



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

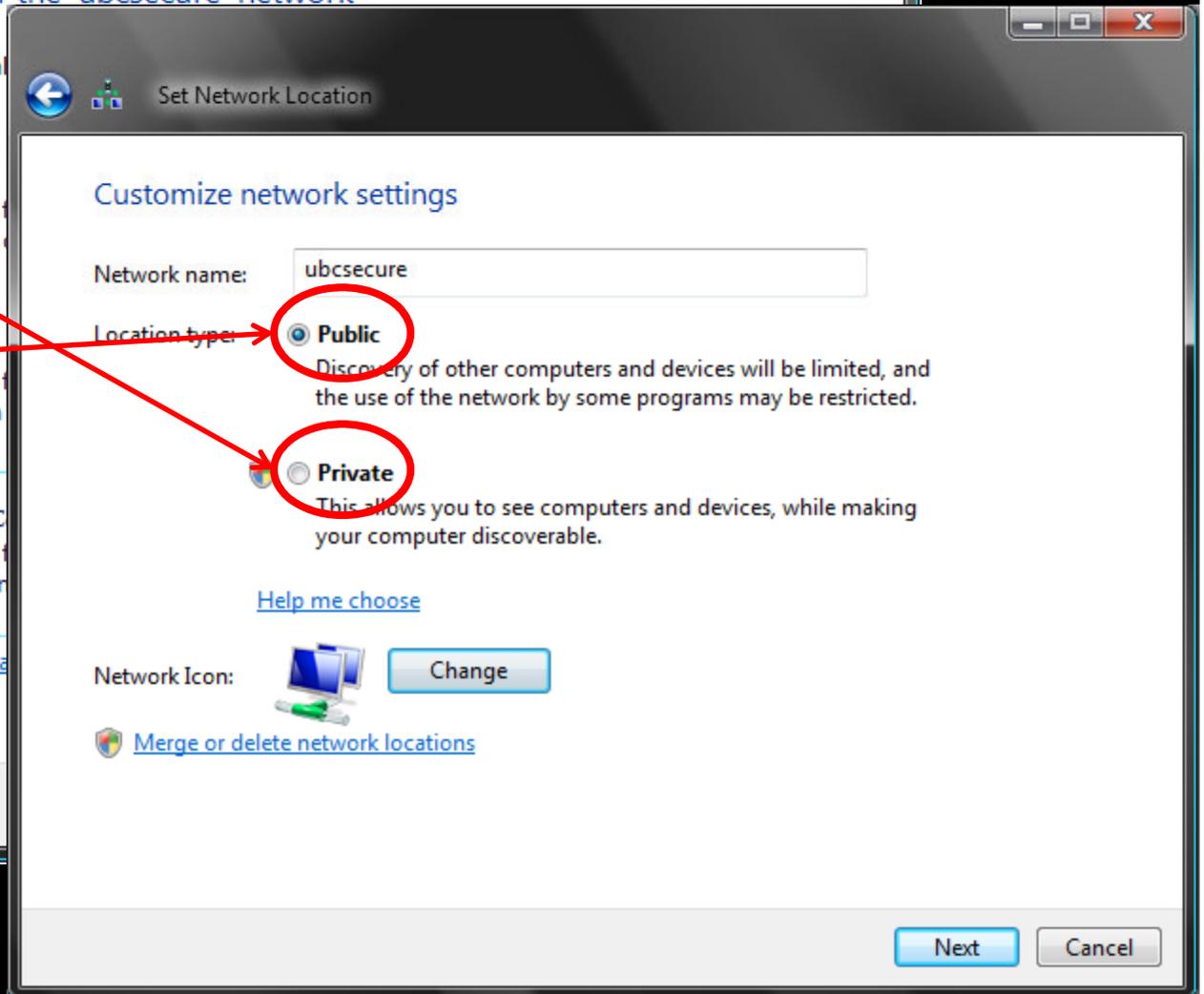
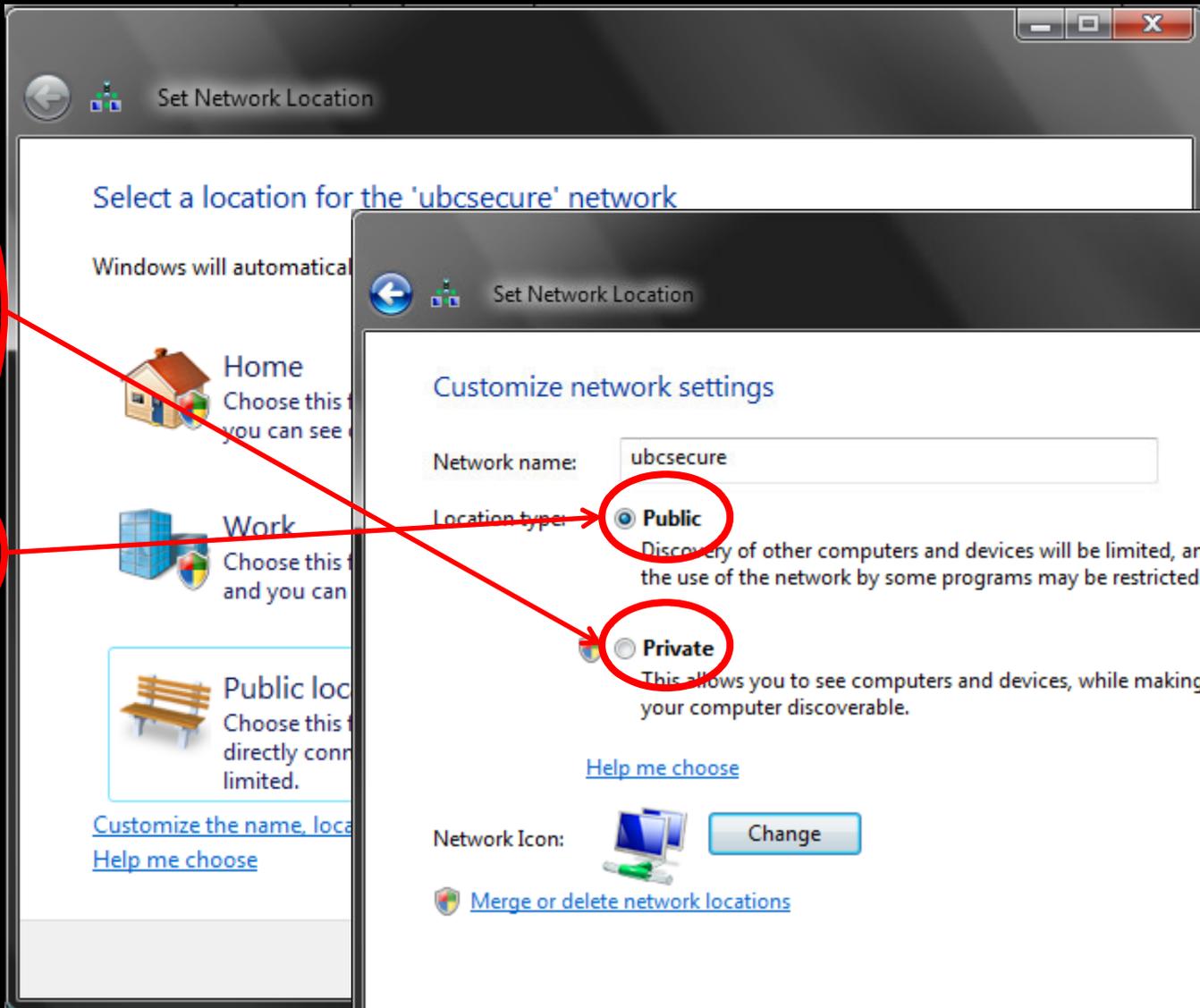
Otherwise

The hidden context can leave user in dangerous situations.

Network Location

in

Windows Vista



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

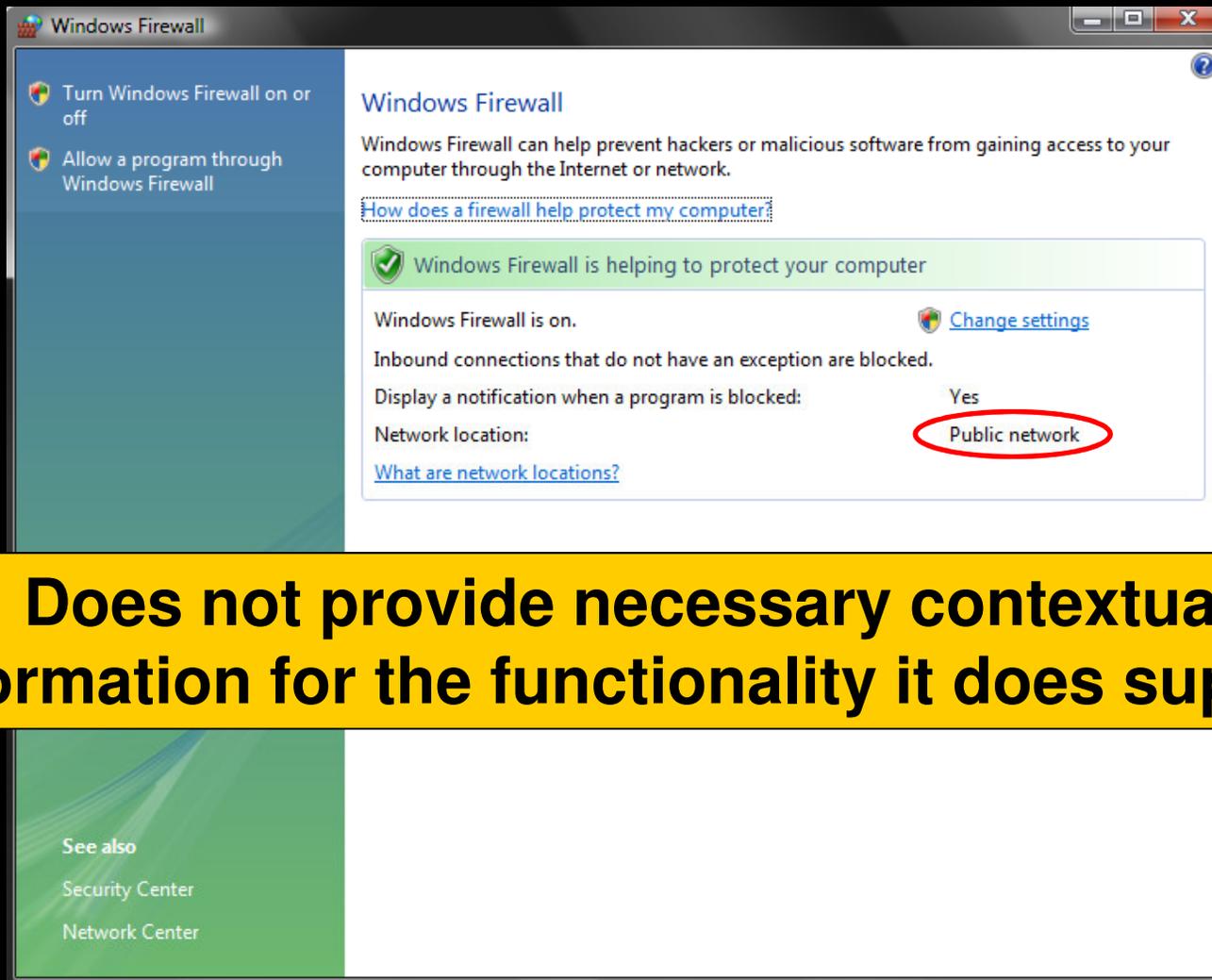
	Public Network Location 	Private Network Location 	Domain Network Location 
Wireless Network Connection 	On	Off	On
Local Area Connection 	On	Off	On
Bluetooth Network Connection 	Off	Off	Off

2 User Interfaces: Basic and Advanced

The screenshot shows the Windows Firewall with Advanced Security console. The left-hand navigation pane lists various settings including Inbound Rules, Outbound Rules, Connection Security Rules, Monitoring, Firewall, and Security Associations. The main pane displays the 'Overview' section for the 'Domain Profile', 'Private Profile', and 'Public Profile is Active'. Each profile section includes status indicators (checkmarks or red X's) and descriptive text about firewall status and connection handling. A yellow callout box is overlaid on the bottom half of the screenshot, containing the following text:

- 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

The image shows two overlapping windows from Windows Firewall. The background window, titled "Windows Firewall", displays a status message: "Your computer is not protected. Windows Firewall is off." This message is circled in red. Below it, it says "Network location:" followed by a link "What are network locations?". A yellow warning box below states "Windows Firewall is not using settings to protect your computer. Click here to view recommended settings?". At the bottom, there are links for "See also", "Security Center", and "Network Center".

The foreground window, titled "Windows Firewall Settings", has tabs for "General", "Exceptions", and "Advanced". The "General" tab is active and shows a green checkmark icon with the text "Windows Firewall is helping to protect your computer". Below this, it explains that Windows Firewall can help prevent hackers or malicious software from gaining access. There are three radio button options: "On (recommended)" (which is selected), "Block all incoming connections", and "Off (not recommended)". The "Off" option is described as making the computer more vulnerable. At the bottom of the dialog are "OK", "Cancel", and "Apply" buttons, along with a link "Tell me more about these settings".

The screenshot shows the Windows Firewall control panel window. On the left, there are two main options: 'Turn Windows Firewall on or off' and 'Allow a program through Windows Firewall'. The main content area is titled 'Windows Firewall' and contains the following text: 'Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.' Below this is a link: 'How does a firewall help protect my computer?'. A red watermark 'But at a cost!' is overlaid diagonally across the center of the window. A red circle highlights the text 'Windows Firewall is on.' in the status section. Below this, it says 'Inbound connections that do not have an exception are blocked.' and 'Display a notification when a program is blocked.' with a 'Yes' radio button selected. The 'Network location' is set to 'Public network'. At the bottom of the window, there is a yellow warning box that says 'Windows Firewall is not using the recommended settings to protect your computer. What are the recommended settings?' with an 'Update settings now' link. At the bottom of the screenshot, there is a yellow callout box with the text: 'Simplified interface: • Hidden network context • Automatic switching of firewall profiles'. The bottom of the window shows 'Security Center' and 'Network Center' links.

Windows Firewall

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 network.

[How does a firewall help protect my computer?](#)

Windows Firewall is not using the recommended settings to protect your computer. [Update settings now](#)

Windows Firewall is on. [Change settings](#)

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](#)

Security Center

Network Center

Simplified interface:

- Hidden 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

- 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

Windows Firewall is on for B...

Inbound connections that d...

[Change Settings for P...](#)

Private Network

Windows Firewall is on for V...

Inbound connections that d...

[Change Settings for P...](#)

Domain Network

Windows Firewall is on for a...

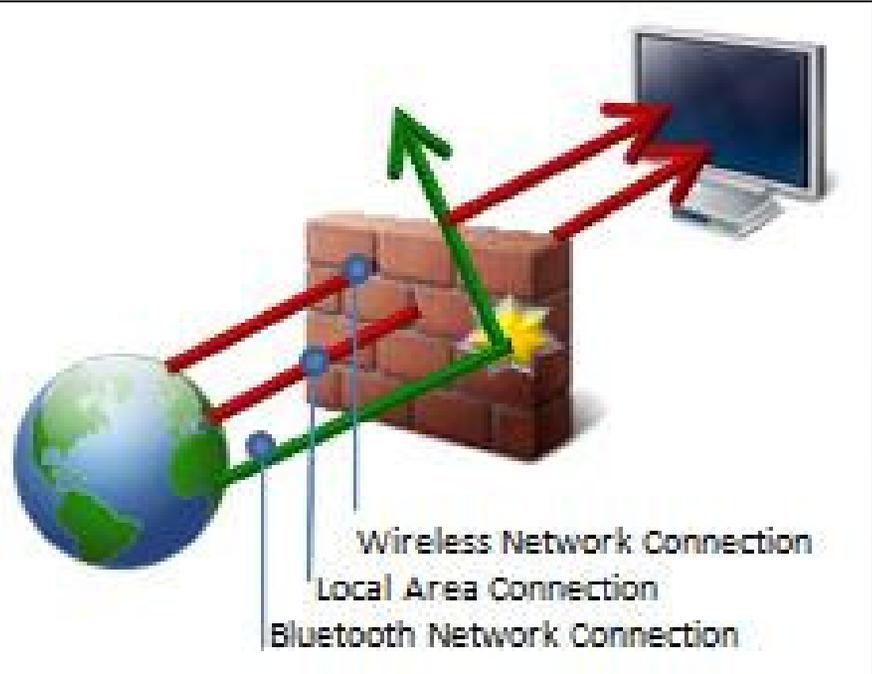
Inbound connections that d...

[Change Settings for D...](#)

[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

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

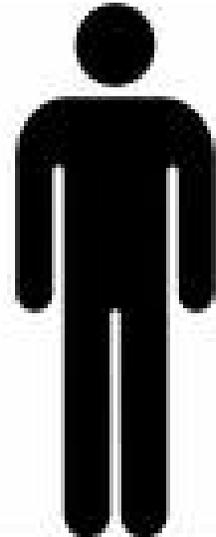
Study Design

- 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

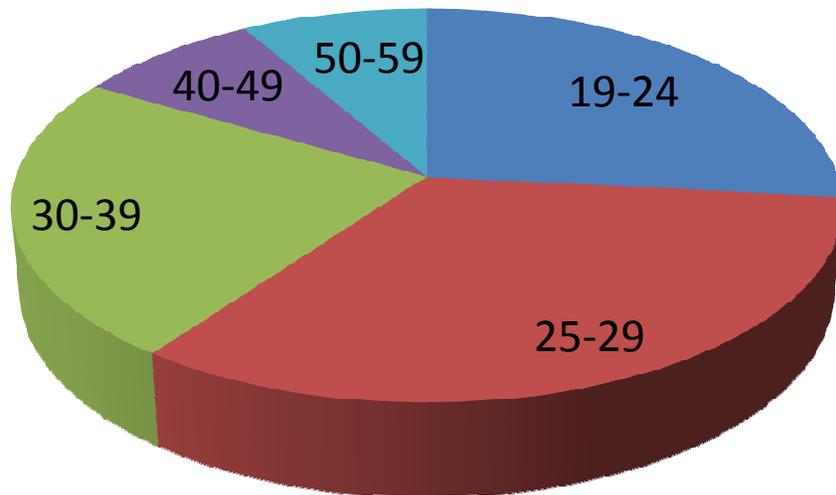


30

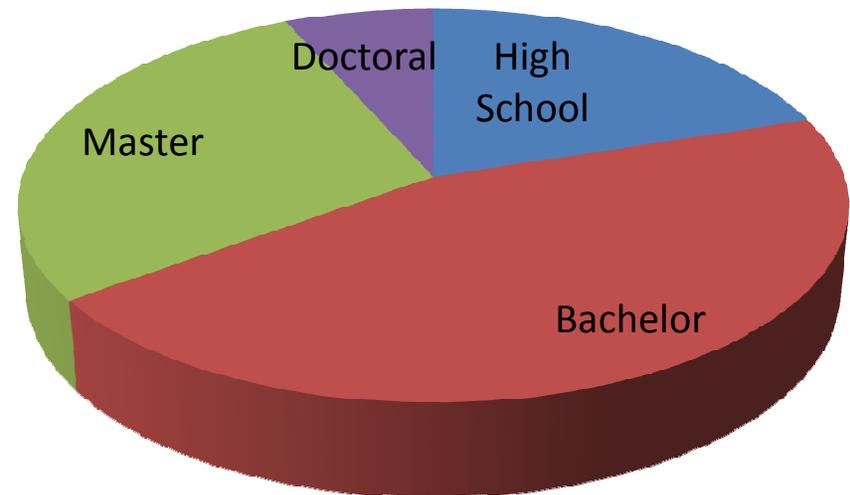


30

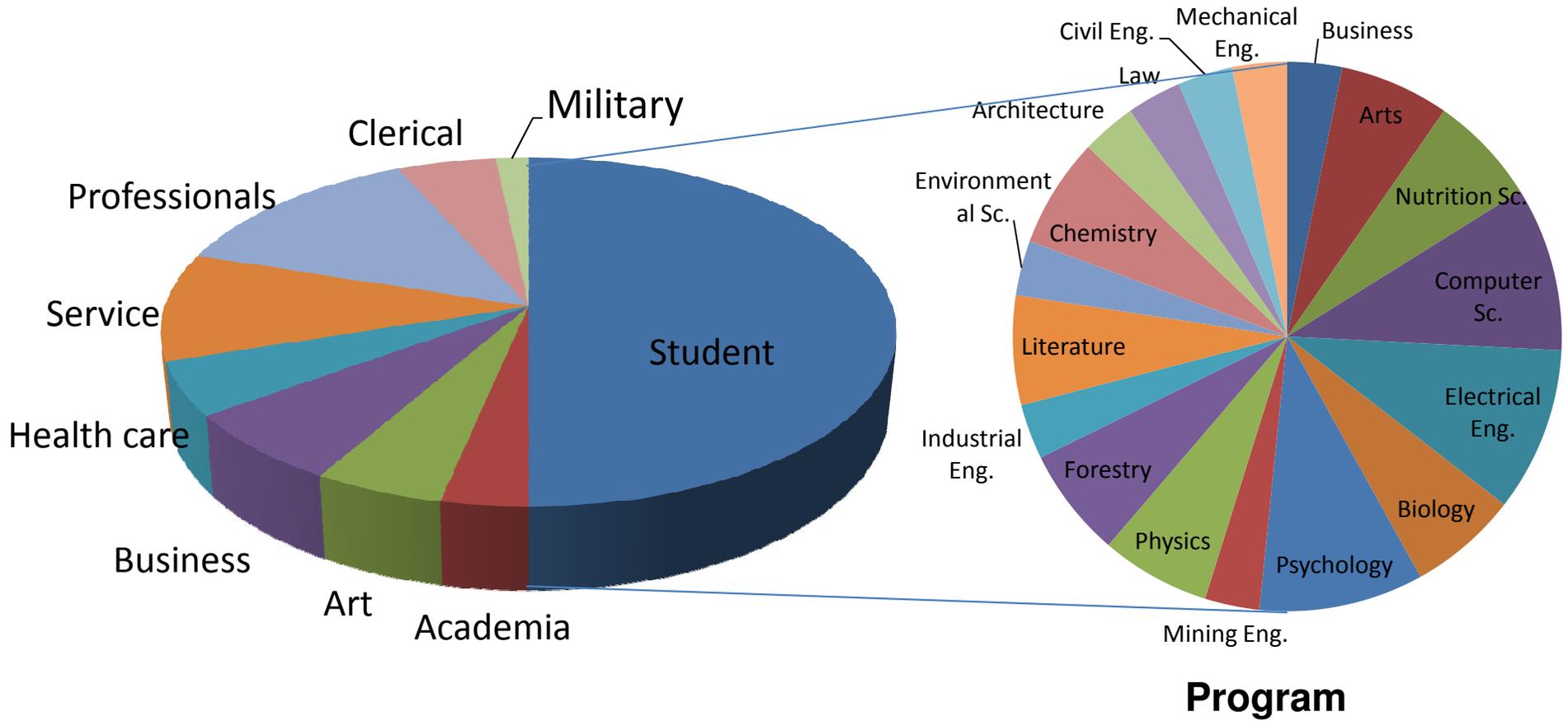
Age



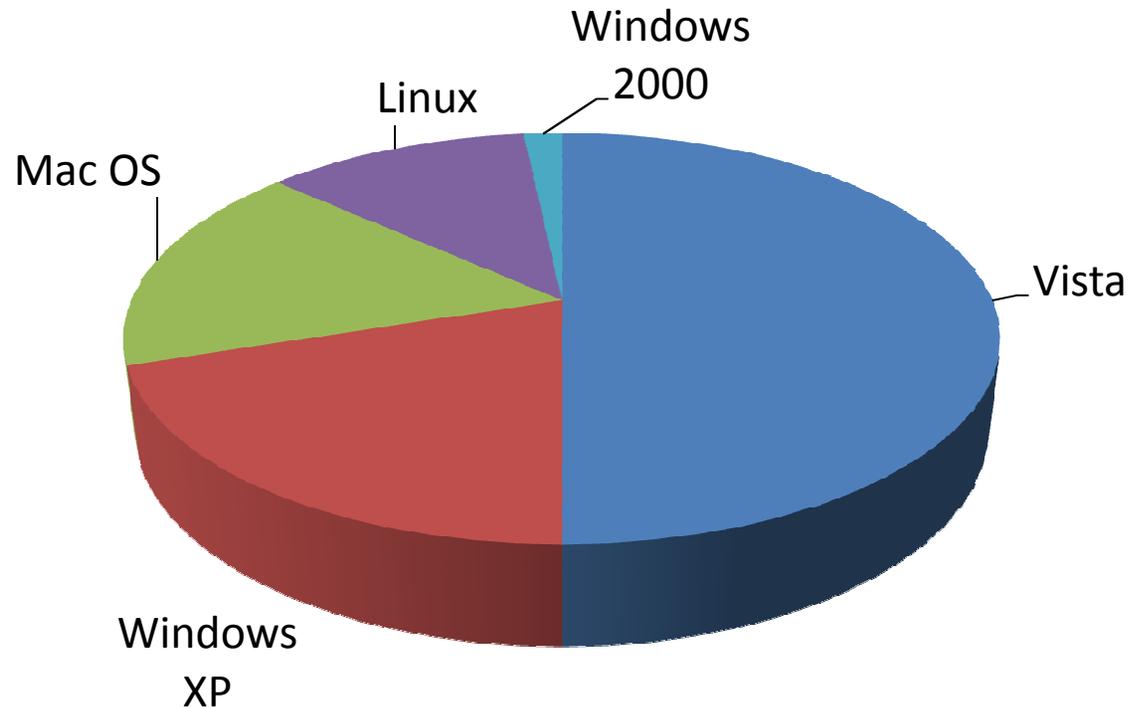
Completed Education



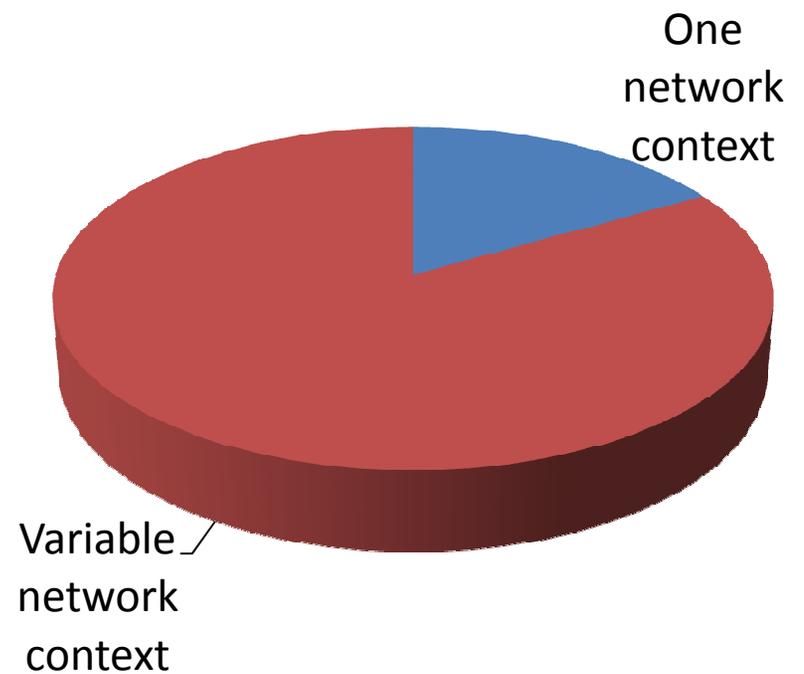
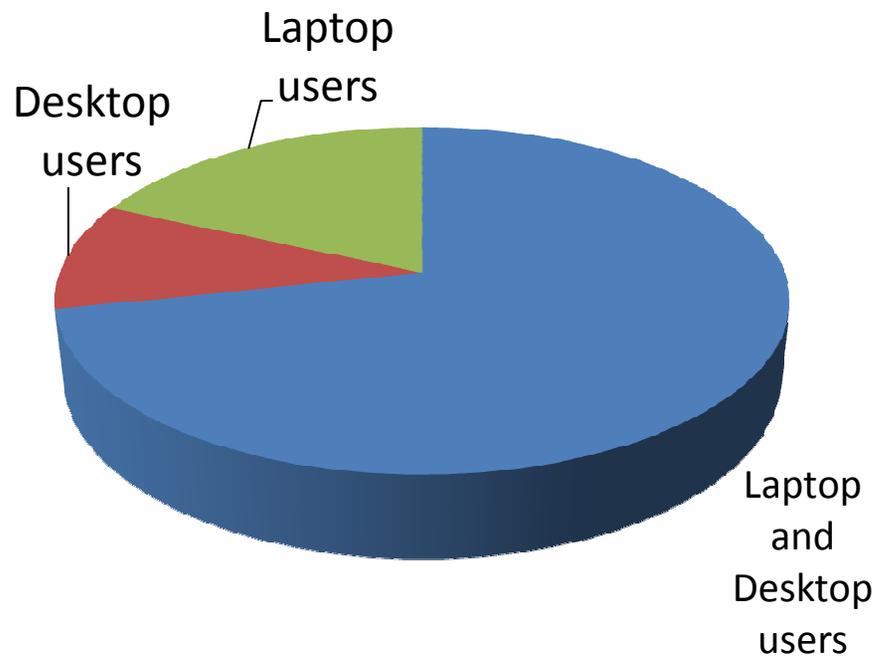
Occupation



All Daily Computer Users



Context of Use



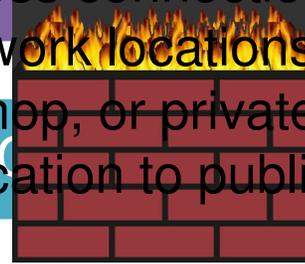
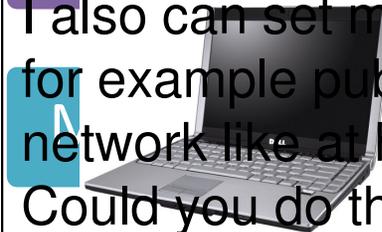
Study Protocol

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?



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

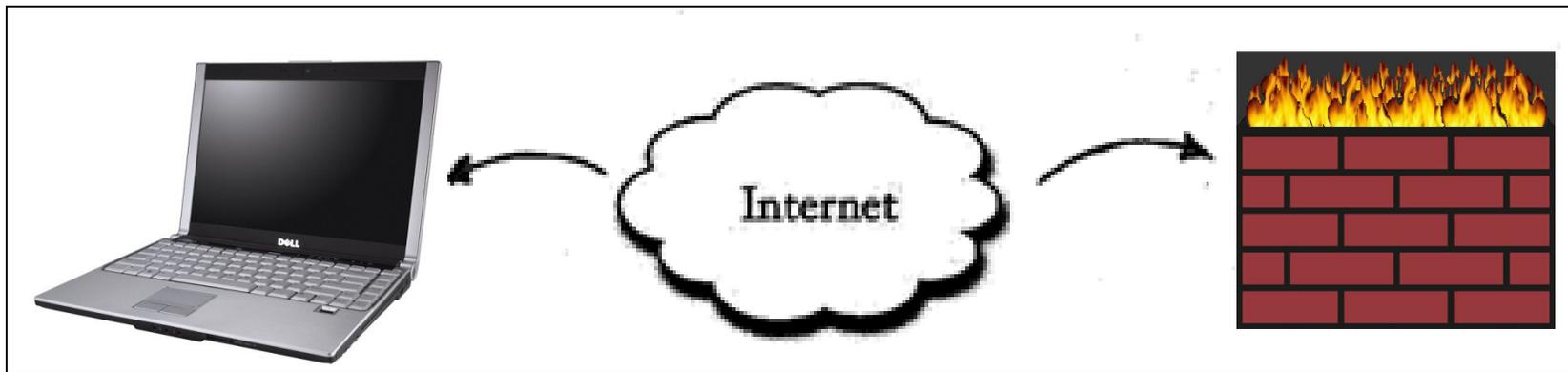
Results

Mental Models

- Incorrect
- Incomplete
- Partially complete
- Complete

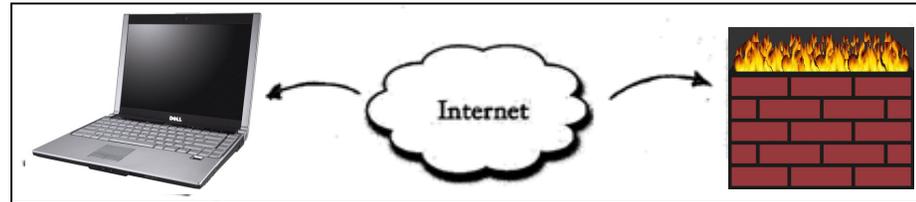
Mental Models

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

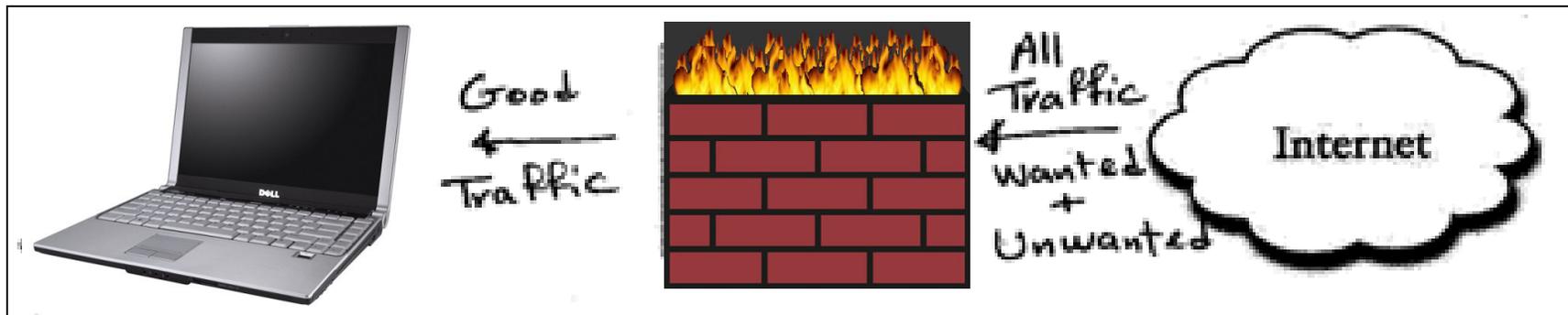


Mental Models

- Incorrect

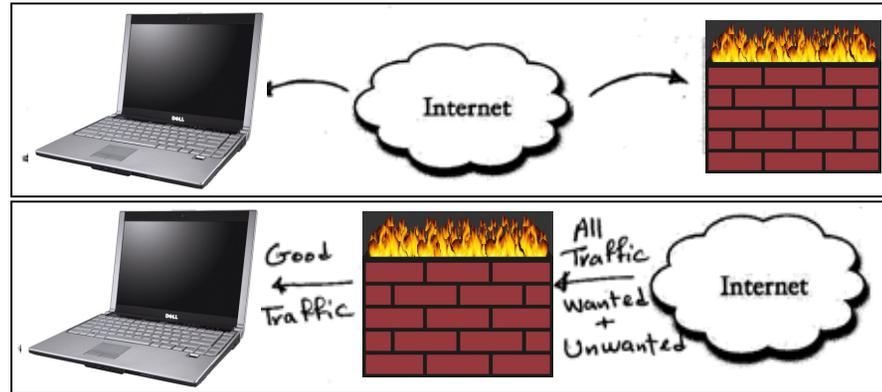


- **Incomplete:** correct basic understanding of firewall operation, without context of network location and connection

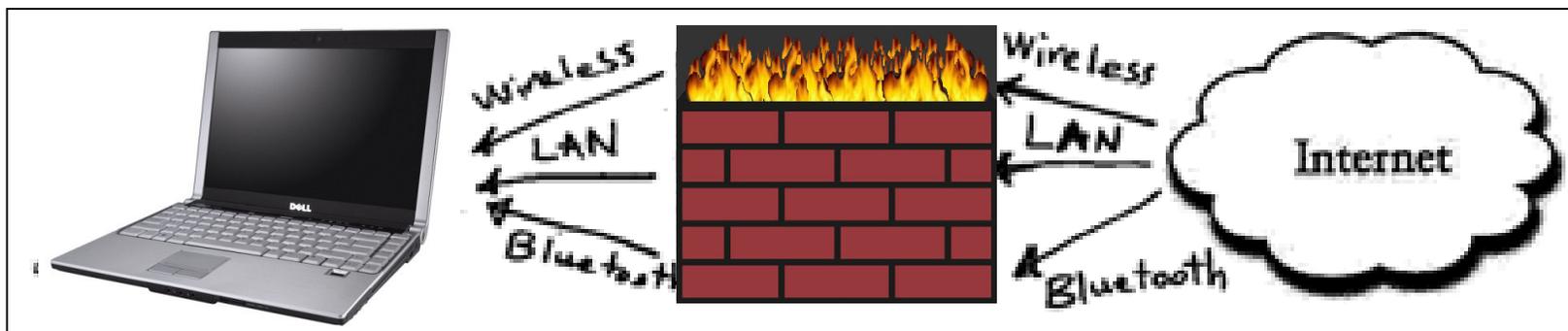


Mental Models

- Incorrect
- Incomplete

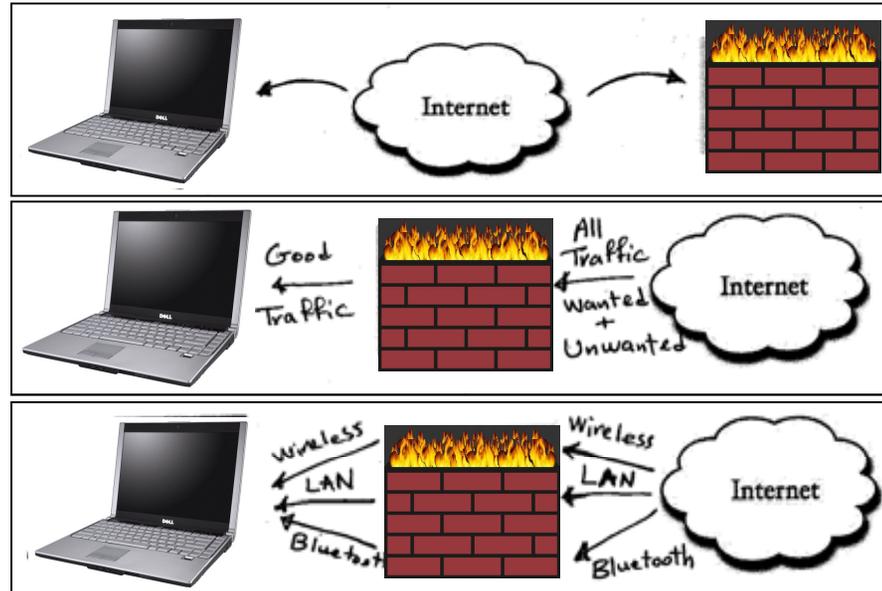


- **Partially complete:** correct basic understanding of firewall operation, with either context of network location or connection

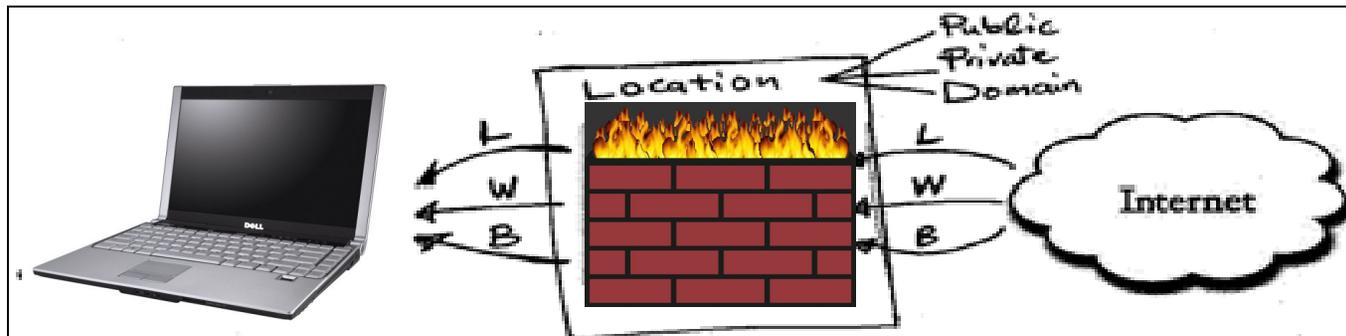


Mental Models

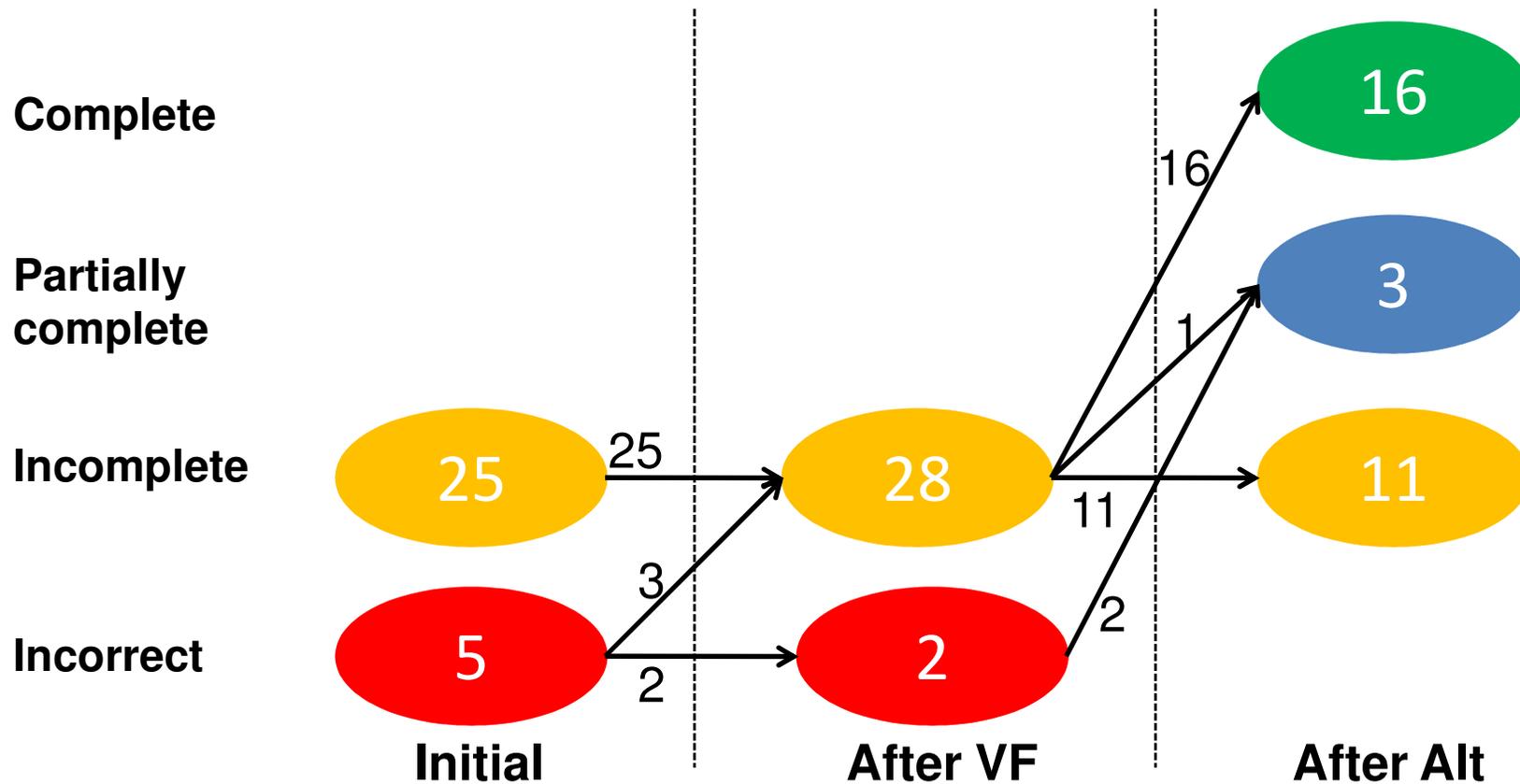
- Incorrect
- Incomplete
- Partially complete



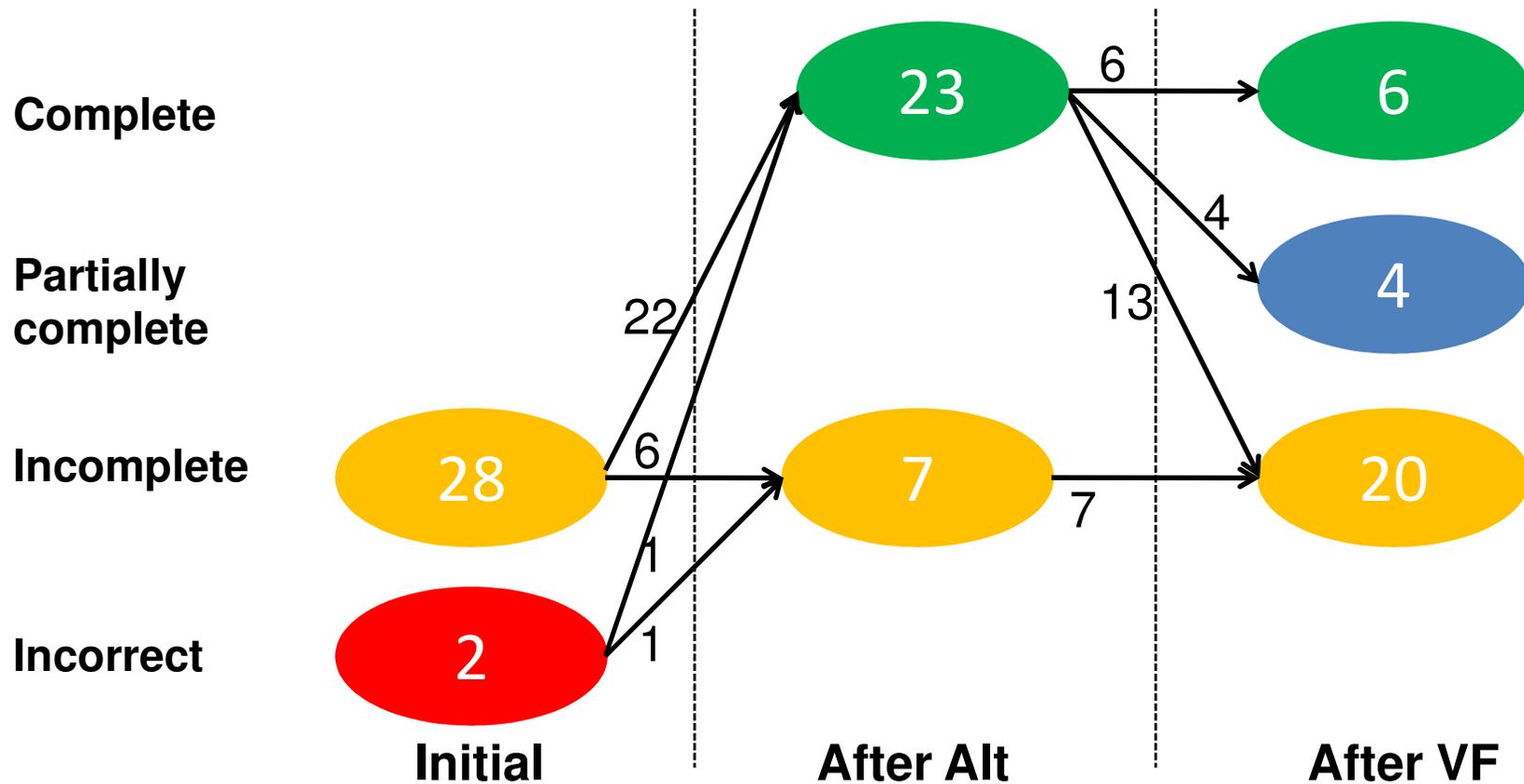
- **Complete:** correct basic understanding of firewall operation, with both context of network location and connection



First Vista Firewall Basic, then Alternative



First Alternative, then Vista Firewall Basic

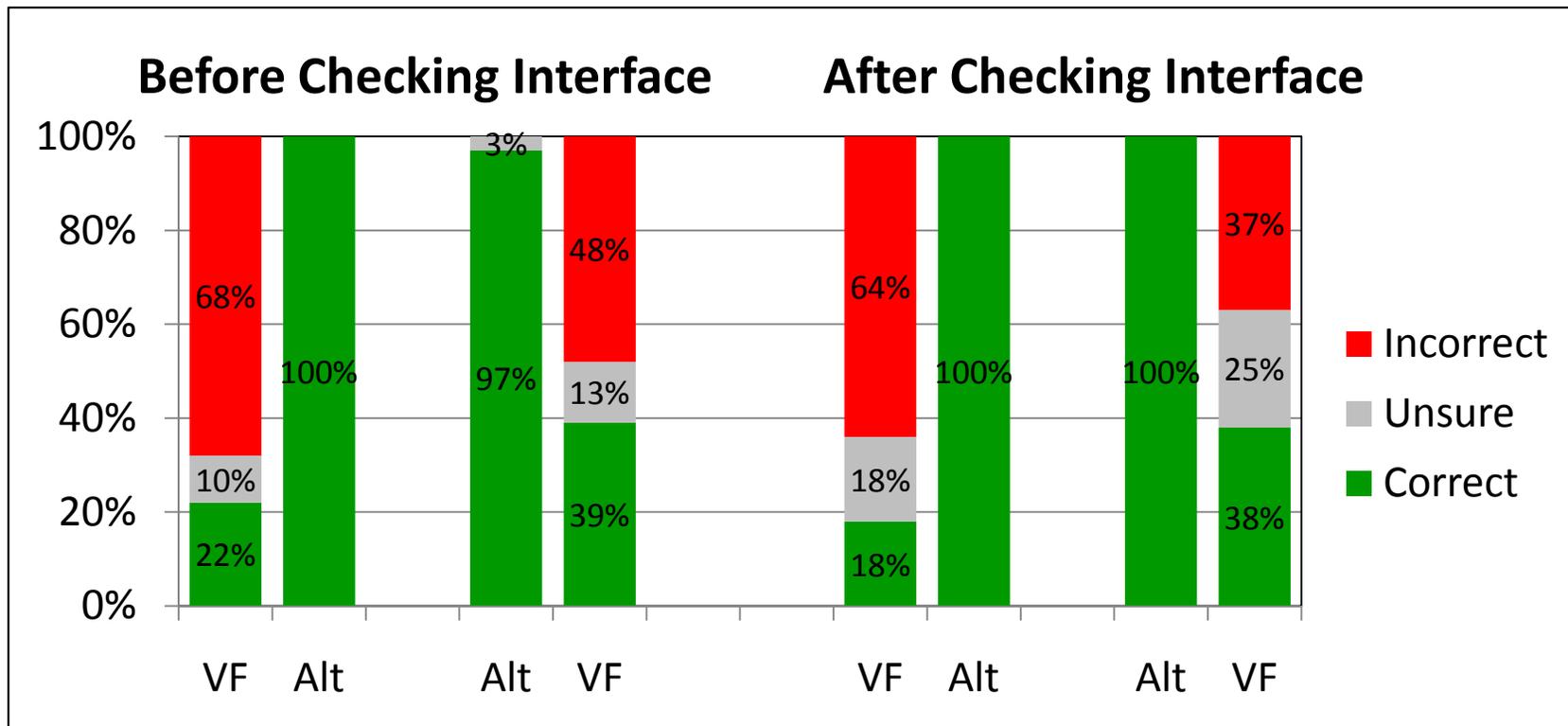


Understanding Firewall Configuration

	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

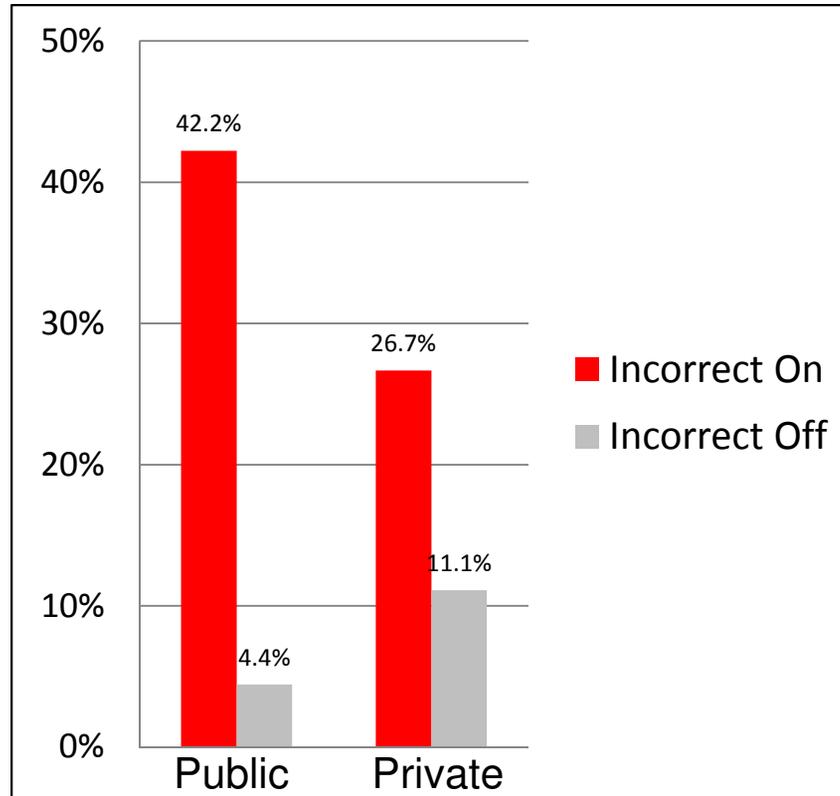
Understanding Firewall Configuration

Public Network



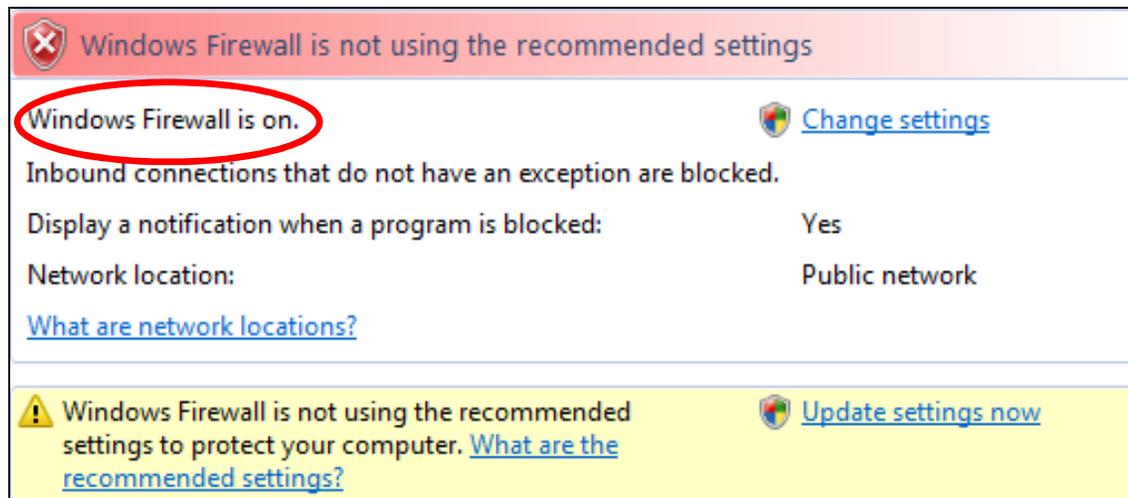
Vista-basic: large % of incorrect
 Alternative interface: Understood config.

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

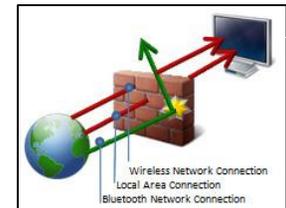
Feedback on Alternative Interface

- 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



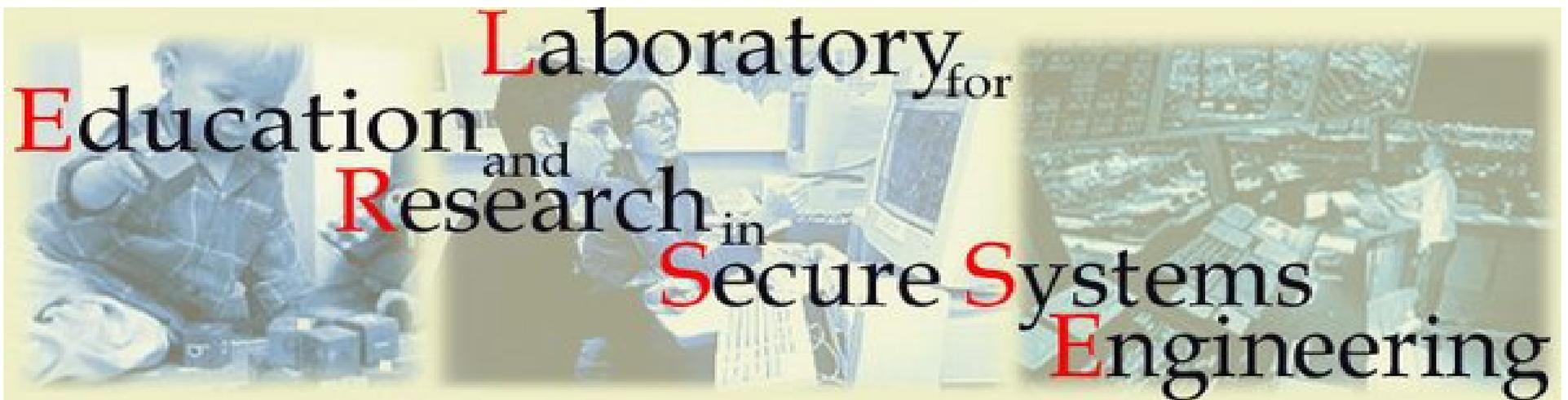
Fahimeh Raja



Kirstie Hawkey



Kosta Beznosov



Windows 7 Firewall

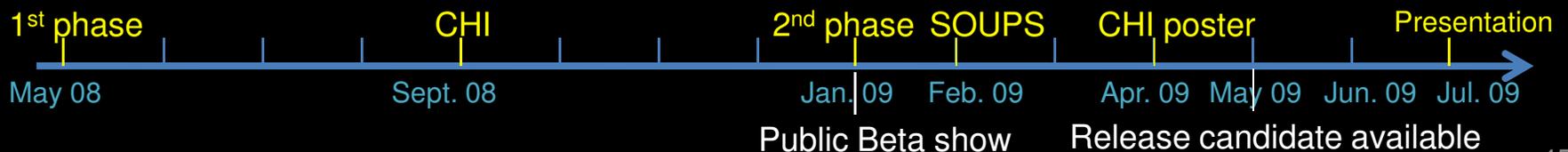
Help protect your computer with Windows Firewall

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	Not Connected 
Networks at home or work where you know and trust the people and devices on the network	
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	None
Notification state:	Notify me when Windows Firewall blocks a new program
 Public networks	Connected 
Networks in public places such as airports or coffee shops	
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	 Network
Notification state:	Notify me when Windows Firewall blocks a new program



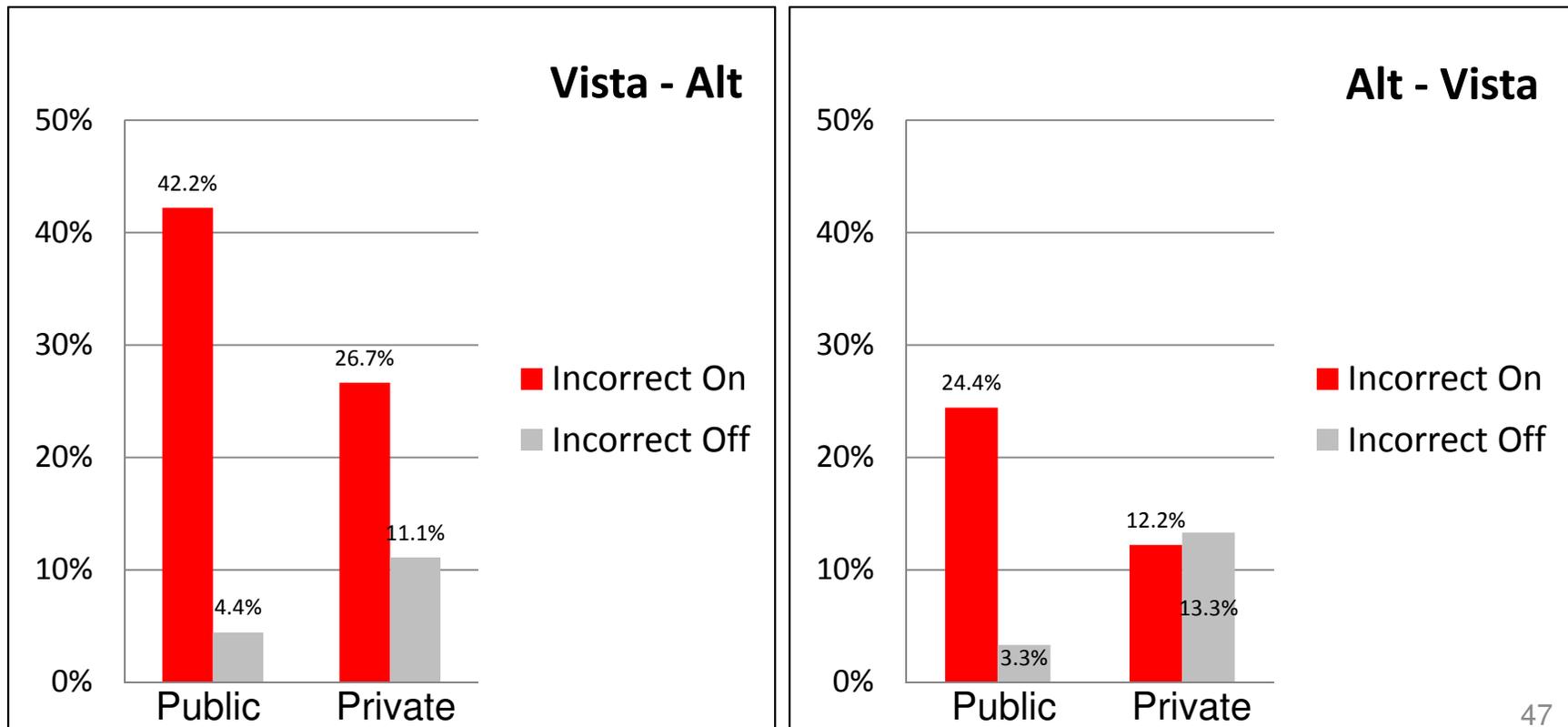
Possible states

The image displays three overlapping screenshots of the Windows Firewall settings interface, illustrating different operational states:

- Top-left panel (Red header):** "Your computer is not protected: turn on Windows Firewall". It shows "Windows Firewall is off." and "Network location: Public network". A "Change settings" link is visible.
- Middle panel (Red header):** "Windows Firewall is not using the recommended settings". It shows "Windows Firewall is on." and "Network location: Public network". It includes a "Change settings" link and a yellow warning banner: "Windows Firewall is not using the recommended settings to protect your computer. What are the recommended settings?".
- Bottom panel (Green header):** "Windows Firewall is helping to protect your computer". It shows "Windows Firewall is on." and "Network location: Public network". It includes a "Change settings" link and a yellow warning banner: "Windows Firewall is not using the recommended settings to protect your computer. What are the recommended settings?".

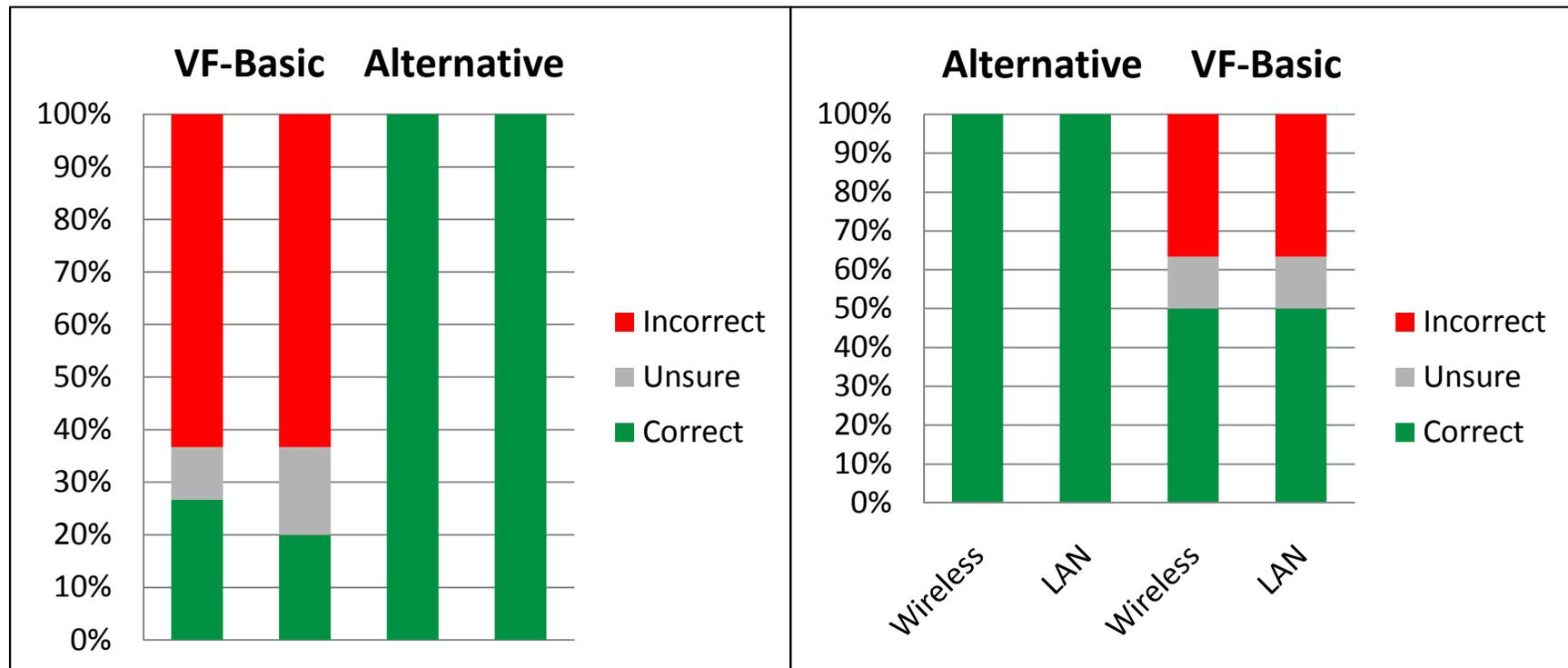
Incorrect Understanding of Vista Firewall Configuration

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.

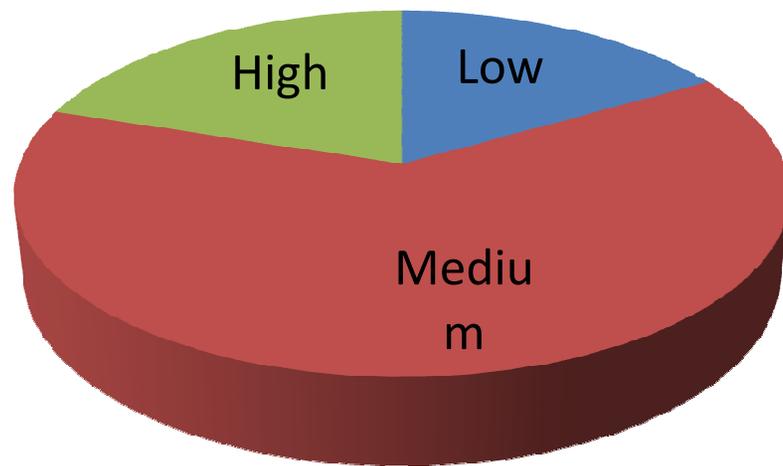
G. Chen and D. Kotz. A survey of context-aware mobile computing research. 2000.

BUT

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

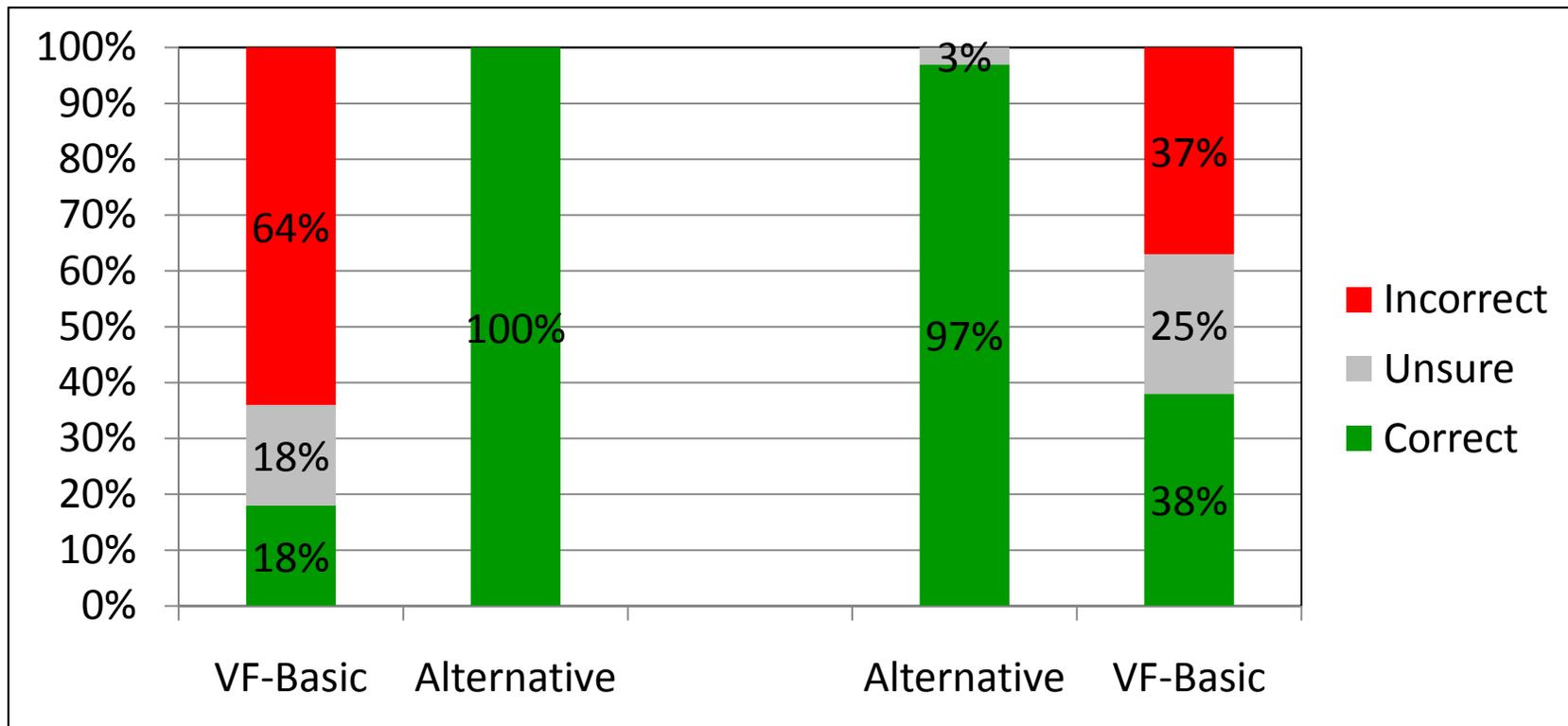
Future work

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



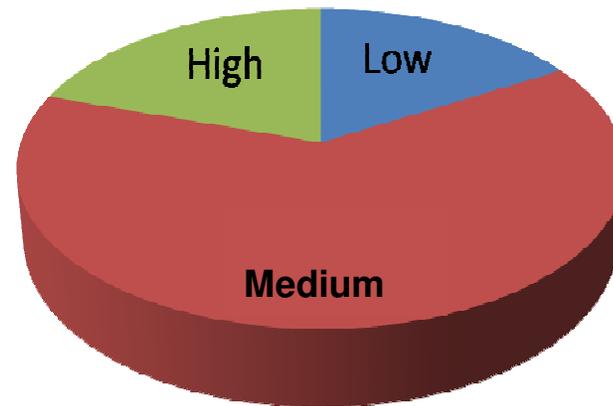
Understanding Firewall Configuration

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