The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.
What is Tor?

Online anonymity 1) open source software, 2) network, 3) protocol
Community of researchers, developers, users, and relay operators
Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, NSF, US State Dept, SIDA, Knight Foundation, ...
The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
Estimated 2,000,000+ daily Tor users
Threat model: what can the attacker do?

Alice

Anonymity network

Bob

watch Alice!

Control part of the network!

watch (or be!) Bob!
Anonymity isn't encryption: Encryption just protects contents.
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?”
Anonymity serves different interests for different user groups.

“It's privacy!”
Anonymity serves different interests for different user groups.

“Anonymity”

[Diagram: Anonymity points to Businesses, Businesses says “It's network security!”]

“Private citizens”

“Anonymity”

“Private citizens” says “It's privacy!”
Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”

Governments

Anonymity

Private citizens

“It's privacy!”

Businesses

“It's network security!”
Anonymity serves different interests for different user groups.

- **Governments**: “It's traffic-analysis resistance!”
- **Private citizens**: “It's privacy!”
- **Human rights activists**: “It's reachability!”
- **Businesses**: “It's network security!”
Current situation: Bad people on the Internet are doing fine

Trojans
Viruses
Exploits

Botnets
Zombies

Espionage
DDoS
Extortion

Spam

Phishing
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a single relay (or eavesdropper!) is a single point of failure.
... or a single point of bypass.

Timing analysis bridges all connections through relay ⇒ An attractive fat target
So, add multiple relays so that no single one can betray Alice.
Alice makes a session key with R1
...And then tunnels to R2...and to R3
Tor's safety comes from diversity

• #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)

• #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!
There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
Orbot

Connected to the Tor network

Download
98.2kbps / 94.1KB

Upload
4.5kbps / 18.4KB
Tails LiveCD

The Amnesic Incognito Live System
Directly connecting users from Egypt

The Tor Project - https://metrics.torproject.org/
Attackers can block users from connecting to the Tor network

1) By blocking the directory authorities
2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services
3) By filtering based on Tor's network fingerprint
4) By preventing users from finding the Tor software (usually by blocking website)
Sorry, the requested page is unavailable.

If you believe the requested page should not be blocked please click here.

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa

Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE’s Internet Access Management Policy.

This site has been blocked

The web page you are trying to access has been blocked as the content contains prohibited materials.
Directly connecting users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
Pluggable transports
Pluggable transports

- Flashproxy (Stanford), websocket
- FTEProxy (Portland St), http via regex
- Stegotorus (SRI/CMU), http
- Skypemorph (Waterloo), Skype video
- uProxy (Google), webrtc
- Lantern (BNS), social network based
- ScrambleSuit (Karlstad), obfs-based
- Telex (Michigan/Waterloo), traffic divert
"Still the King of high secure, low latency Internet Anonymity"

Contenders for the throne:
- None
NSA targets the privacy-conscious
von J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge

One of NSA's German targets is 212.212.245.170. The string of numbers is an IP address assigned to Sebastian Hahn, a computer science student at the University of Erlangen. Hahn operates the server out of a grey high-security building a few kilometers from where he lives. Hahn, 28 years old and sporting a red beard, volunteers for the Tor Project in his free time. He is especially trusted by the Tor community, as his server is not just a node, it is a so-called Directory Authority. There are nine of these worldwide, and they are central to the Tor Network, as they contain an index of all Tor nodes. A user's traffic is automatically directed to one of the directory authorities to download the newest list of Tor relays generated each hour.

Hahn's predecessor named the server Gabelmoo, or Fork Man, the nickname of a local statue of Poseidon. After a look at the NSA source code, Hahn quickly found his predecessor listed in...
Only a piece of the puzzle

We hope the users aren't attacked by their hardware and software
No spyware installed, no cameras watching their screens, etc
Users can fetch a genuine copy of Tor?
Some open questions: how do we...

• Measure Tor's safety?
• Prevent censors from blocking Tor?
• Safely (and usefully) measure Tor?
• Learn the state of surveillance adversaries (and defeat them)
• Teach everybody about all these issues?