Carnegie Mellon
CyLab
CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab
4616 HENRY STREET
PITTSBURGH, PA 15213
PH: (412) 268-7195
FX: (412) 268-7196
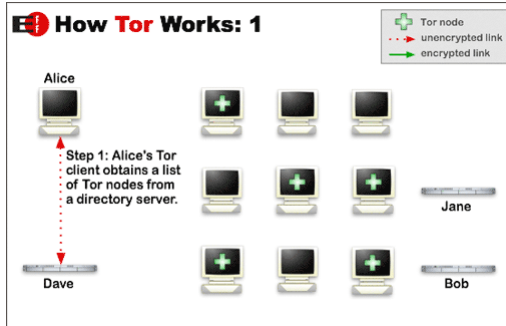www.cylab.cmu.edu

Web Browser
Privacy and Security

Cynthia Kuo

cykuo@cmu.edu

Today's Agenda

- Web browser privacy
  – FoxTor

- Surprise! A quick experiment

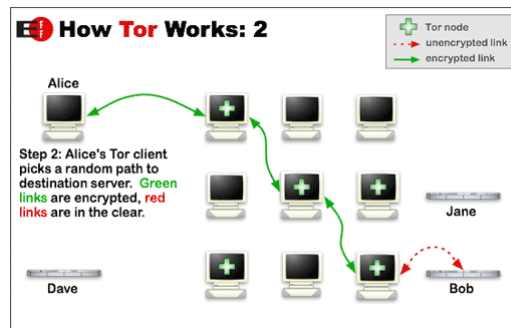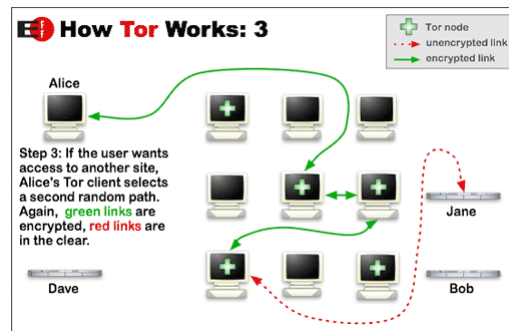- Web browser security
  – Firefox Phishing Prevention

2

Tor

How **Tor** Works: 1

Tor node
- - - ▸ unencrypted link
━━━▸ encrypted link

Alice

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

Dave

Jane

Bob

www.torproject.org

3

Tor

How **Tor** Works: 2

Tor node
- - - ▸ unencrypted link
━━━▸ encrypted link

Alice

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Dave

Jane

Bob

www.torproject.org

4

Tor

How Tor Works: 3

Tor node
unencrypted link
encrypted link

Alice

Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Dave

Jane

Bob

www.torproject.org

5

Web Browsing Privacy

- Tor
  - Onion routing
- Vidalia
  - Tor status
- Privoxy
  - Proxy (block cookies, etc.)

6

3

Needfinding

- Observe class trying to download and install Tor bundle
  - Several pieces to download
  - Many configuration steps
  - Slows down web traffic
  - Inadequate feedback
    - Unclear if application is using Tor
  - May not want to use Tor
    - Online shopping

7

Design Goals

- Simplify installation
  - One bundle to download
  - Minimal configuration
    - How?

8

Segment the Market

- Critical privacy needs
  - Anonymity is first priority
  - Political dissidents
- Selective privacy needs
  - Anonymity for some sites and when convenient
  - People looking for sensitive health information
- Basic privacy needs
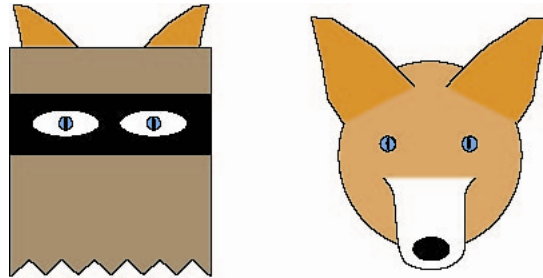 - Anonymity is attractive but not necessary
  - Cover traffic

9

Design Goals

- Simplify installation
  - One bundle to download
  - Minimal configuration
    - By level of privacy need
    - Target web browser
- Provide feedback
  - Is Tor working?
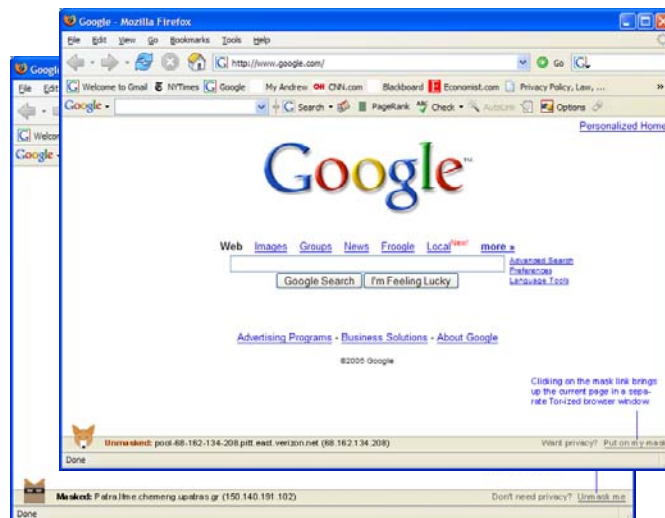- Increase convenience
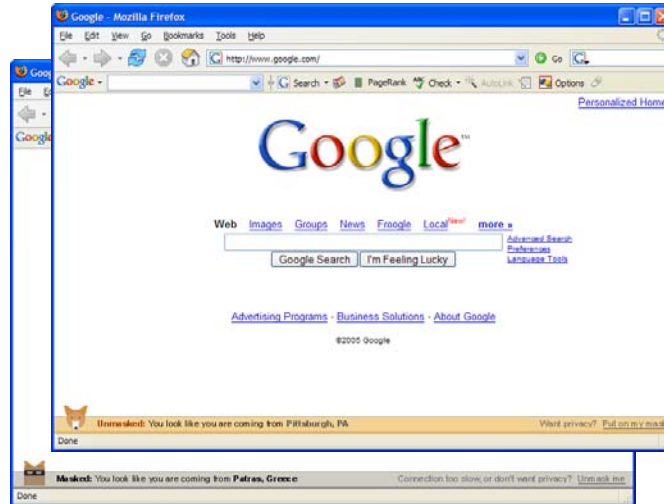 - Turn on/off as desired
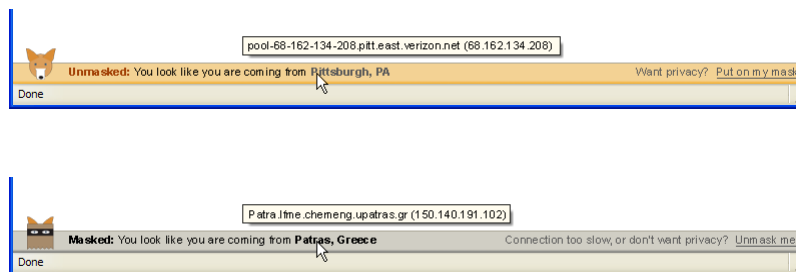
10

Masked/Unmasked

11

Browser Extension

12

6

Color, No IP Addresses

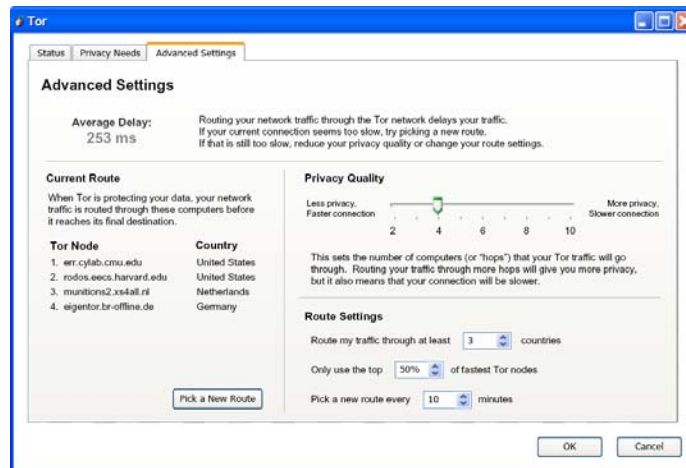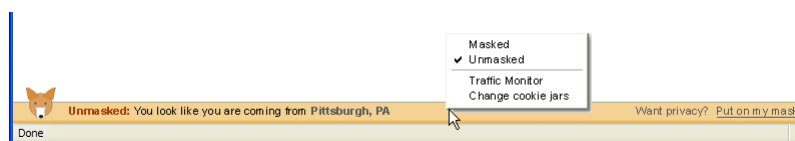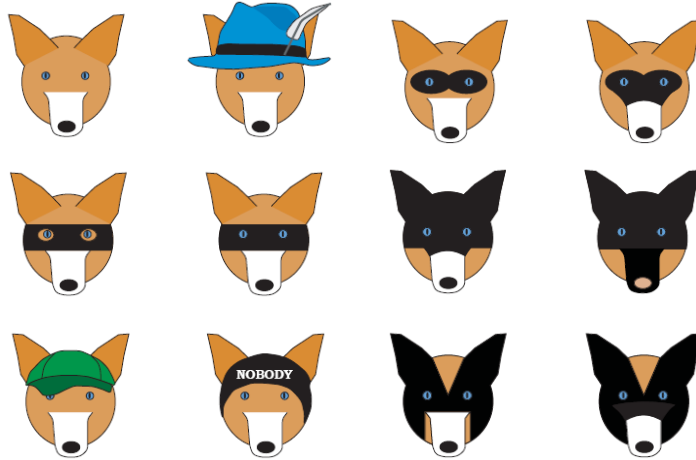## Advanced Rollover

Configuration

Cookie Jars

- What if you have cookies in one mode that you want to use in another mode?

Implementation

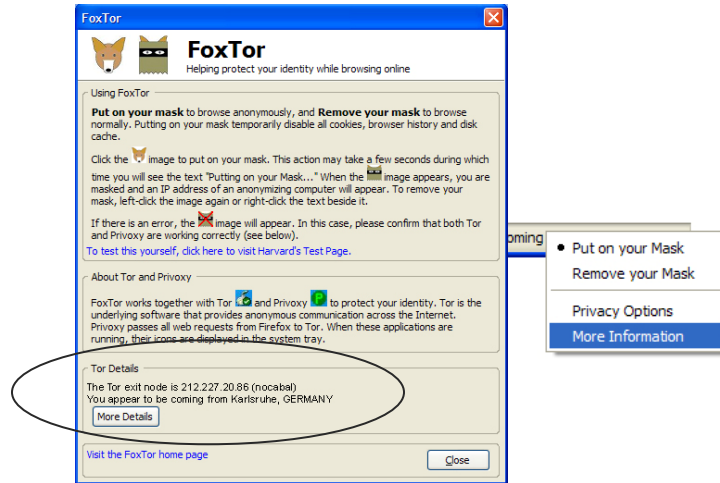**FoxTor**
Helping protect your identity while browsing online

Using FoxTor

Put on your mask to browse anonymously, and **Remove your mask** to browse normally. Putting on your mask temporarily disable all cookies, browser history and disk cache.

Click the 🦊 image to put on your mask. This action may take a few seconds during which time you will see the text "Putting on your Mask..." When the 🎭 image appears, you are masked and an IP address of an anonymizing computer will appear. To remove your mask, left-click the image again or right-click the text beside it.

If there is an error, the ✗ image will appear. In this case, please confirm that both Tor and Privoxy are working correctly (see below).
To test this yourself, click here to visit Harvard's Test Page.

About Tor and Privoxy

FoxTor works together with Tor and Privoxy to protect your identity. Tor is the underlying software that provides anonymous communication across the Internet. Privoxy passes all web requests from Firefox to Tor. When these applications are running, their icons are displayed in the system tray.

Tor Details

The Tor exit node is 212.227.20.86 (nocabal)
You appear to be coming from Karlsruhe, GERMANY

More Details

Visit the FoxTor home page   Close

- Put on your Mask
  Remove your Mask

  Privacy Options
  More Information

FoxTor

- > 130,000 downloads since 10/2006

- https://addons.mozilla.org/en-US/firefox/addon/3606

Today's Agenda

- Web browser privacy
  - FoxTor

- Surprise! A quick experiment

- Web browser security
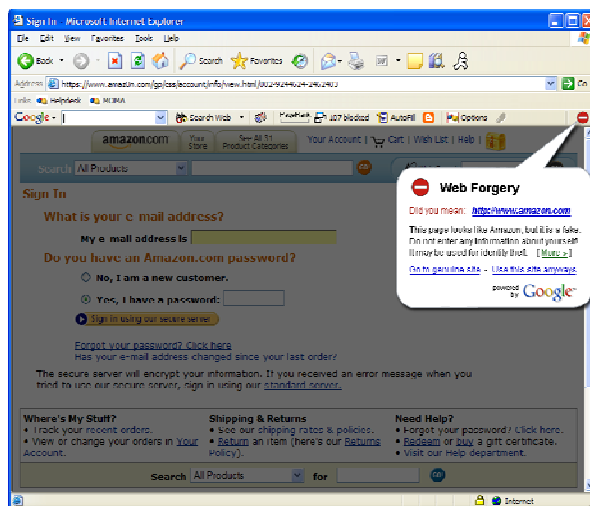 - Firefox Phishing Prevention

21

How to Stop Phishing?

- Don't click on links
  - Rate every link
  - Rollover & see rating
  - Won't miss a site you never saw

22

[Mockups removed for posting on website]

Maps Bubble

- Warning bubble and icon used to appear trustworthy

- Gray background to emphasize danger and to catch attention

- Bubble attached to browser chrome to convey message origin
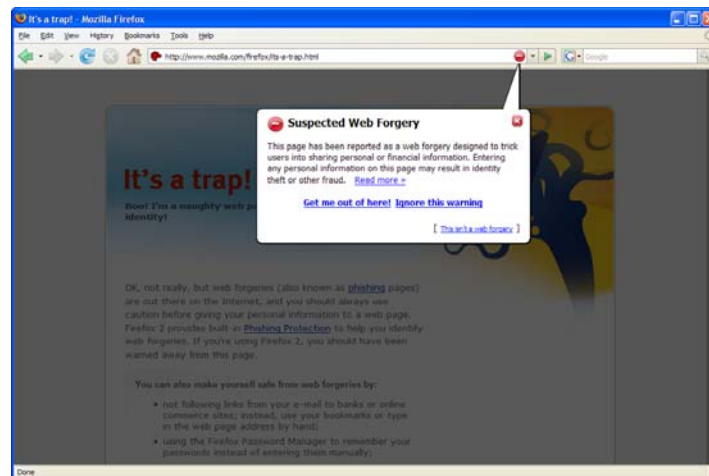
- Active elements on page disabled

Lessons

- Establish trustworthiness of message
  - Origin
  - Authority
- Match intrusiveness to severity
  - No false positives
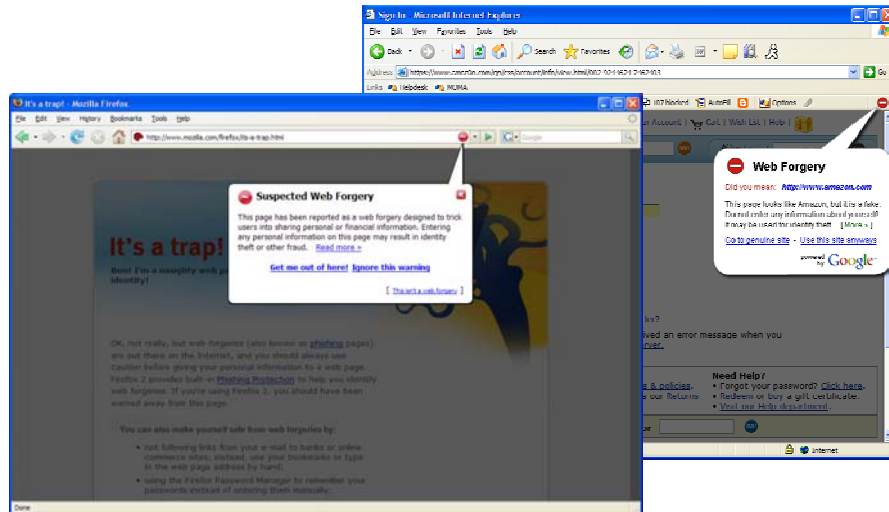- Recommend what actions to take
- Provide a feeling of closure

25

Firefox Phishing Prevention

26

Design vs. Implementation

Thank you!

Questions? Comments?
cykuo@cmu.edu