Anonymity, Usability, and Humans. Pick Two.

Andrew Lewman
andrew@torproject.org

16 May 2011
What are we talking about?

- Crash course on anonymous communications
- Quick overview of Tor
- Usability, Security, and Humans
Anonymity, Usability, and Humans. Pick Two.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy.
What is anonymity?
Anonymity isn’t cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.
Anonymity isn’t steganography

Attacker can tell Alice is talking to someone, how often, and how much data is sent.
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
Anonymity isn’t just wishful thinking...

- ”You can’t prove it was me!”
- ”Promise you won’t look”
- ”Promise you won’t remember”
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
- "Promise you won’t tell"
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
- "Promise you won’t tell"
- "I didn’t write my name on it!"
Anonymity isn’t just wishful thinking…

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
- "Promise you won’t tell"
- "I didn’t write my name on it!"
- "Isn’t the Internet already anonymous?"
..since “weak” isn’t anonymity.

“*You can’t prove it was me!*” Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
“Since "weak" isn’t anonymity.

- "Promise you won’t look/remember/tell" Will other parties have the abilities and incentives to keep these promises?
..since "weak" isn't anonymity.

- "I didn't write my name on it!" Not what we're talking about.
..since "weak" isn't anonymity.

"Isn't the Internet already anonymous?" Nope!
Anonymous communication

• People have to hide in a crowd of other people ("anonymity loves company")
• The goal of the system is to make all users look as similar as possible, to give a bigger crowd
• Hide who is communicating with whom
• Layered encryption and random delays hide correlation between input traffic and output traffic
Low-latency versus High-latency anonycomm systems

- Tor is not the first system; ZKS, mixmaster, single-hop proxies, Crowds, Java Anon Proxy.
- Low-latency systems are vulnerable to end-to-end correlation attacks.
- High-latency systems are more resistant to end-to-end correlation attacks, but by definition, less interactive.
Low-latency systems are all the rage

- Interactive apps: web, instant messaging, VOIP, ssh, X11, cifs/nfs, video streaming (millions of users)
- Multi-hour delays: email, nntp, blog posting? (tens of thousands of users?)
Low-latency systems are all the rage

- And if anonymity loves company...
What is Tor?

- online anonymity software and network
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  - Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  - Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- increasingly diverse toolset:
  - Tor, Torbutton, Tor Browser Bundle, TAILS Anonymous Operating System, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, Tor Wall, TorVM
How is Tor different from other systems?
How is Tor different from other systems?

[Diagram showing a network of connections involving Alice, Bob, Amy, Bert, and Ann, with an evil relay in the center.]

Andrew Lewman andrew@torproject.org

Anonymity, Usability, and Humans. Pick Two.

16 May 2011 13 / 29
How is Tor different from other systems?
Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims
estimated 300k to 800k daily users
How many people use Tor daily?

Directly connecting users from all countries

The Tor Project - https://metrics.torproject.org/
Online and Offline change happens
...spring is in the air...
The text of this version is primarily taken from the first collected 1788 "McLean edition", but spelling and punctuation errors -- mainly printer's lapses -- have been corrected. The main heads have also been taken from that edition and are something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", so have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are those in the edition used a variety of special typographical symbols for superscripts, we use numerals. Editors's footnotes are in original typography used for emphasis, such as all caps or italics, has been used here. We have tried to identify the original newspapers were the Independent Journal [J], the New-York Packet [P], and the Daily Advertiser [A], all based in New York, actually first appeared May 28, 1788, in a bound volume published by J. and A. McLean, Federalist II. We have followed each paper to its primary author, James Madison [M], John Jay [J], or Alexander Hamilton [H], which is shown follow.
Anonymity, Usability, and Humans

- Allow the user to fully configure Tor rather than manually searching for and opening text files.
- Let users learn about the current state of their Tor connection, and configure or find out whether any of their applications are using it.
- Make alerts and error conditions visible to the user.
- Run on Windows, Linux, and OS X, on a normal consumer-level machine.
First iteration: command line

```bash
(0) (phobos@necrid:4) (0.00 0.04 0.00 1/165 17617) (~) (03:42:16)
--> /etc/init.d/tor start
```
Second iteration: GUI controller contest

News:
Jul 2006: Phase two is over, and brought us three fine interface projects for you who participated. The GUI competition is now ended — but don't let that stop you from exploring the Tor project!

Feb 2006: The first design phase is over, and we have two winners. The "Best Overall," and the April3rd team won "Most Aesthetically Pleasing Design".

Dec 2005: We're excited to have just added Edward Tufte and Bruce S. Marriott to our team! And don't forget the free Tor T-shirt for every submission!

Tor: GUI Competition Overview
Tor is a decentralized network of computers on the Internet that increases the privacy and security of other applications. We estimate there are some 200,000 Tor users currently communicating network status and security levels to the user.

The Tor project, affiliated with the Electronic Frontier Foundation, is running a GUI competition to develop a visual, secure, and anonymous browsing experience. Some of the challenges include how to make alerts and error conditions visible to the user, how to track and avoid certain routes or nodes; how to learn about the current state of a Tor connection, including which servers in the applications are using Tor safely.
This is the default view when user opens the Tor Control Panel for the first time. The text in the caption is used to explain how to get started with Tor. Once the user chooses to hide the caption text, this setting is remembered when Tor Control Panel is accessed again.
Time for a demo

Demonstration of Tor Browser Bundle
Experience so far

- Our web site is confusing to users and not technical enough for researchers.

Cultural differences and their expectations of software, usability, anonymity, privacy, and what Tor provides.

Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users. "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users. "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
- Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users. "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
- Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.
- Five years since we last dabbled in Usability.
Next steps

Visit https://www.torproject.org/ for more information, links, and ideas.
who uses tor?
http://www.flickr.com/photos/mattw/2336507468/siz, Matt Westervelt, CC-BY-SA.


spring is in the air, Paco Pomet, http://pacopomet.wordpress.com/