

Anonymity, Usability, and Humans. Pick Two.

Andrew Lewman
andrew@torproject.org

11 Jan 2012



What are we talking about?

- Crash course on anonymous communications
- Quick overview of Tor
- Usability, Security, and Humans

The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy



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

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

Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted

Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted

Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- I2P - Garlic routing, closed network, anonymity and reputation

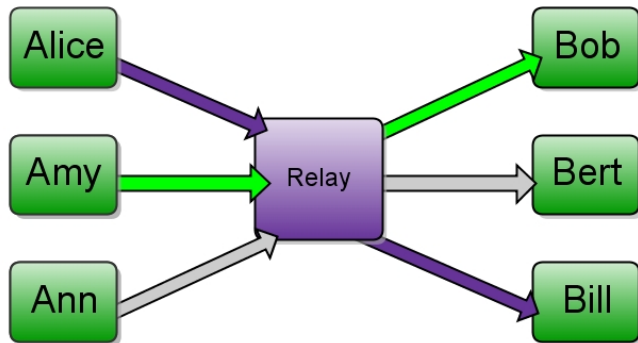
Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- I2P - Garlic routing, closed network, anonymity and reputation
- Freenet - closed network, anonymity, distributed file storage and sharing

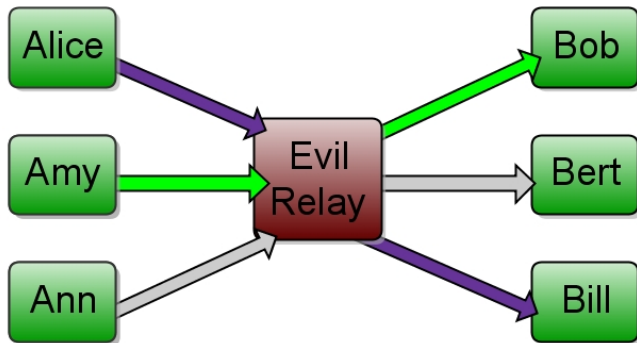
Other Systems

- VPN - Virtual Private Network, 1 to 1 connection, can redirect all traffic, generally encrypted
- Proxy - 1 to 1 connection, per application traffic redirection, sometimes encrypted
- I2P - Garlic routing, closed network, anonymity and reputation
- Freenet - closed network, anonymity, distributed file storage and sharing
- GNUnet - closed network, anonymity, distributed file storage and sharing

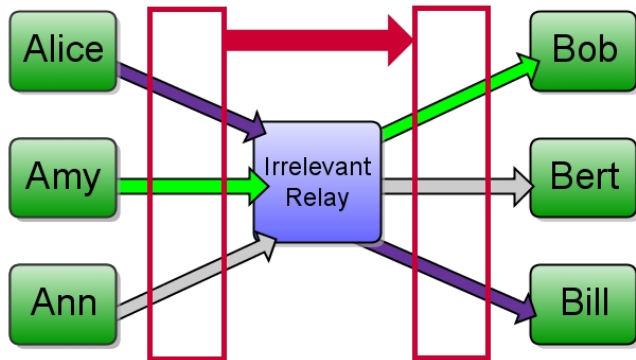
How is Tor different from other systems?



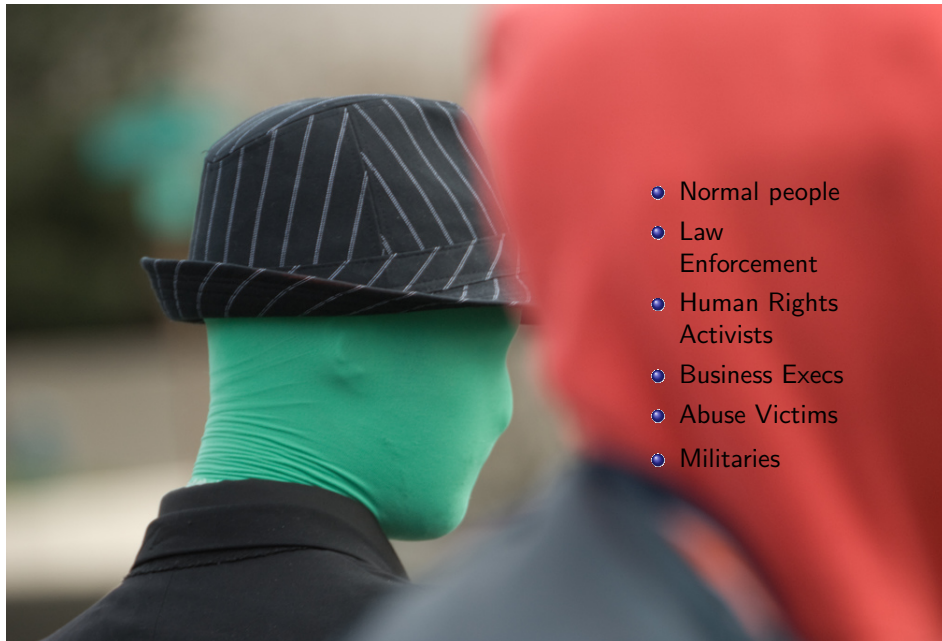
How is Tor different from other systems?



How is Tor different from other systems?



Who uses Tor?



- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Abuse Victims
- Militaries

Who uses Tor?

- *Normal users*

linking sensitive information to their current identities, online advertising networks, search engines, censorship circumvention

Who uses Tor?

- *Law enforcement*

accidental disclosure to targets, family and friend concerns, separating work from home life

Who uses Tor?

- *Rights Activists*

Personal safety, family safety, narrowly-defined publicity, censorship circumvention

Who uses Tor?

- *Business Execs*
separating work from home life, competitor research, censorship
circumvention

Who uses Tor?

- *Abuse Victims and Survivors*

complete separation of past abuse and current life, finding help and safety, need to help others anonymously

Who uses Tor?

- *Militaries*

intelligence gathering, separating work from home life, other activities

estimated 400k to 800k daily users



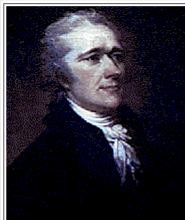
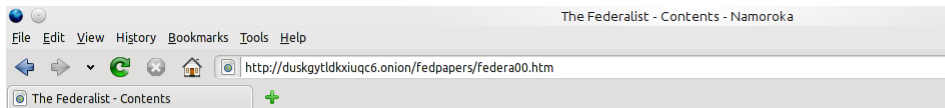
Online and Offline change happens



...spring is in the air...



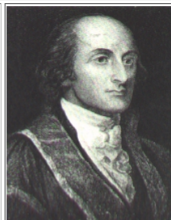
Tor hidden services



Alexander Hamilton



James Madison

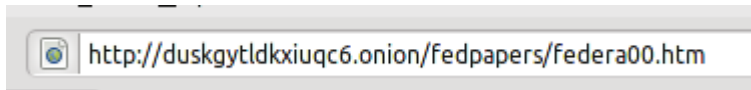


John Jay

The Federalist

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 something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", s have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are 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 newspapers were the *Independent Journal* [J], the *New-York Packet* [P], and the *Daily Advertiser* [A], all based in New York. The first 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

Tor hidden services



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, Android, iOS, on normal computers and phones.

First iteration: command line

```
(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



[Home](#) [Overview](#) [Download](#) [Docs](#) [Volunteer](#) [People](#) [Blog](#) [Donate!](#)

Tor GUI Competition

Overview & Goals

[What to Submit](#)

[How to Submit](#)

[Judging & Timeline](#)

[Technical Notes](#)

[Licensing](#)

[Wiki/FAQ](#)

News:

Jul 2006: Phase two is over, and brought us three fine interface projects from you who participated. The GUI competition is now ended — but don't let

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

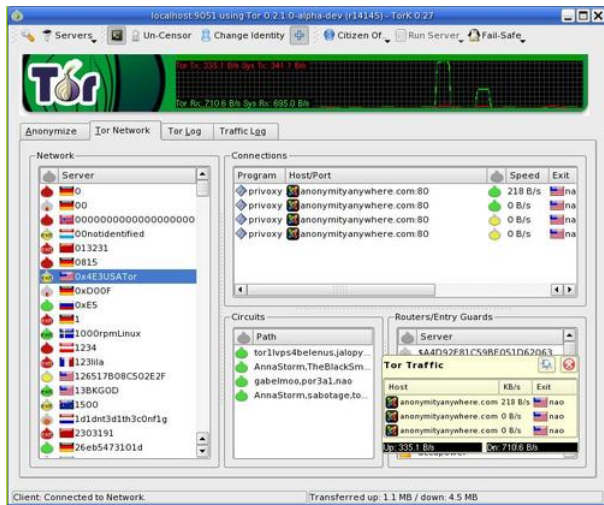
Dec 2005: We're excited to have just added [Edward Tufte and Bruce](#). don't forget the free [Tor T-shirt](#) for every submission!

Tor: GUI Competition Overview

Tor is a decentralized network of computers on the Internet that increases the security of other applications. We estimate there are some 200,000 Tor users currently

volunteer Tor servers on six continents. However, Tor's current user interface approach — running as a service — communicates 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 visually appealing and anonymous browsing experience. Some of the challenges include how to make alerts and error conditions visible or avoid certain routes or nodes; how to learn about the current state of a Tor connection, including which server 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.

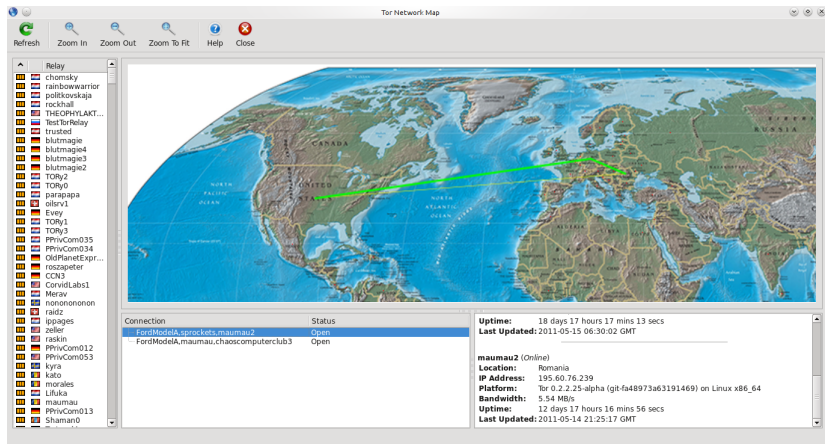
Caption-help includes diagrams and links to further help topics.

Getting Started with Tor

To create a [private network](#) pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through servers on the network.

The circuit is extended one [hop](#) at a time, and each server along the way knows only which server gave it data and which server it is giving data to. No individual server ever knows the complete path that a data packet has taken.

Name	Up Speed	Down Speed	# Onion Layers
News Crawler (version 1.8b)	2.34 kB/s	378 B/s	2
Internet Explorer (version 6.021.23)	1.50 kB/s	-- B/s	6
Mozilla Firefox (version 1.50 beta)	1.29 kB/s	23.29 kB/s	4
Gmail notifier	1010 B/s	0 B/s	4
Zonelabs Zonealarm Personal Firewall (version 6.00...)	234 B/s	4 B/s	8
ToDoList (version 4.5.2)	150 B/s	0 B/s	1
Picasa2 (version 2.0.1)	24 B/s	0 B/s	



Experience so far

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

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.
- Six years since we last dabbled in Usability.

Next steps

Visit <https://www.torproject.org/> for more information, links, and ideas.

Time for a demo

Demonstration of Tor Browser Bundle

Copyright

- who uses tor?
<http://www.flickr.com/photos/mattw/2336507468/siz>, Matt Westervelt, CC-BY-SA.
- 500k, <http://www.flickr.com/photos/lukaskracic/334850378/sizes/1/>, Luka Skracic, used with permission.
- spring is in the air, Paco Pomet, <http://pacopomet.wordpress.com/>