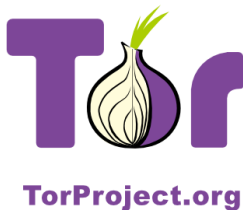


Understanding, Growing, & Extending Online Anonymity with Tor

Andrew Lewman
andrew@torproject.org

07 Feb 2010

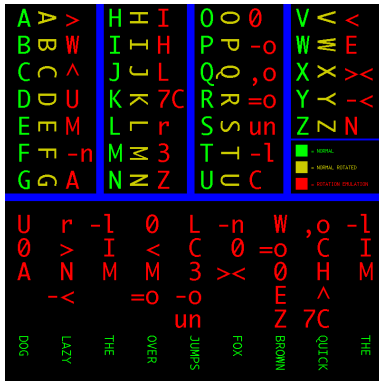


What is anonymity?



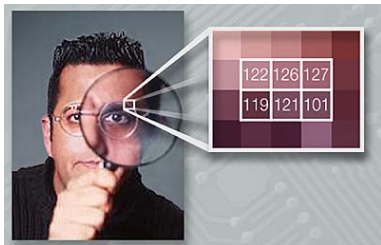
Anonymity isn't cryptography

- 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.

- "*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!

Who wants anonymity online?

- Ordinary people
 - To avoid personal information being sold to marketers
 - Protect themselves when researching sensitive topics
- Militaries and law enforcement
 - To carry out intelligence gathering
 - Protect undercover field agents
 - Offer anonymous tip lines
- Journalists
 - To protect sources, such as whistle blowers
- Human rights workers
 - To publicize abuses and protect themselves from surveillance
 - Blogging about controversial subjects
- Businesses
 - To observe their competition and build anonymous collaborations

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...

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

- 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

- 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, TorVM, Incognito
LiveCD, Tor Weather, Tor auto-responder, Secure Updater,
Orbot, TorFox, Torora, Portable Tor, Tor Check, Arm,
Nymble, Tor Control, Tor Wall

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

Lines of Code By Language

Language	Code Lines	Comment Lines	Comment Ratio	Blank Lines	Total Lines
C	78,718	16,125	17.0%	9,647	104,490
TeX/LaTeX	6,628	1,128	14.5%	1,181	8,937
HTML	4,105	16	0.4%	605	4,726
C++	3,110	1,768	36.2%	662	5,540
shell script	2,051	820	28.6%	507	3,378
XML	1,091	0	0.0%	3	1,094
Autoconf	696	26	3.6%	123	845
Python	673	169	20.1%	130	972
Perl	379	72	16.0%	53	504
Automake	242	30	11.0%	77	349
Make	143	46	24.3%	39	228
Ruby	62	35	36.1%	18	115
CSS	14	0	0.0%	0	14

Tor hides communication patterns by relaying data through volunteer servers

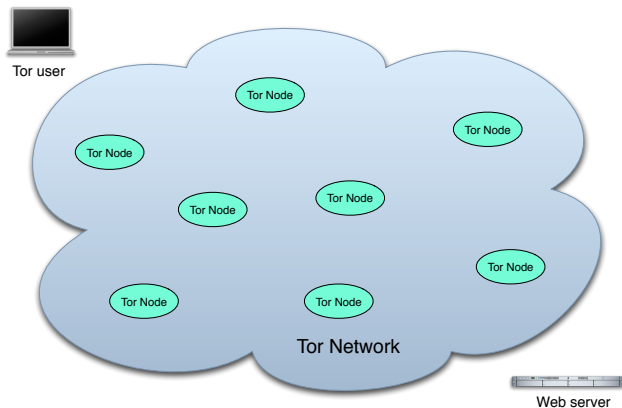


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

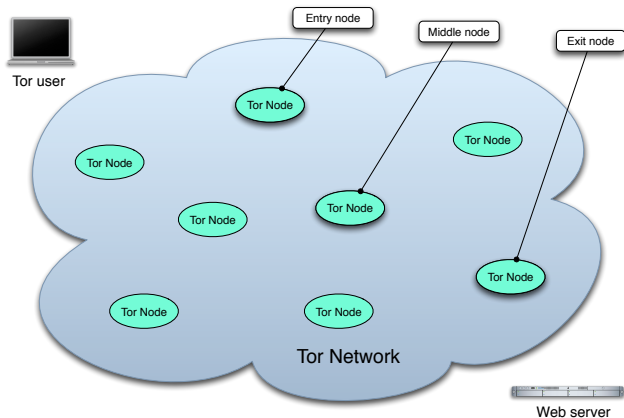


Diagram: Robert Watson

Tor hides communication patterns by relaying data through volunteer servers

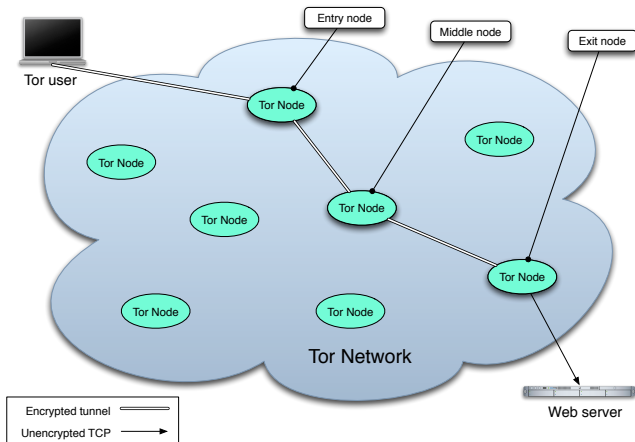


Diagram: Robert Watson

How many people use Tor?

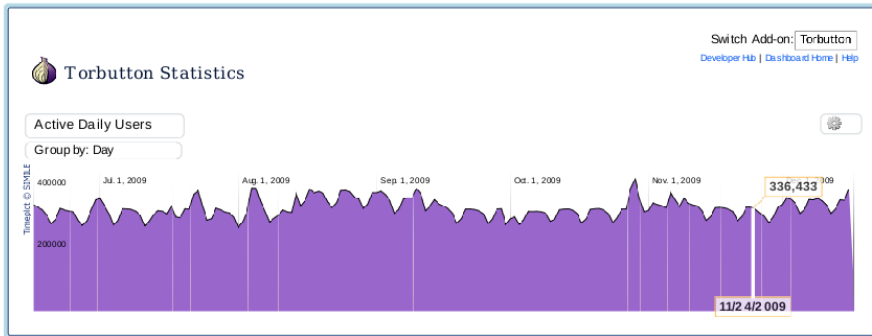
It's an anonymity system.

How many people use Tor?

It's an anonymity system.

<http://metrics.torproject.org/> for an idea.

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

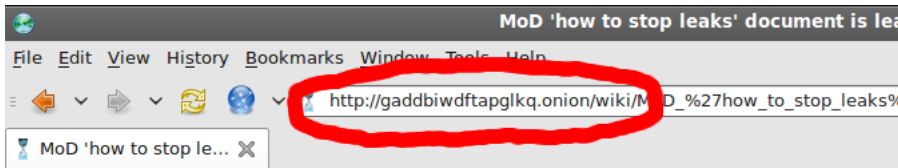
20,508

Average Daily Users this Week

+0.63% from last week

360,676

Tor hidden services allow privacy enhanced hosting of services



[article](#) [discuss](#) [view source](#) [history](#)

Keep us a strong and independent

[English](#) | [Español](#) | [Français](#) | [Deutsch](#) | [Português](#) | [Italiano](#) | [Català](#) | [Hrvatski](#) | [Nederlands](#) | [Dan](#)
[Latviešu](#) | [Eesti](#) | [Slovenčina](#) | [Lietuvių](#) | [Galego](#) | [Malti](#) | [العربية](#) | [לאדינו](#) | [Türkçe](#) | [EA](#)

MoD 'how to stop leaks' document is leaked

October 4, 2009

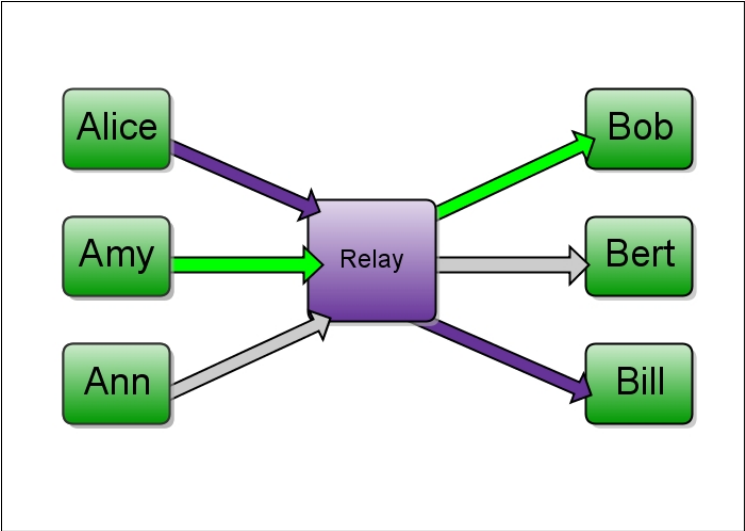
By **Tom Chivers** (*Telegraph*)[\[1\]](#) [✉](#)

The Defence Manual of Security is intended to help MoD, armed forces and intelligence agencies protect themselves from foreign spies and others.

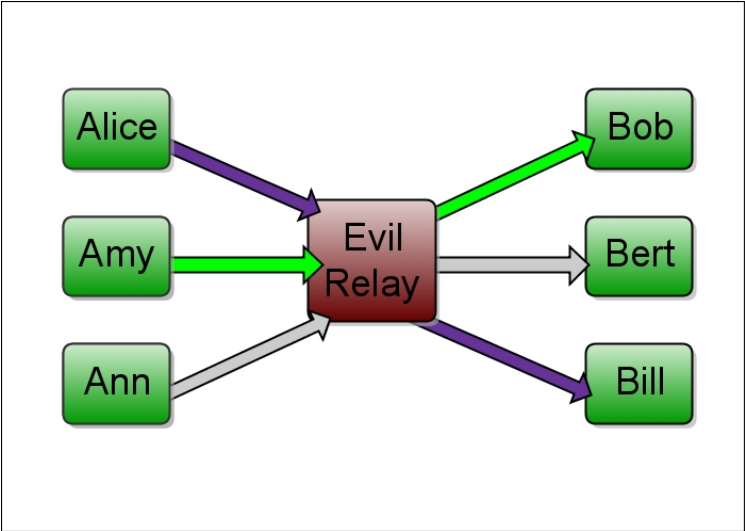
But the 2,400-page restricted document has found its way on to Wikileaks, a website that has become a hub for leaked documents, including governments, corporations and religions.

- [Main Page](#)
- [Main Page \(secure\)](#)

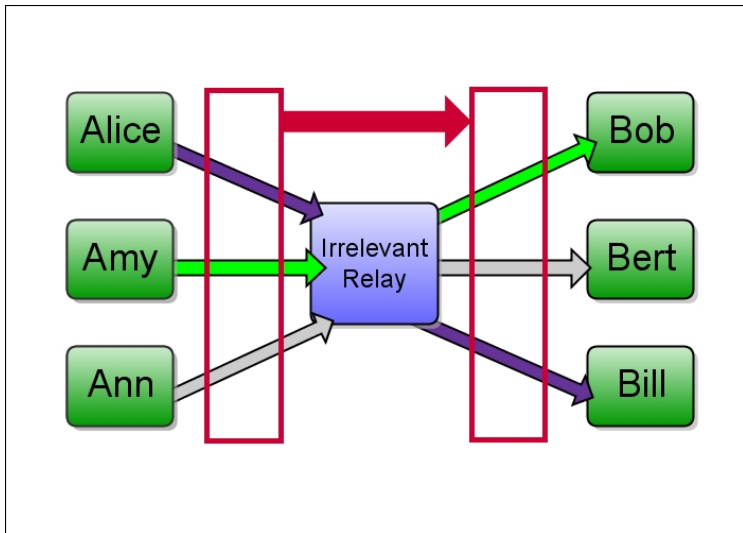
How is Tor different from other systems?



How is Tor different from other systems?



How is Tor different from other systems?



Universal Declaration of Human Rights

Article 19

“ *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

Article 20

“ *Everyone has the right to freedom of peaceful assembly and association.*

George Orwell was an optimist



Who controls the past, controls the future: who controls the present controls the past

— George Orwell, *Nineteen Eighty Four*, 1949

The re-writing of history is now much more efficient than when George Orwell imagined armies of Winston Smiths cutting holes in newspaper archives.



The Net interprets censorship as damage and routes around it.

— John Gilmore, 1993

No longer true on a technical level: censorship is in the routers.

Remains true on a social level: when material is censored, people distribute copies and draw attention to them

But what if people are too afraid to do this?

Internet surveillance is pervasive

- Conventional surveillance methods had to be targeted
- Internet censorship is capable of monitoring everyone, all of the time
- Governments are increasing monitoring: SORM (Russia), Golden Shield (China), Data Retention Directive (EU), and Interception Modernisation Programme (UK)
- 1 in 7 East German citizens worked for the Stasi. Today we can achieve the same results with a fraction of the cost



- Traffic data (who talks to whom, how often and for how long) is the core of intelligence capabilities
- This information is cheaper to record and store, compared to full content
- Because it can be easily processed by computer, data mining techniques can be used to understand social structures

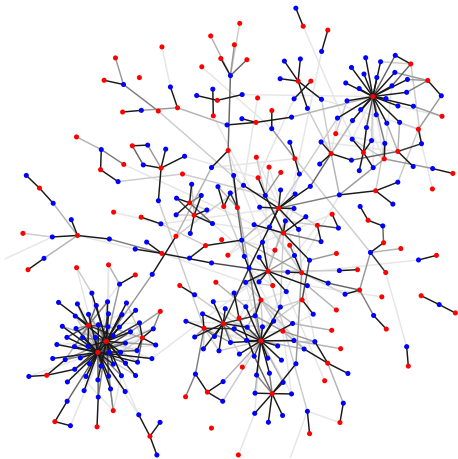


No government of any colour is to be trusted with such a roadmap to our souls

— Sir Ken Macdonald, former director of public prosecutions, on the UK Interception Modernisation Program

Importantly, information on social networks can be derived

- Communities
- People



From "The Economics of Mass Surveillance" by George Danezis and Bettina Wittneben



<https://torproject.org/volunteer>

- 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.