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.
• Online Anonymity
  - Open Source
  - Open Network

• Community of researchers, developers, users and relay operators.

• U.S. 501(c)(3) non-profit organization
Estimated 2,000,000+ daily Tor users
Threat model: what can the attacker do?

- Alice
  - watch Alice!
  - Anonymity network
  - Control part of the network!
  - Bob
  - watch (or be!) Bob!
Anonymity isn't encryption: Encryption just protects contents.
Anonymity serves different interests for different user groups.

“It's privacy!”

Anonymity

Private citizens
Anonymity serves different interests for different user groups.

“Anonymity”

Private citizens

“'It's privacy!'”

Businesses

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

“Anonymity”

Governments

Private citizens

Businesses

“It's traffic-analysis resistance!”

“It's network security!”

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

- **Governments**: “It's traffic-analysis resistance!”
- **Human rights activists**: “It's reachability!”
- **Businesses**: “It's network security!”
- **Private citizens**: “It's privacy!”

"It's privacy!"
The simplest designs use a single relay to hide connections.

(example: some commercial proxy providers)
But a central relay is a single point of failure.

Alice1 \(\rightarrow\) E(Bob3, “X”) \(\rightarrow\) Evil Relay

Alice2 \(\rightarrow\) E(Bob1, “Y”) \(\rightarrow\) Evil Relay

Alice3 \(\rightarrow\) E(Bob2, “Z”) \(\rightarrow\) Evil Relay

Evil Relay \(\rightarrow\) “Y” \(\rightarrow\) Bob1

Evil Relay \(\rightarrow\) “Z” \(\rightarrow\) Bob2

Evil Relay \(\rightarrow\) “X” \(\rightarrow\) Bob3
... 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
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 »
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.
Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction: privacy is about choice!
Pluggable transports
Pluggable transports

- Flashproxy (Stanford), websocket
- FTEProxy (Portland St), http via regex
- Stegotorus (SRI/CMU), http
- Skypemorph (Waterloo), Skype video
- uProxy (Google), webrtc
- ScrambleSuit (Karlstad), obfs-based
- Telex (Michigan/Waterloo), traffic divert
Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.
1 Million People use Facebook over Tor

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely - particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the "onion" domain name, and implemented Tor connectivity for our Android mobile app by enabling connections through Orbot.
World Map

Measurements
- More than 100,000
- More than 10,000
- Less than 10,000

Discoveries
- Confirmed censorship cases
- Vendors identified
“Still the King of high secure, low latency Internet Anonymity”

Contenders for the throne:
• None