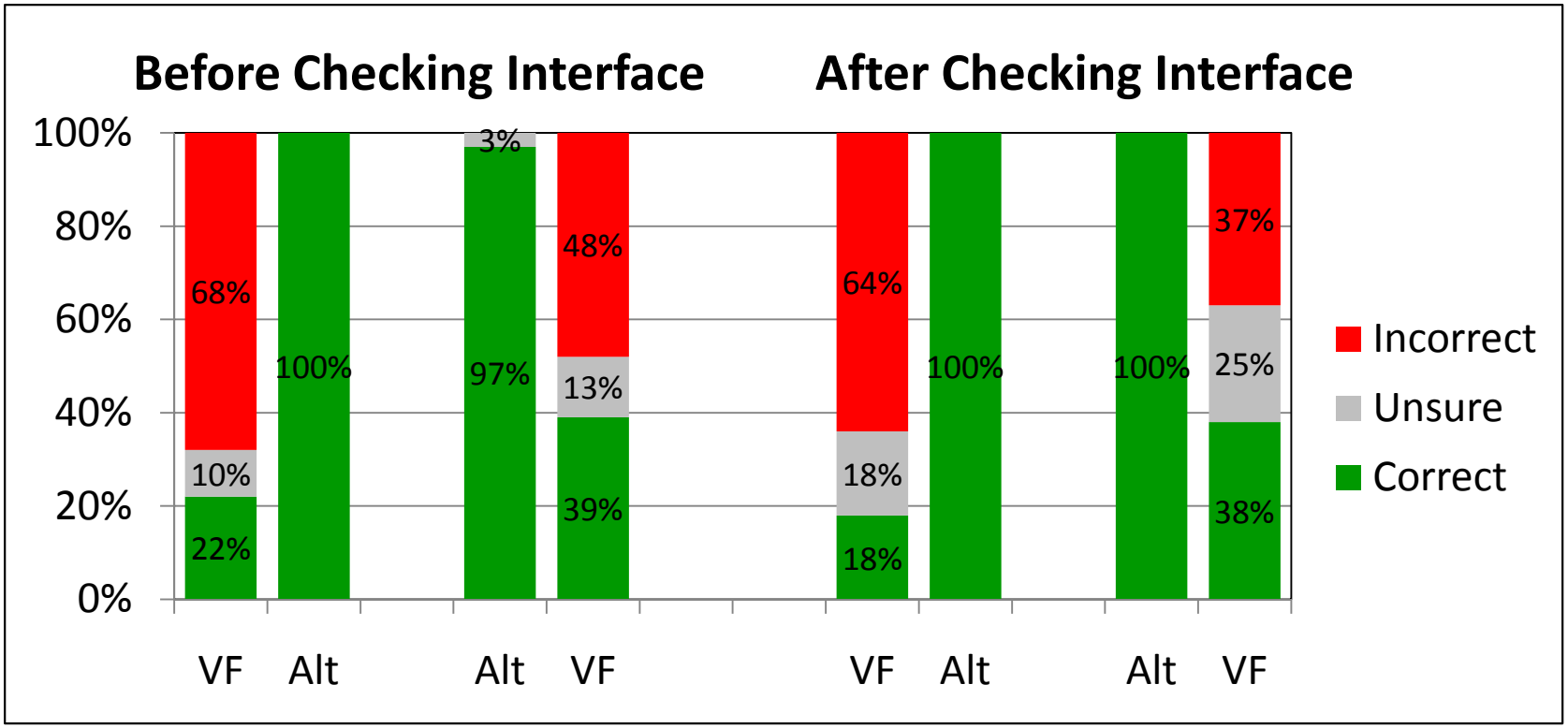


Understanding Firewall Configuration

	Public Network Location	Private Network Location	Domain Network Location
Wireless Network Connection	On ✗	On ✗	Unsure
Local Area Connection	On ✗	Off ✗	Unsure
Bluetooth Network Connection	On ✓	Unsure	Unsure

Understanding Firewall Configuration

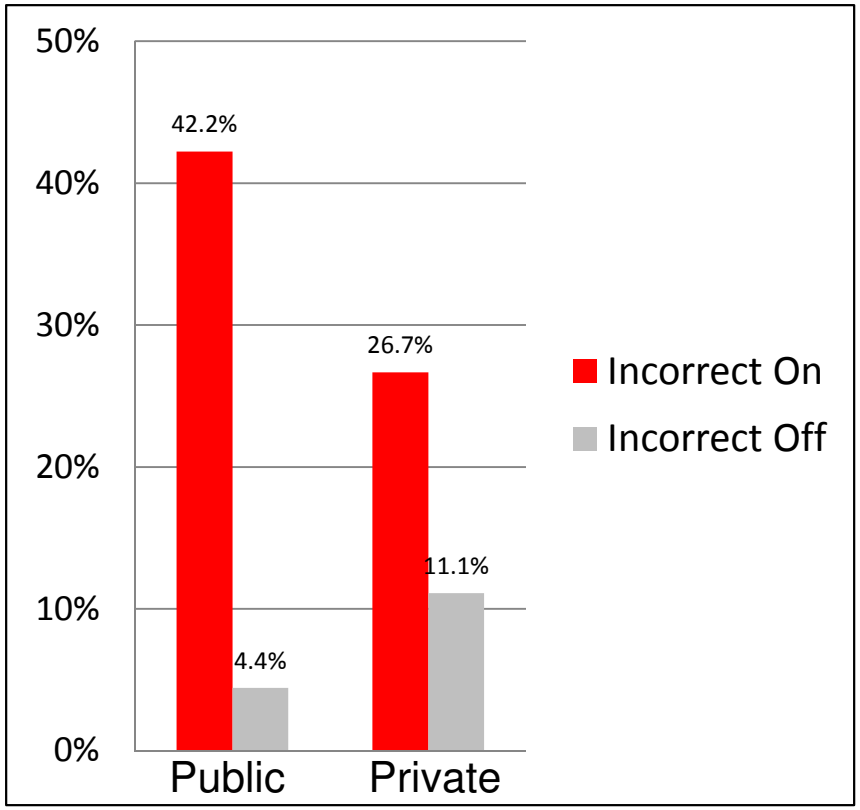
Public Network



Vista-basic: large % of incorrect

Alternative interface: Understood config.

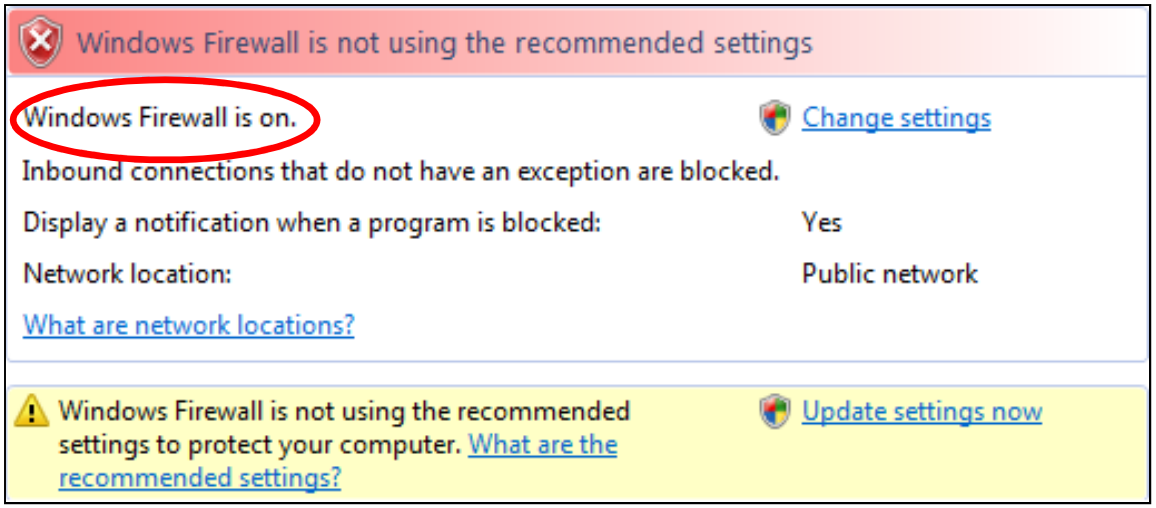
Incorrect Understanding of ***Vista*** Firewall Configuration



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

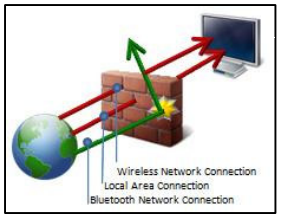
Feedback on Alternative Interface

- 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

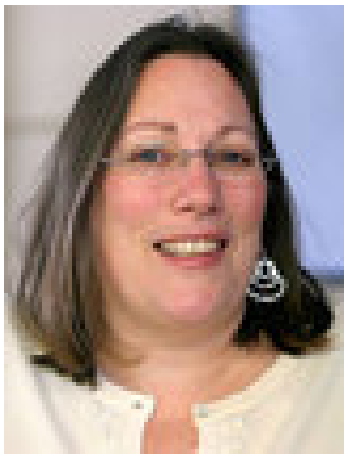
Summary

- **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

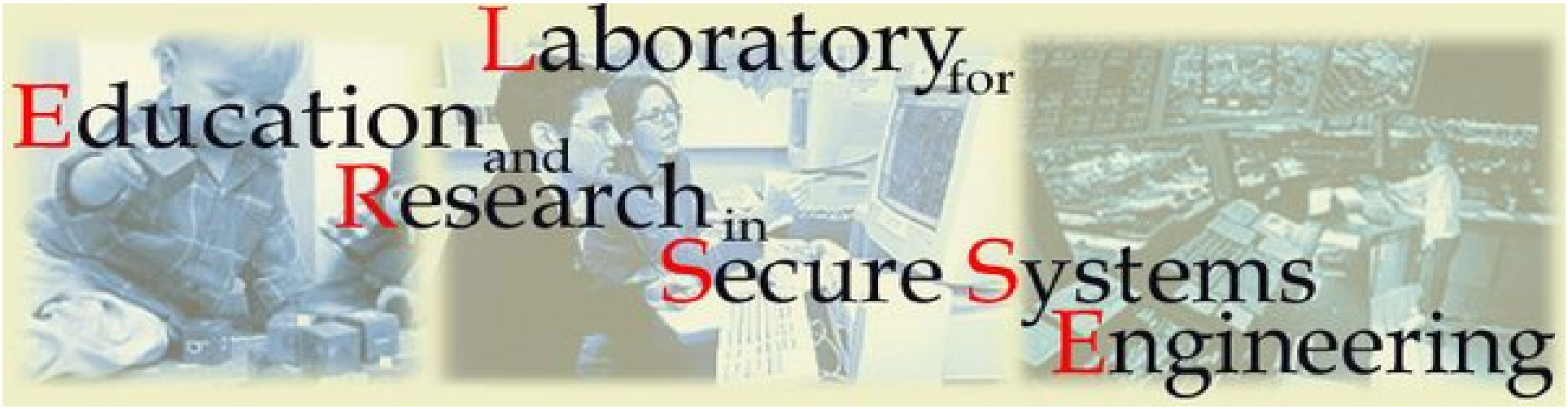
Improving Users' Mental Models of Personal Firewall

Fahimeh Raja

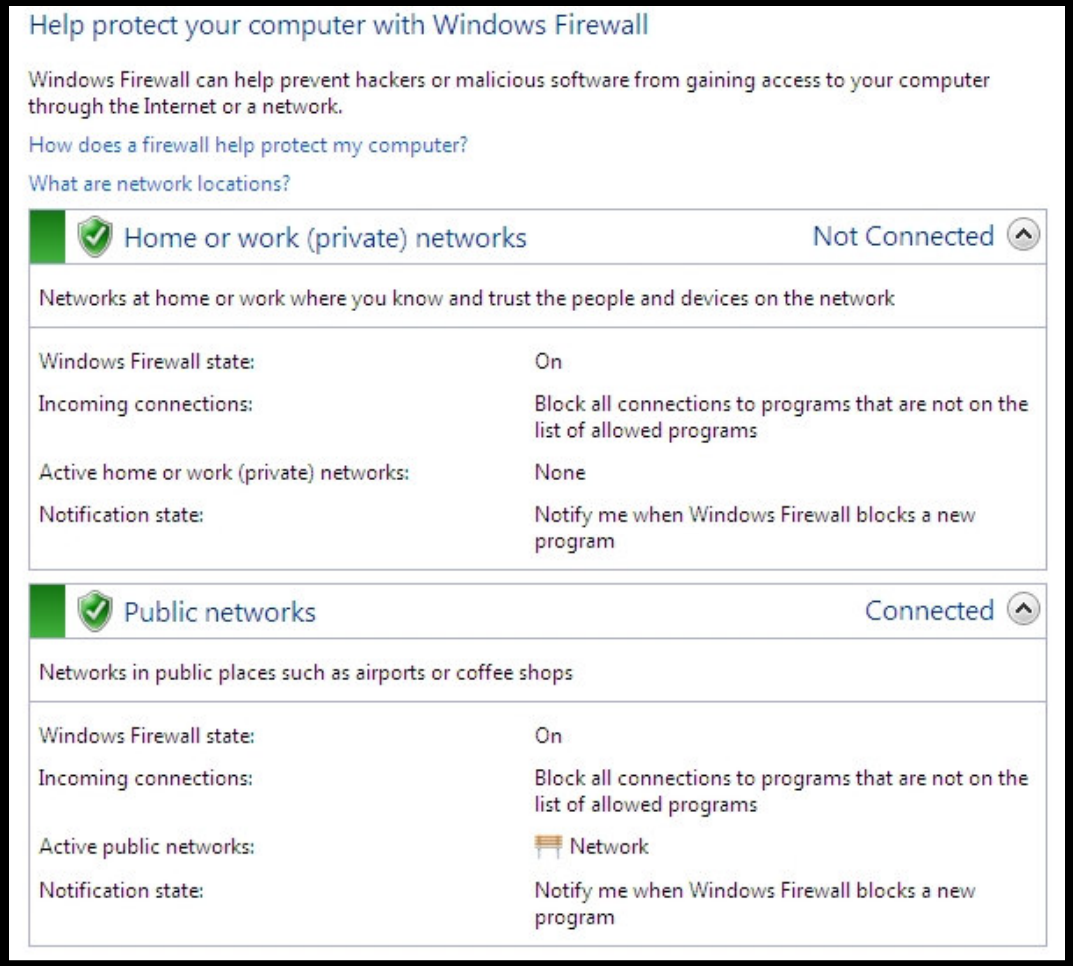


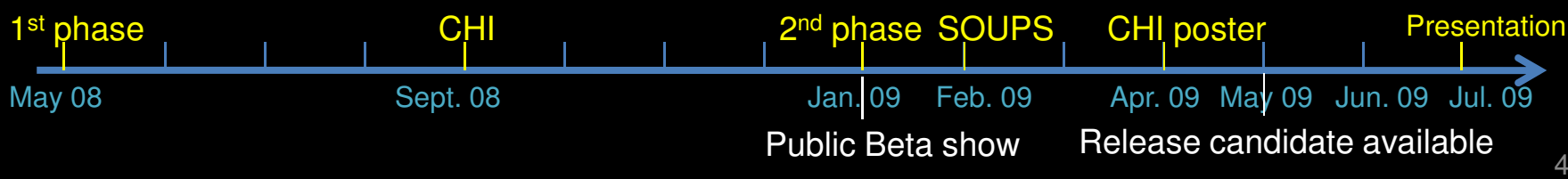
Kirstie Hawkey

Kosta Beznosov

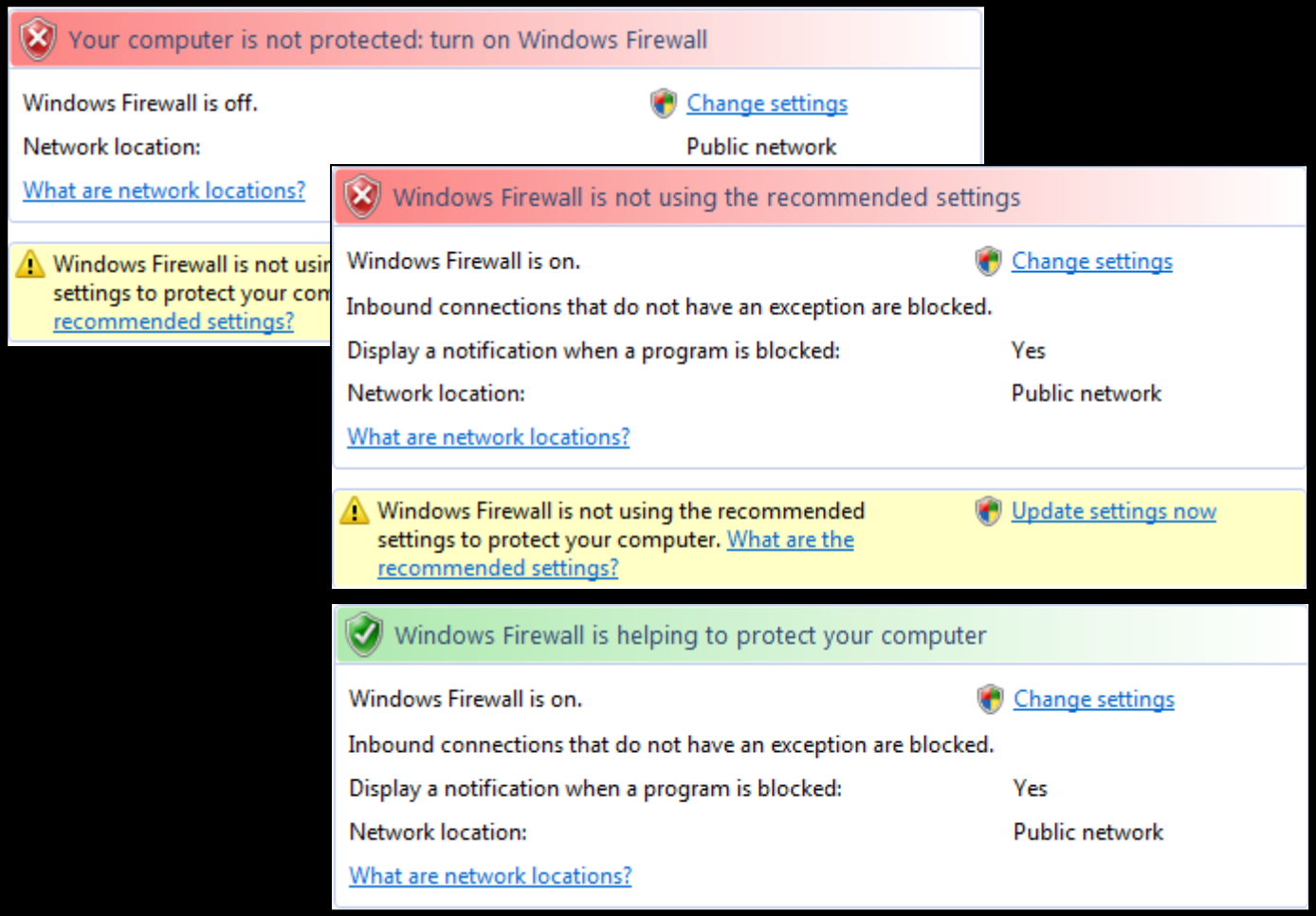


Windows 7 Firewall





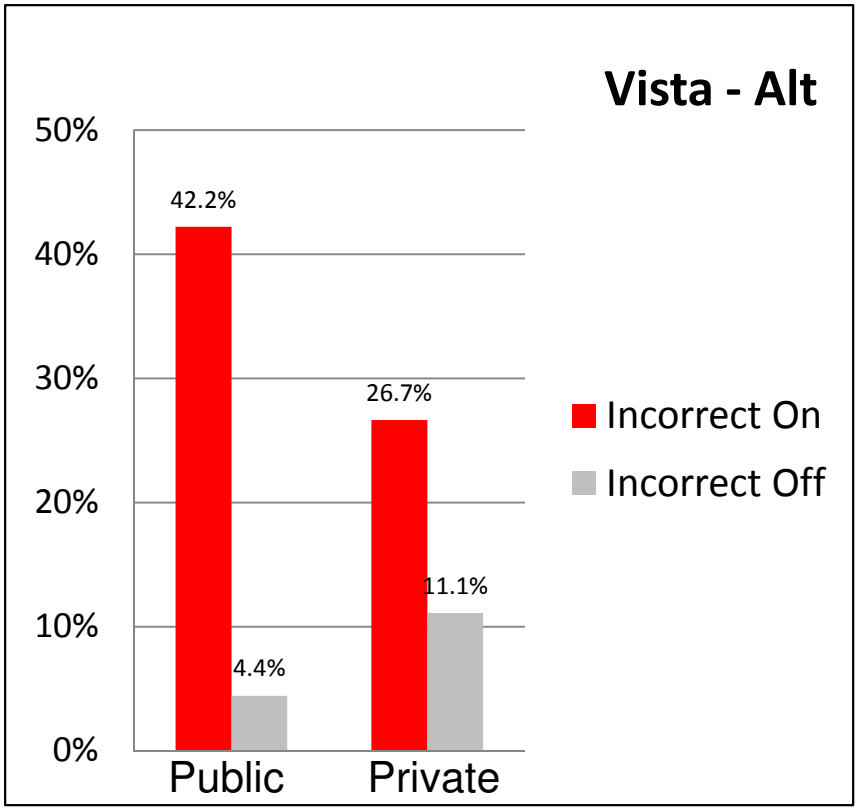
Possible states

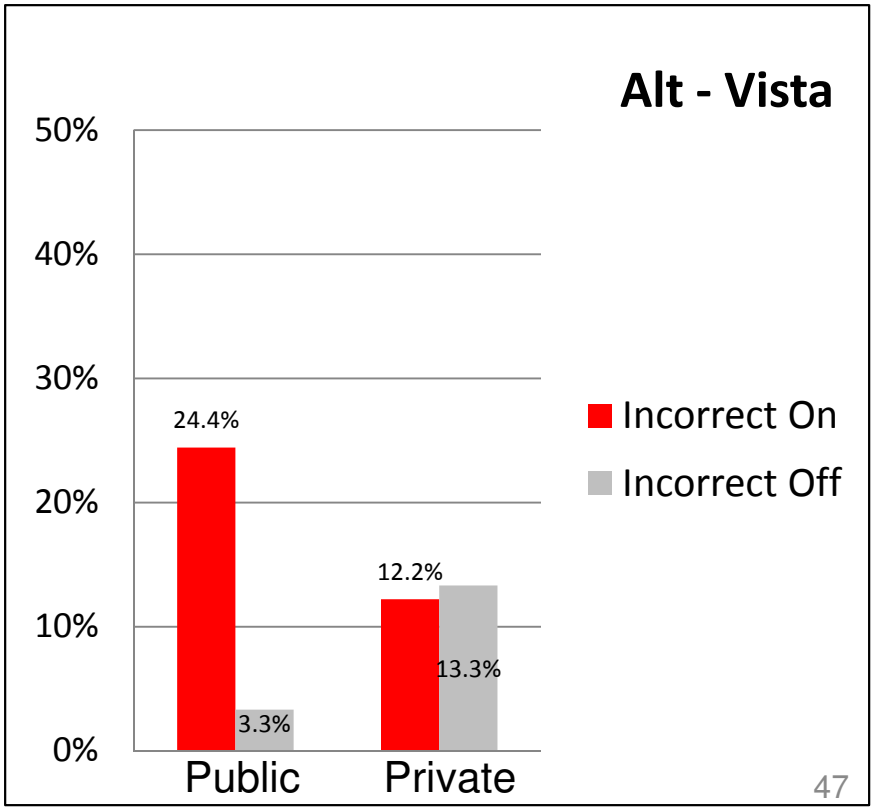


Incorrect Understanding of ***Vista*** Firewall Configuration

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

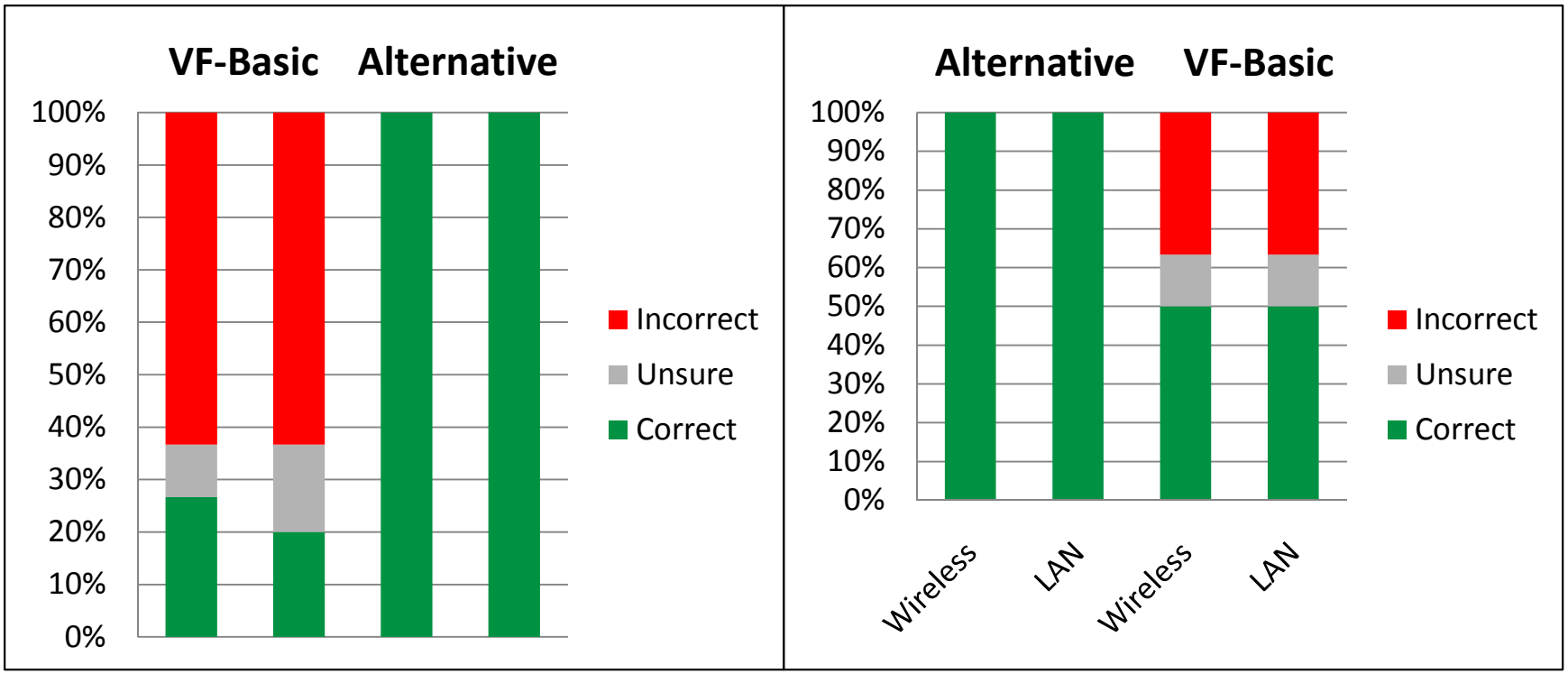
Incorrect on: Incorrectly believe that firewall is on, when it is off





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

J. Nielsen. User Education is not the Answer to Security Problems. 2004.

W. K. Edwards et. al. Security automation considered harmful? In NSPW'07.

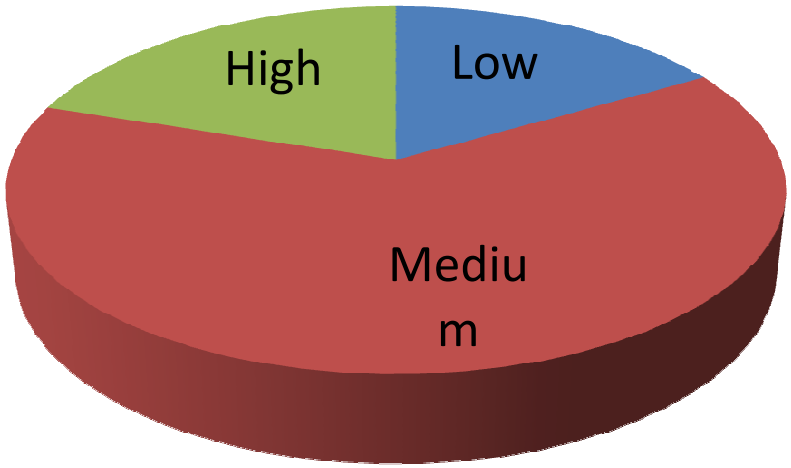
G. Chen and D. Kotz. A survey of context-aware mobile computing research. 2000.

BUT

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

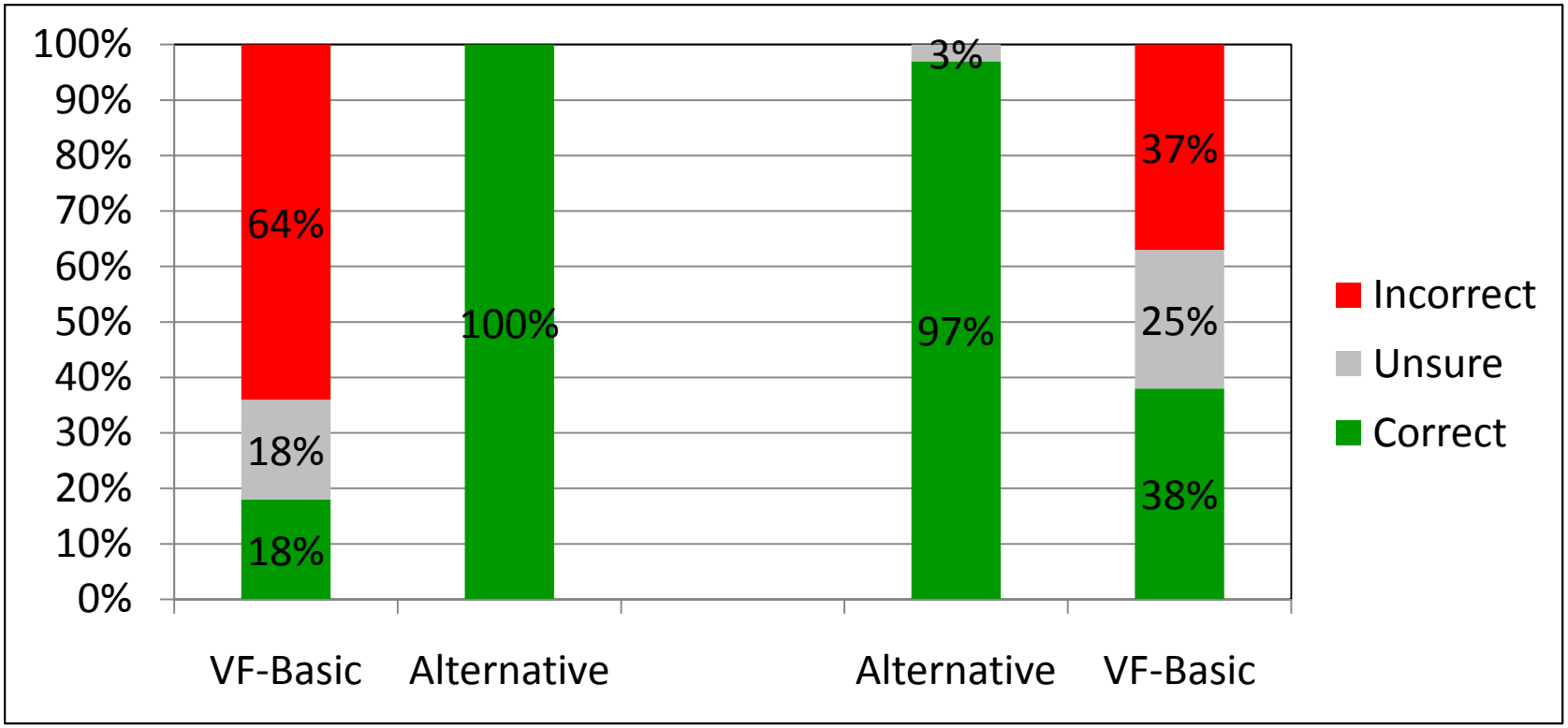
Future work

- Filed study examining what users know about or expects from a personal firewall
- How it would affect design and usability of personal firewalls


High
Low
Mediu
m

Understanding Firewall Configuration

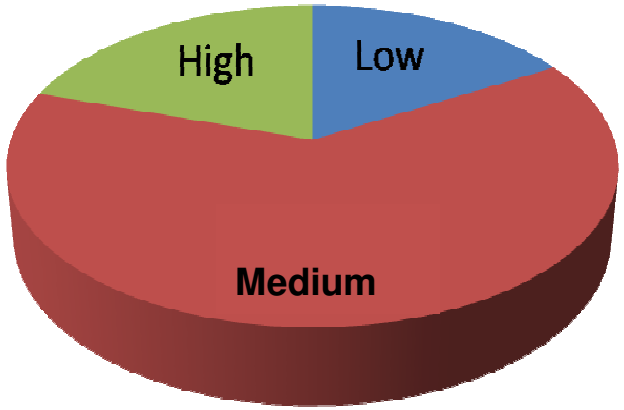
Public Network- Before Checking Interface



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