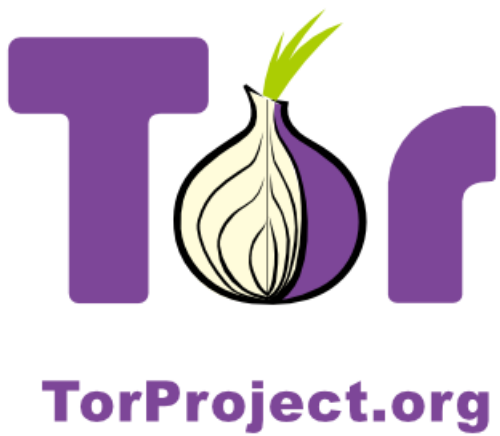
Free Software, Free Internet, Anonymity & Tor

Andrew Lewman
andrew@torproject.org

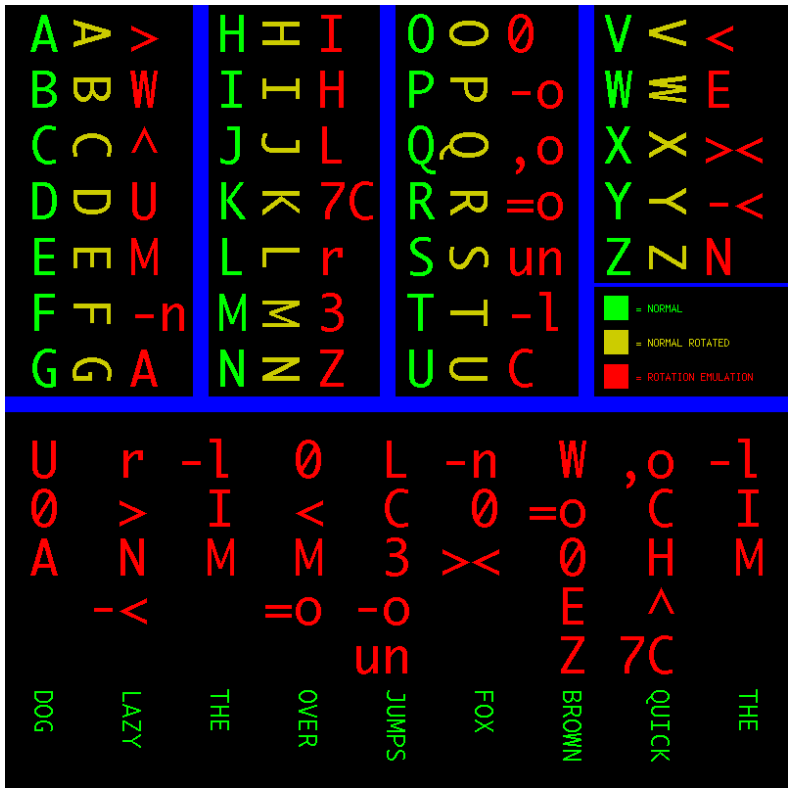
24 Feb 2011



What is anonymity?

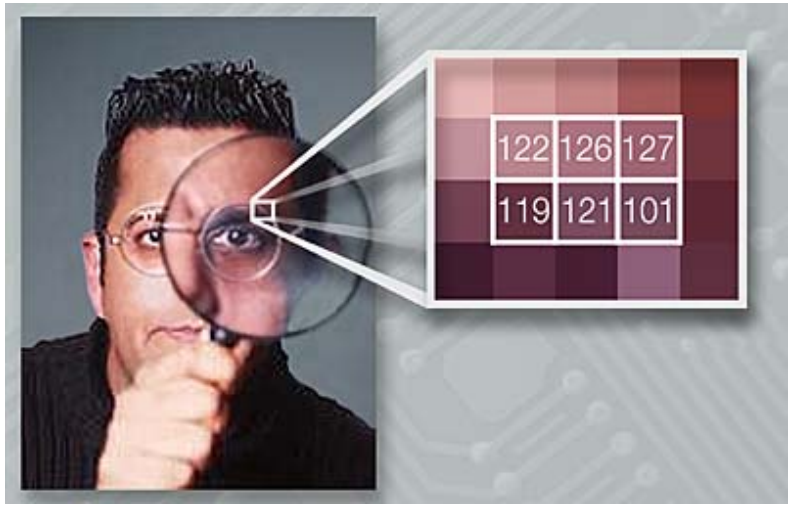
Anonymity isn't cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.
- This is the core of traffic analysis.



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.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?

..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.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?
- *"I didn't write my name on it!"* Not what we're talking about.

..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.
- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?
- *"I didn't write my name on it!"* Not what we're talking about.
- *"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 versus High-latency anonymous communication 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 generally more attractive to today's user

- 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 generally more attractive to today's user

- 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?)
    - And if anonymity loves company...

What is Tor?

- online anonymity, circumvention software and network
- open source, free software (BSD 3-clause & GPLv2 licenses)

What is Tor?

- online anonymity, circumvention software and network
- open source, free software (BSD 3-clause & GPLv2 licenses)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK,
  Bamberg Germany, Boston U, Harvard, MIT, RPI, GaTech

What is Tor?

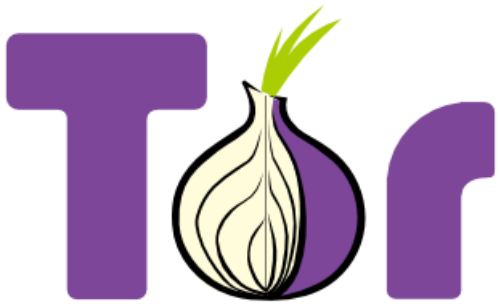
- online anonymity, circumvention software and network
- open source, free software (BSD 3-clause & GPLv2 licenses)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston U, Harvard, MIT, RPI, GaTech
- increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TAILS LiveCD/USB, Tor Weather, Tor auto-responder, Secure Updater, Orbot/Orlib, Tor Check, Arm, Nymble, Tor Control, Metrics, TorBEL, etc...

Who is The Tor Project, Inc?

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

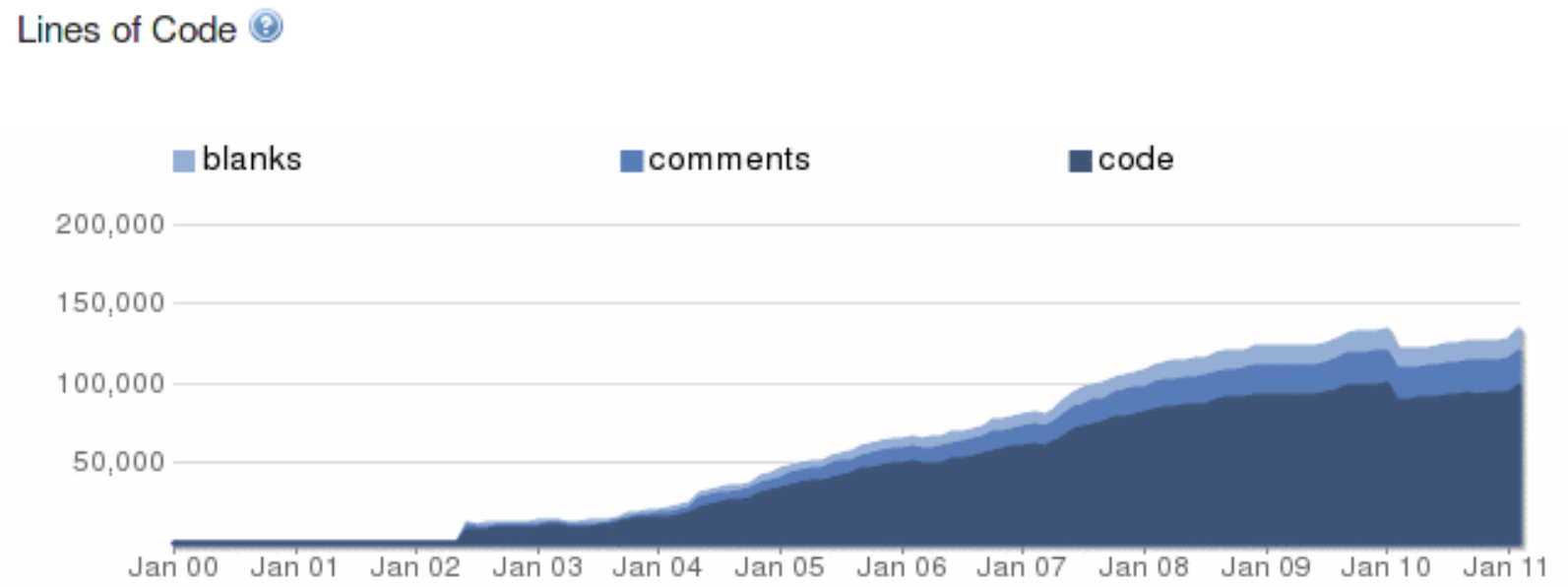
Tor is a low-latency anonymity system

- Based on technology developed in the Onion Routing project
- Privacy by design, not by policy (no data collected)
- Commonly used for web browsing and instant messaging (works for any TCP traffic)
- Originally built as a pure anonymity system (hides who is talking to whom)
- Now designed to resist censorship too (hides whether someone is using the system at all)
- Centralized directory authorities publish a list of all servers



TorProject.org

Tor code stats



stats from ohloh.net

Tor code stats

Lines of Code By Language

Language	Code Lines	Comment Lines	Comment Ratio	Blank Lines	Total Lines
C	92,733	18,830	16.9%	11,822	123,385
C++	1,811	1,893	51.1%	518	4,222
Autoconf	1,197	49	3.9%	168	1,414
shell script	1,127	505	30.9%	333	1,965
Python	570	168	22.8%	117	855
Automake	564	41	6.8%	96	701
Perl	401	78	16.3%	59	538
HTML	114	16	12.3%	18	148
Ruby	62	35	36.1%	18	115
Make	11	3	21.4%	3	17

This analysis was updated about 23 hours ago. (21 Feb 2011 23:28 UTC)

stats from ohloh.net

Tor hides communication patterns by relaying data through volunteer servers

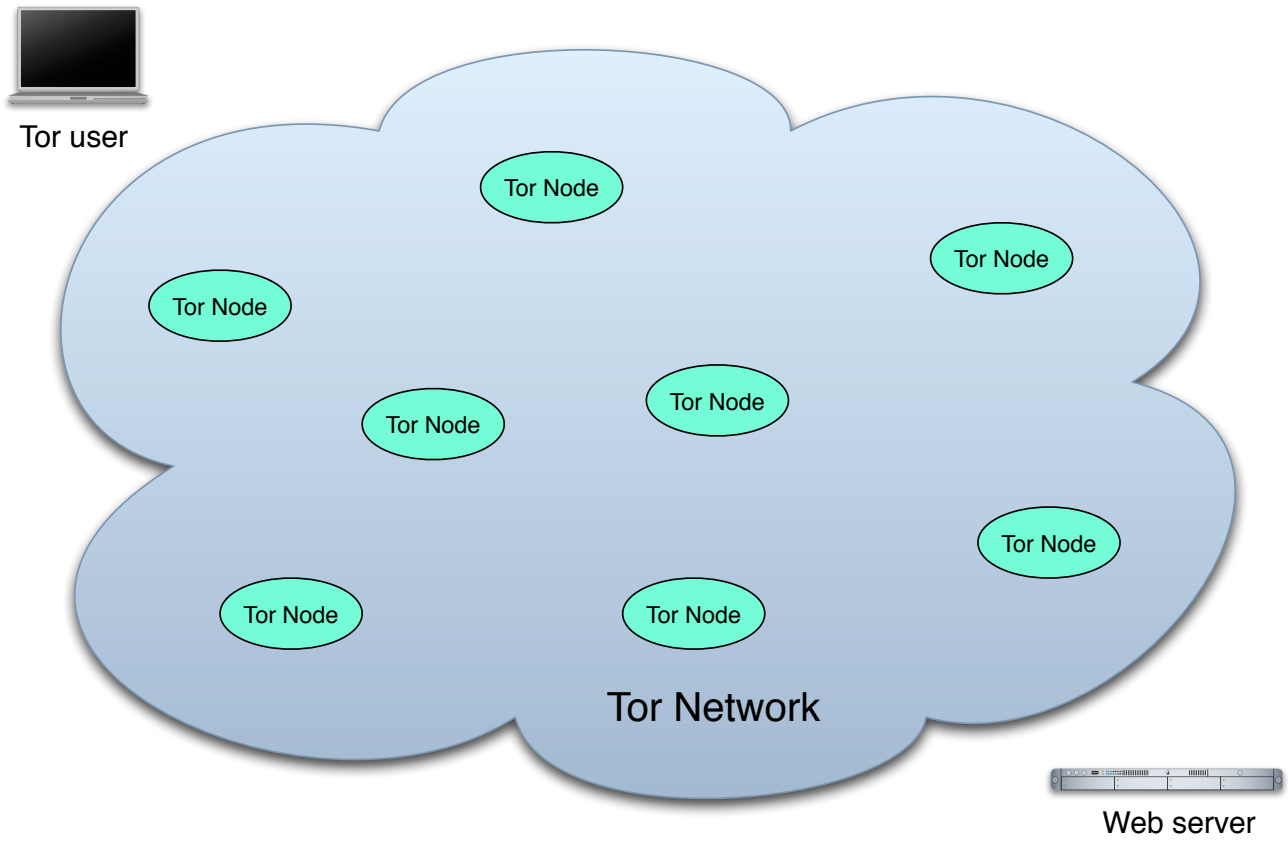


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

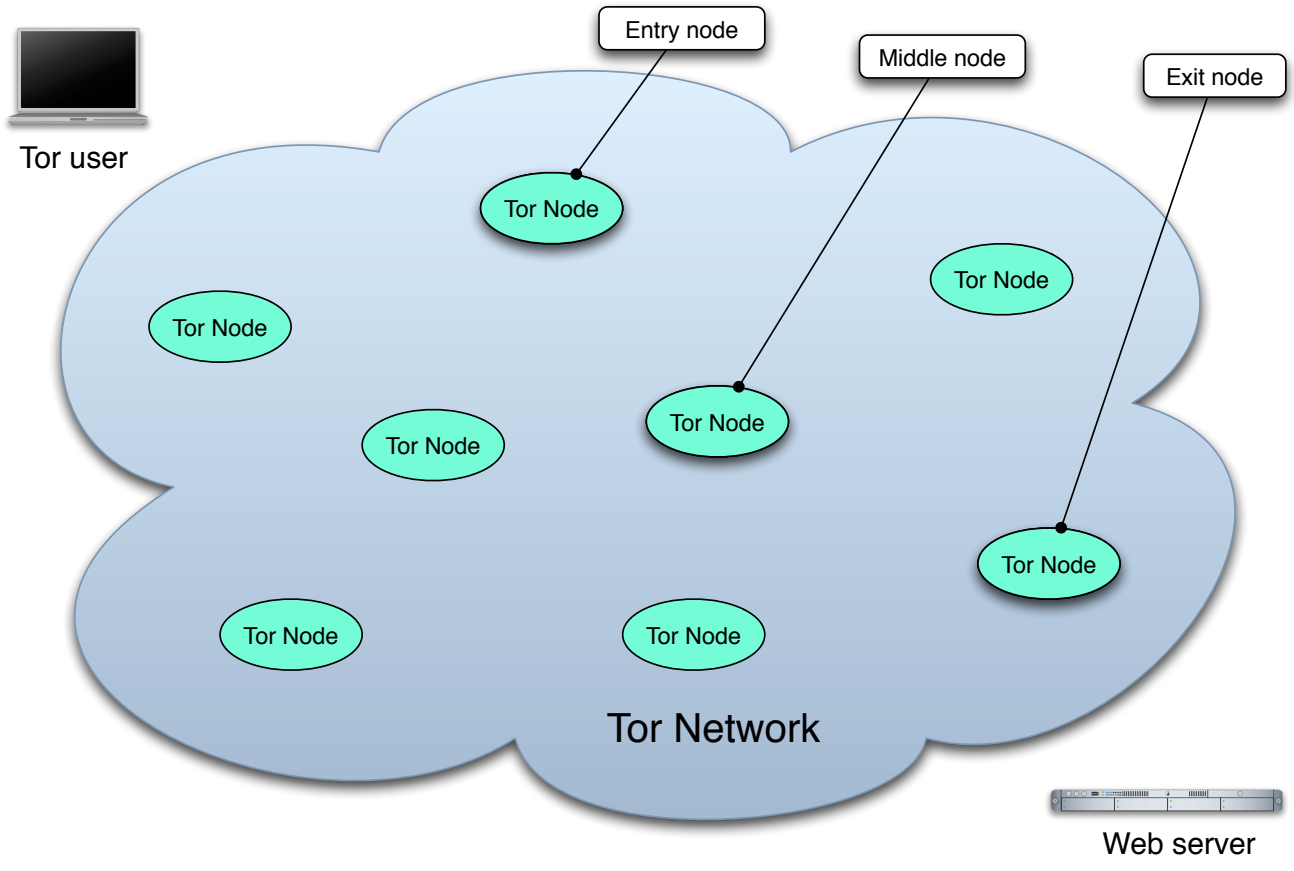


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

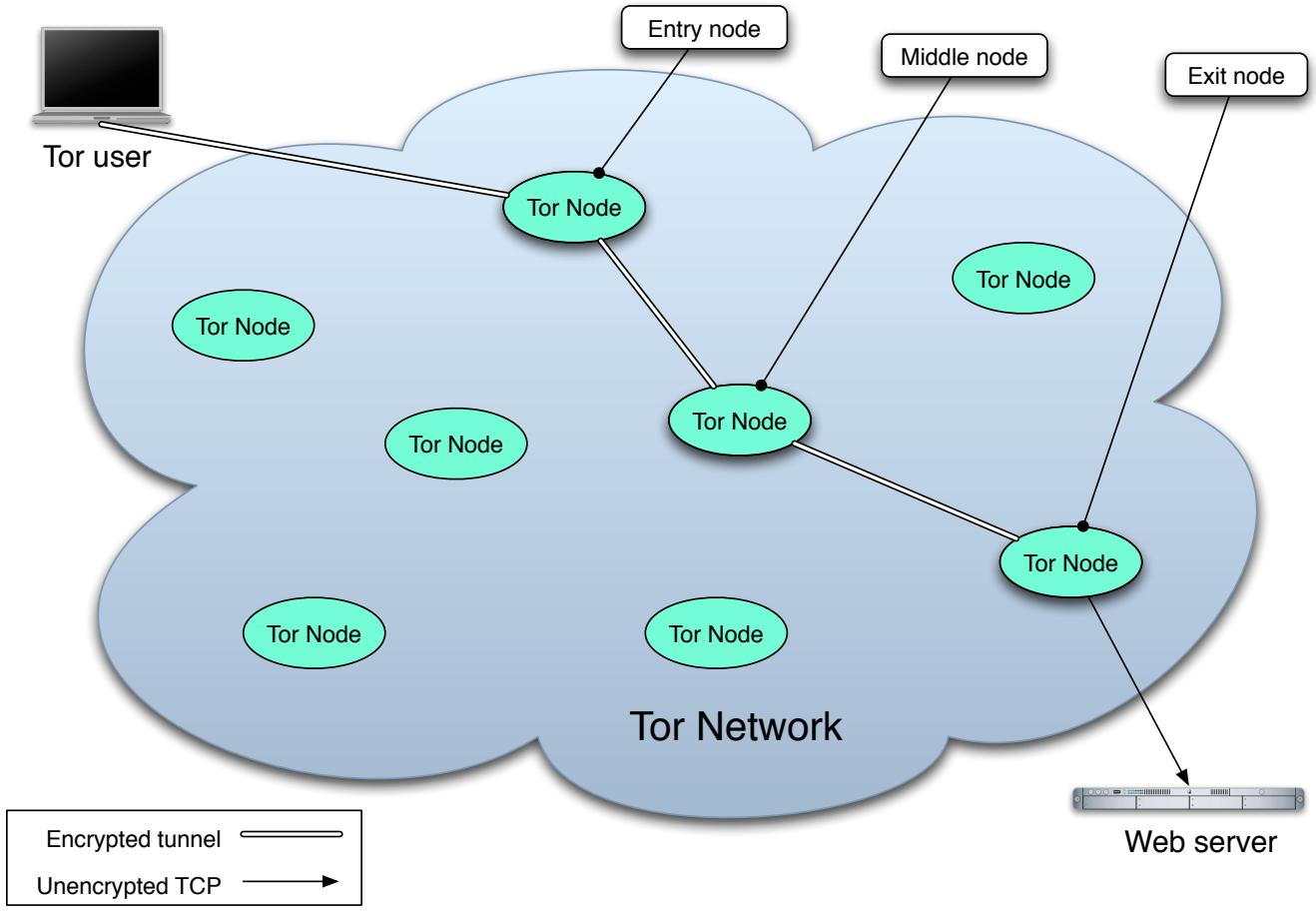


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

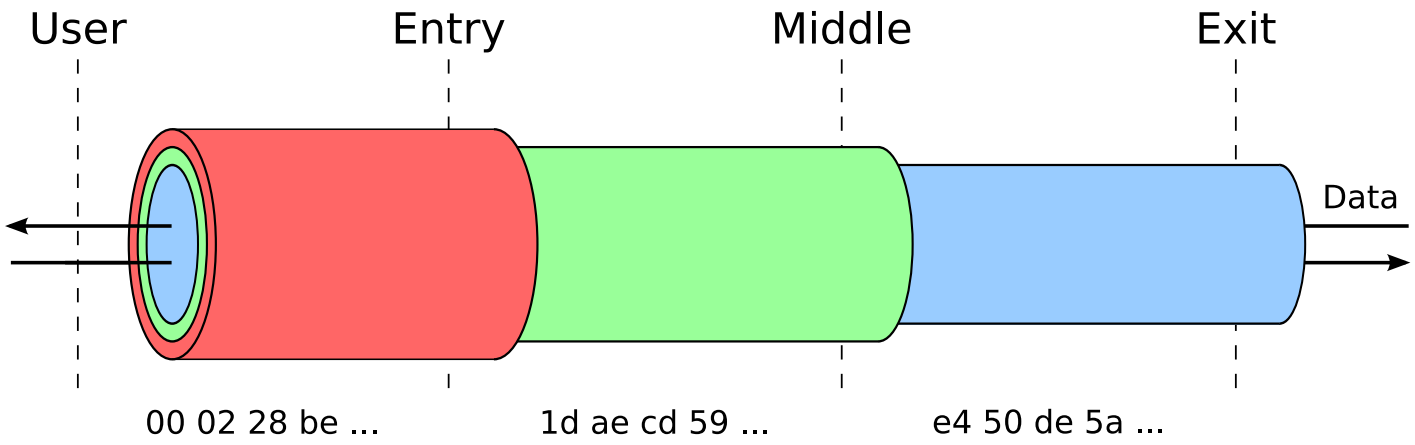
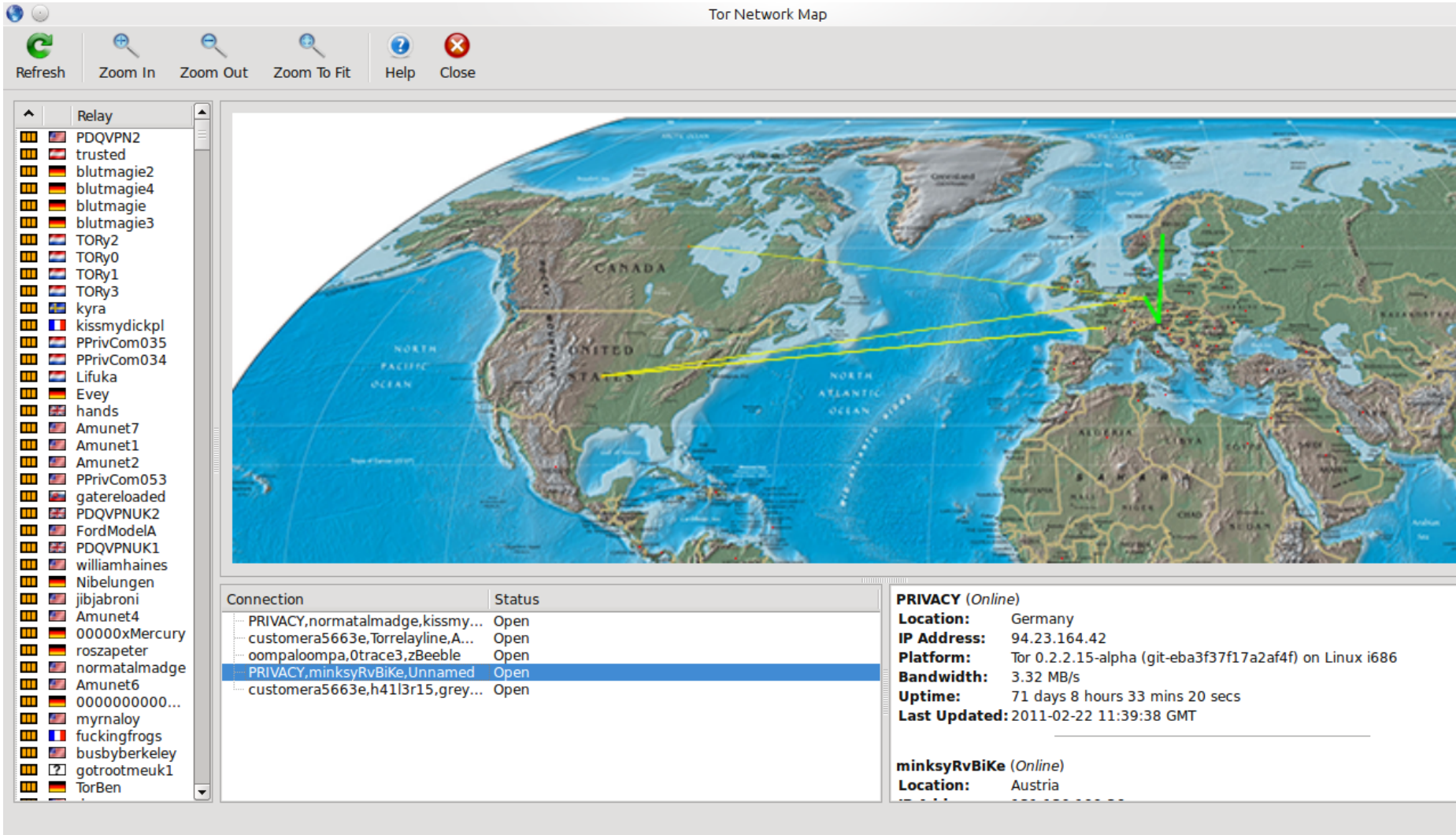


Diagram: Robert Watson

Vidalia Network Map



Measuring the Tor Network

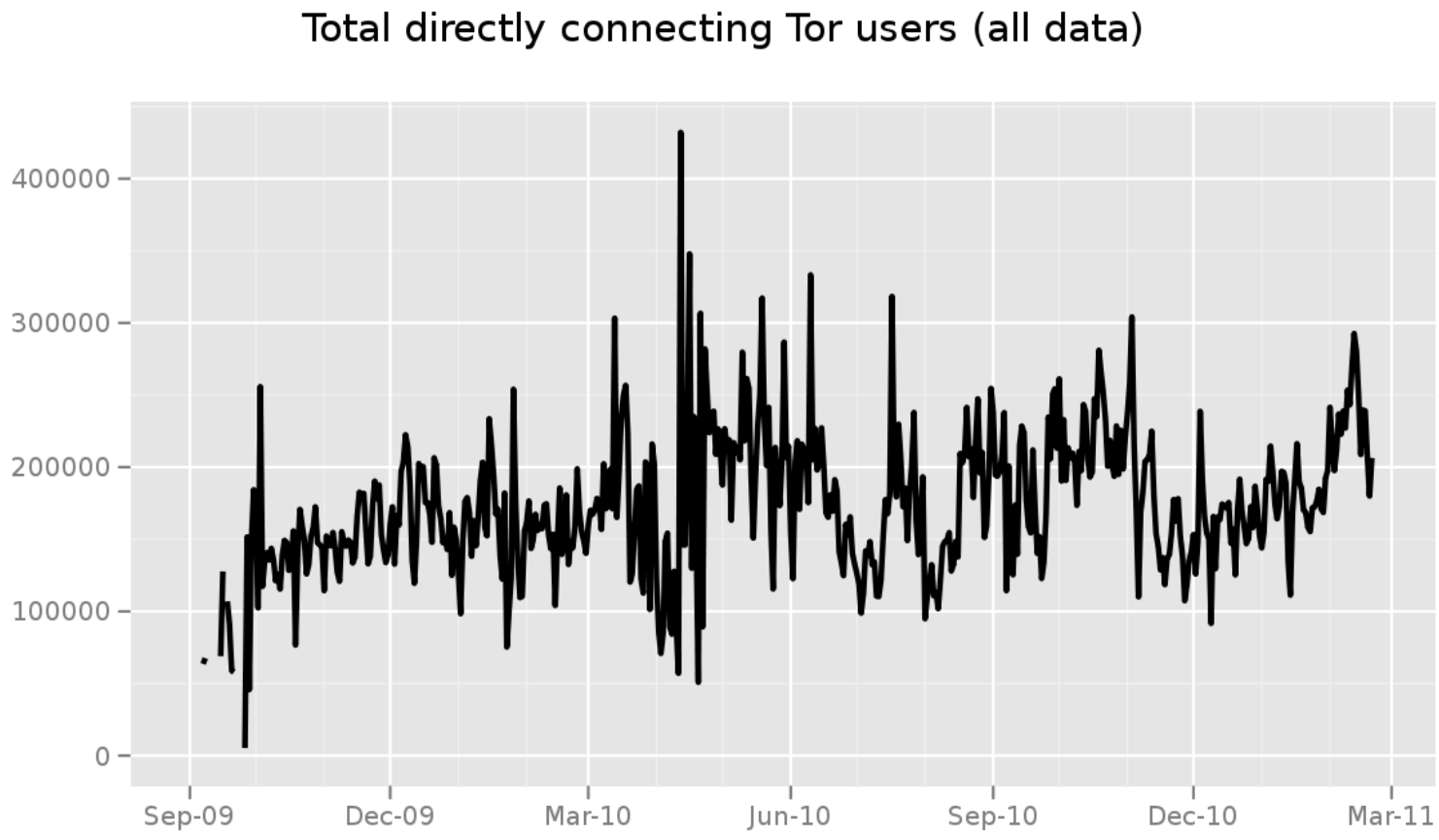
- Measuring metrics anonymously
- NSF grant to find out
- Archive of hourly consensus, ExoneraTor, VisiTor
- Metrics portal:
  `https://metrics.torproject.org/`

How many people use Tor?

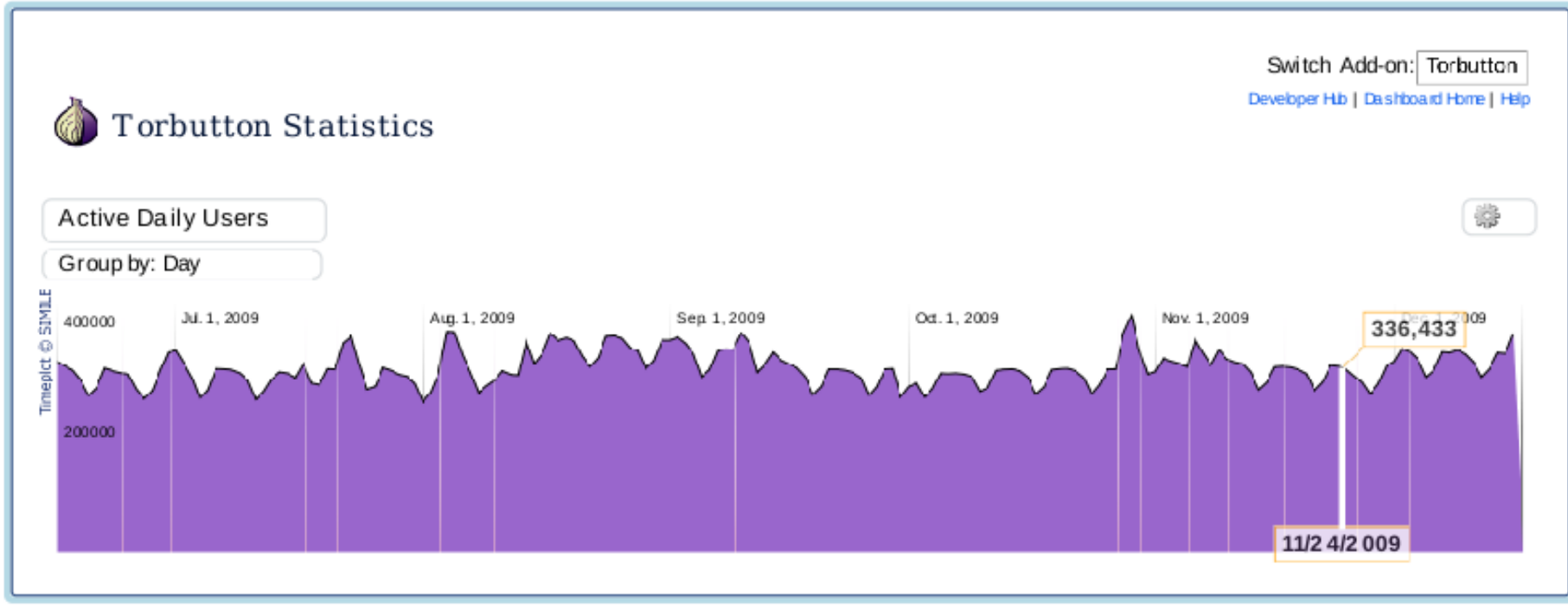
It's an anonymity system.

How many people use Tor?

It's an anonymity system.

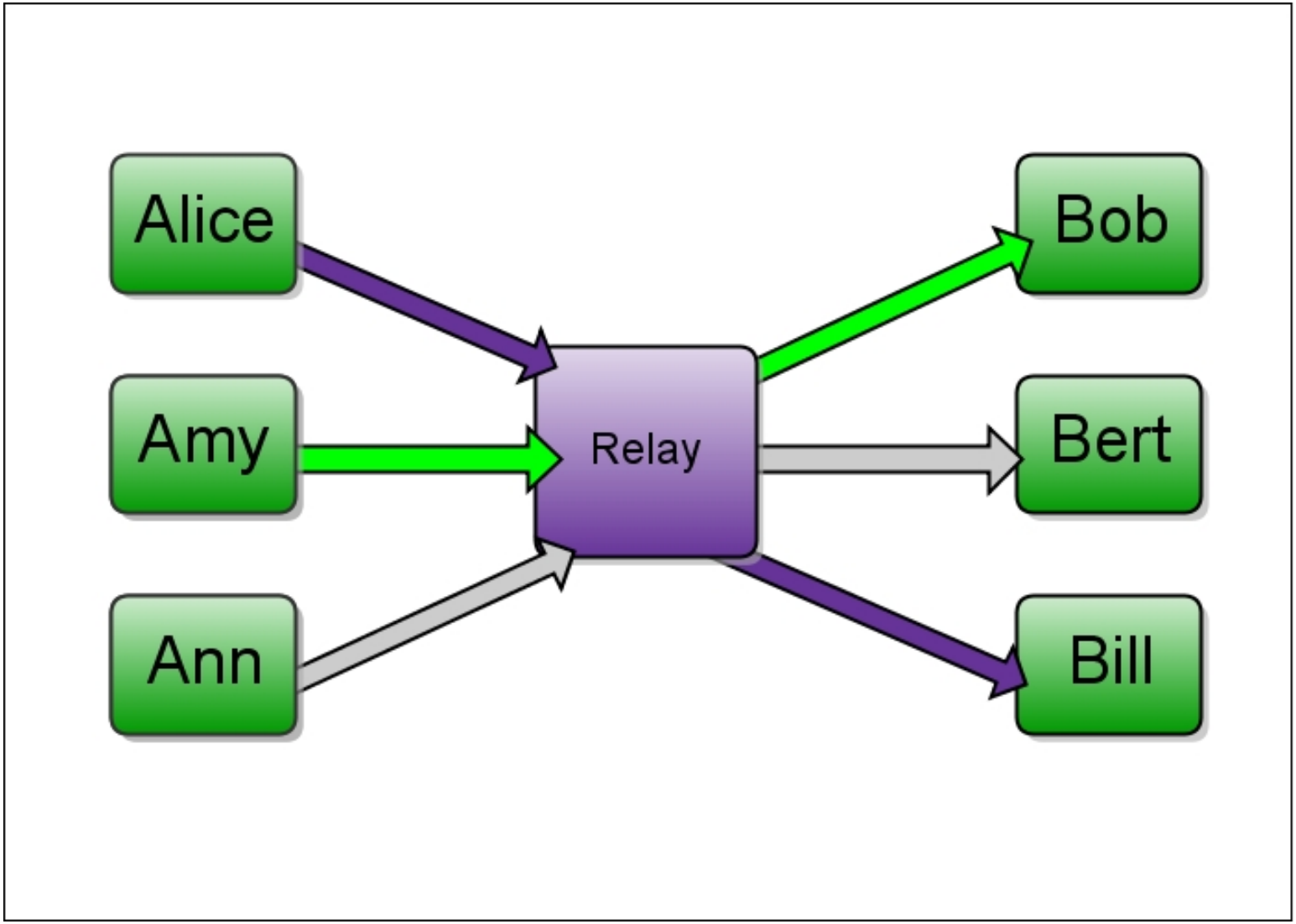


Seriously, how many people use Tor?

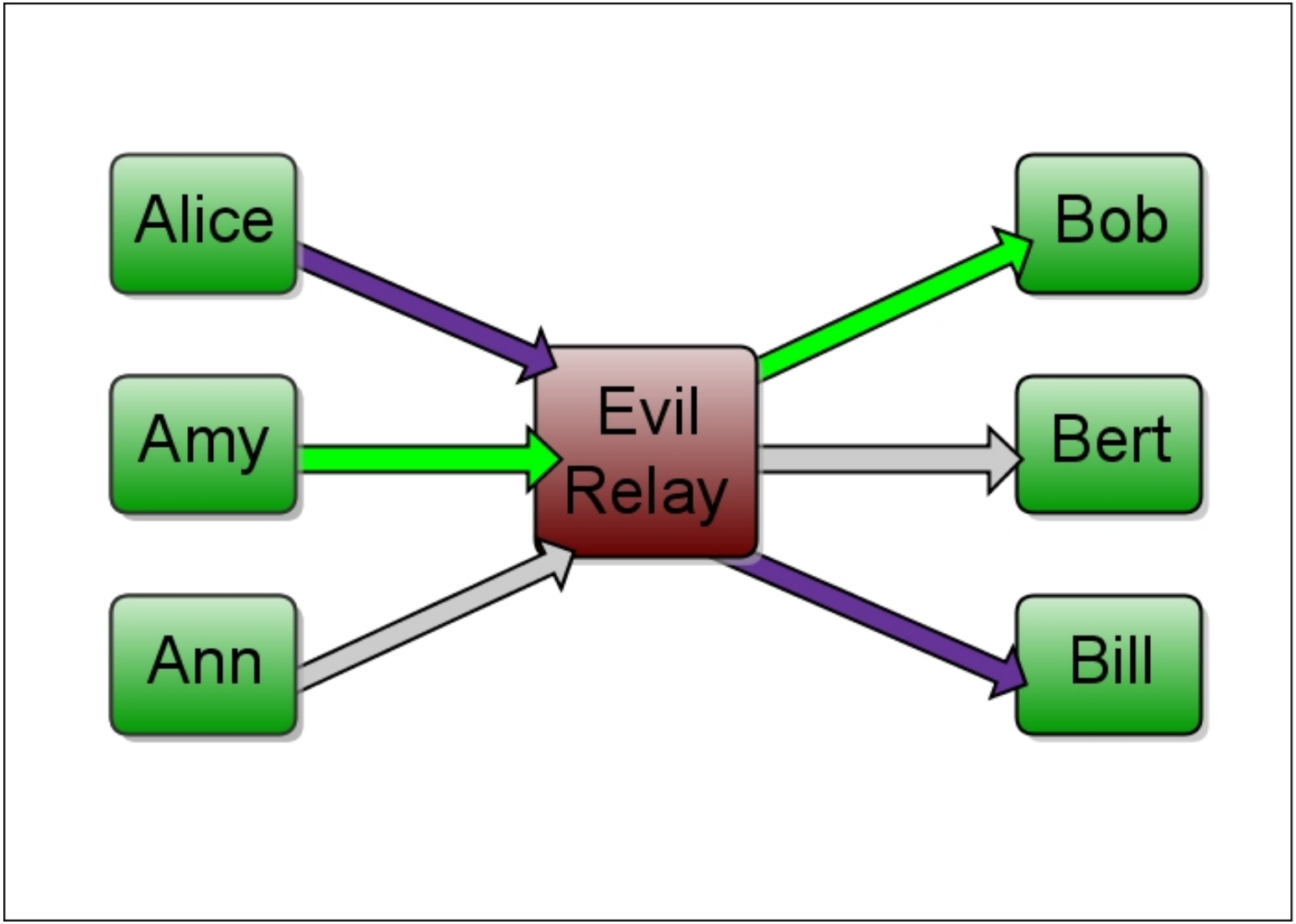


Total Downloads Since Mar. 23, 2006	**3,392,240**	**Active Daily Users** On Wednesday, Dec. 16	**403,079**
Last Day Count Wednesday, Dec. 16	2,720	Change from previous count 365,969 on Dec. 15	+10.14%
Average Daily Downloads	3,765	Average Daily Active Users	298,291
Downloads in the last 7 days	20,508	Average Daily Users this Week +0.63% from last week	360,676

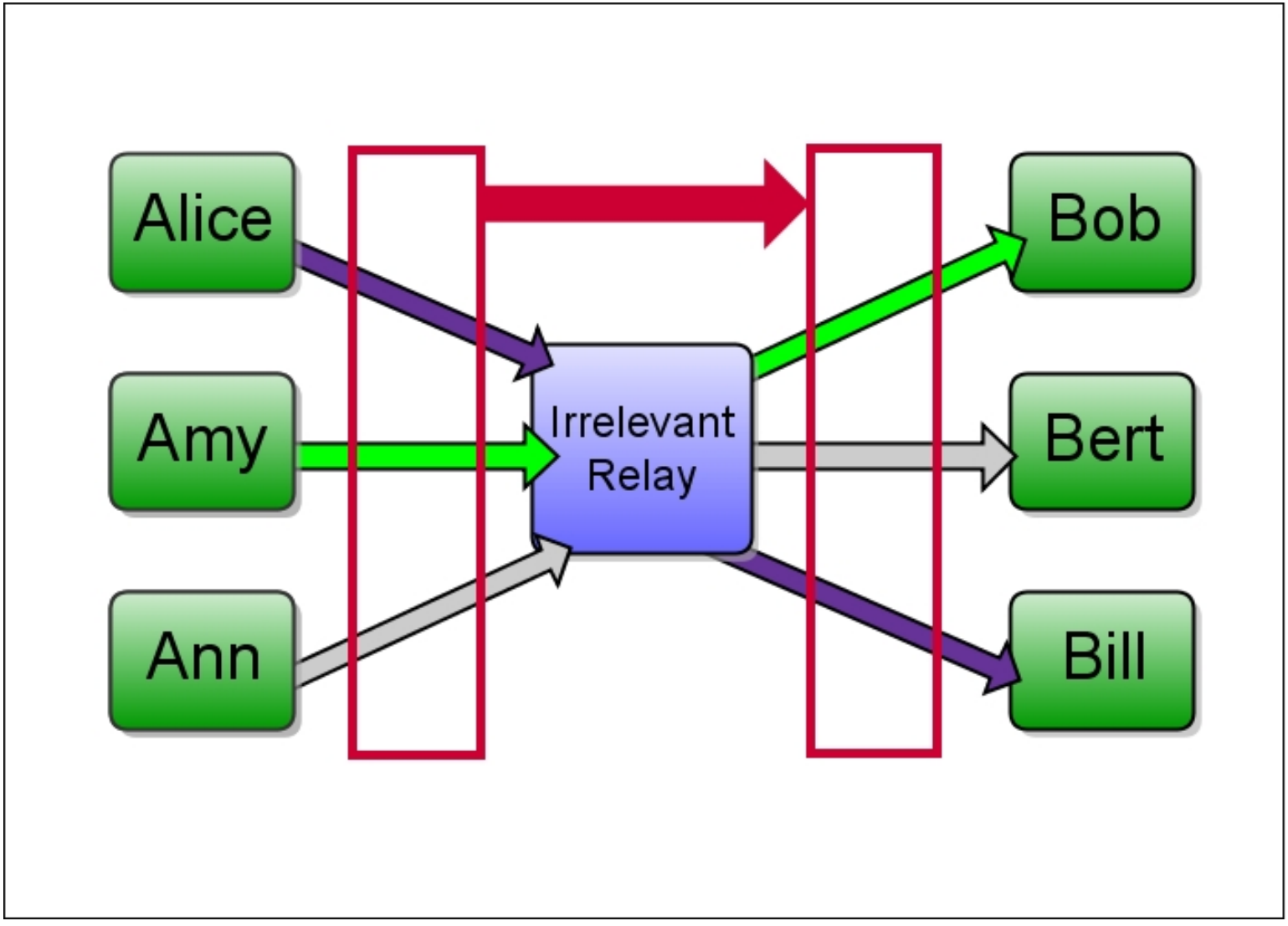
How is Tor different from other systems?



How is Tor different from other systems?



How is Tor different from other systems?



Hidden services allow privacy enhanced hosting

The Federalist - Contents - Namoroka

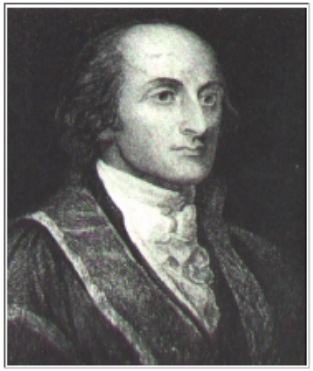
File Edit View History Bookmarks Tools Help

http://duskgytldkxiuqc6.onion/fedpapers/federa00.htm

The Federalist - Contents

Alexander Hamilton

James Madison



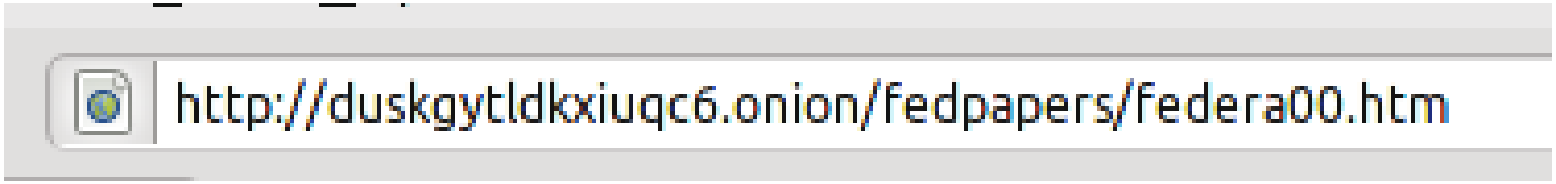
John Jay

The Federalist

The text of this version is primarily taken from the first collected 1788 "McLean edition", but spelling and punctuation have been moderni errors -- mainly printer's lapses -- have been corrected. The main heads have also been taken from that edition and a few later ones, excep something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", so that each document have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are those of the authors, exc edition used a variety of special typographical symbols for superscripts, we use numerals. Editors's footnotes are indicated by being prec original typography used for emphasis, such as all caps or italics, has been used here. We have tried to identify the date of earliest appea newspapers were the*Independent Journal* [**J**], the *New-York Packet* [**P**], and the *Daily Advertiser* [**A**], all based in New York, shown prece actually first appeared May 28, 1788, in a bound volume published by J. and A. McLean, *Federalist II*. We have followed the consensus of each paper to its primary author, James Madison [**M**], John Jay [**J**], or Alexander Hamilton [**H**], which is shown following the date. Please corrections to jon.roland@constitution.org.

Done

Did you catch that url?



Hidden services, in text

- Distributed Hash Table (DHT) Directory

Hidden services, in text

- Distributed Hash Table (DHT) Directory
- Rendezvous points

Hidden services, in text

- Distributed Hash Table (DHT) Directory
- Rendezvous points
- Anonymity for both the server and client

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my....

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?

Operating Systems leak info like a sieve

- Applications, network stacks, plugins, oh my.... some call this "sharing"
- Did you know Microsoft Word and OpenOffice Writer are browsers?
- `www.decloak.net` is a fine test

Mobile Operating Systems

- Entirely new set of challenges for something designed to know where you are at all times.
- Orbot: Tor on Android. `https://guardianproject.info/apps/`
- Tor on iphone, maemo/meego, symbian, etc
- Tor on Windows CE, `http://www.gsmk.de` as an example.
- Guardian Project, `https://guardianproject.info/`

How can coding help?

Name	Category	Language	Activity	Contributors
Tor	Core	C	Heavy	nickm, arma, Sebastian
*JTor	Core	Java	None	
TBB	Usability	Sys Admin	Moderate	Erinn
TAILS	Usability	Sys Admin	Heavy	#tails
Torsocks	Usability	C	Light	mwenge
*Torouter	Usability	Sys Admin	Light	ioerror, Runa
Vidalia	User Interface	C++, Qt	Light	chiiph
Arm	User Interface	Python, Curses	Heavy	atagar
Orbot	User Interface	Java	Light	n8fr8
Torbutton	Browser Add-on	Javascript	Moderate	mikeperry
*Thandy	Updater	Python	Light	Sebastian, Erinn, nickm
TorCtl	Library	Python	Light	mikeperry
Metrics	Client Service	Java	Heavy	karsten
TorStatus	Client Service	PHP	None	
Weather	Client Service	Python	Light	kaner
GetTor	Client Service	Python	None	kaner
TorCheck	Client Service	Python, Perl	None	
BridgeDB	Backend Service	Python	None	kaner, nickm
TorFlow	Backend Service	Python	None	mikeperry
*TorBEL	Backend Service	Python	None	Sebastian

* Project is still in an alpha state.

How to get involved?

https://torproject.org/volunteer

Supporters

Credits

- Thank you to Steven J. Murdoch, `http://www.cl.cam.ac.uk/users/sjm217/`, for the research and basis for the latter parts of the presentation.
- Photographer and Diagram credits as listed throughout the presentation.