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.

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
WHAT IS TOR?

- Online Anonymity
  - Open Source
  - Open Network

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

- U.S. 501(c)(3) non-profit organization

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Estimated 2,000,000+ daily Tor users

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
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.

Alice

“Hi, Bob!”

<gibberish>

attacker

Bob

“Hi, Bob!”
Anonymity serves different interests for different user groups.

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

- **Private citizens**: “It's privacy!”
- **Businesses**: “It's network security!”

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Anonymity serves different interests for different user groups.

"It's traffic-analysis resistance!"

Governments \[\rightarrow\] Anonymity \[\rightarrow\] Businesses

"It's network security!"

"It's privacy!"

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Anonymity serves different interests for different user groups.

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

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
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.
... or a single point of bypass.

Timing analysis bridges all connections through relay ⇒ An attractive fat target

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
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 »

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Total relay bandwidth

Advertised bandwidth
Bandwidth history

Bandwidth (Gbit/s)

The Tor Project - https://metrics.torproject.org/
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!
But what about bad people?

• Remember the millions of daily users.
• Still a two-edged sword?
• Good people need Tor much more than bad guys need it.
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Directly connecting users from Russia

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

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Directly connecting users from the Islamic Republic of Iran

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

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Pluggable transports

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
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

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
MESS WITH ONE OF US. 
MESS WITH ALL OF US.

Supporting totalitarian regimes is our business.
Sleep safe Assad, Blue Coat is here.
Directly connecting users from Kazakhstan

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

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Bridge users from Kazakhstan

The Tor Project - https://metrics.torproject.org/
I CAN HAZ FREEDOM?

TorProject.org
Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
“Still the King of high secure, low latency Internet Anonymity”

Contenders for the throne:
• None
Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Client registers its address using secure rendezvous

1. Client
2. Proxy polls
3. Facilitator responds with address
4. Proxy connects to client
5. Proxy connects to relay

Facilitator

Flash proxy (web browser)

Tor relay

Transport plugin

Transport plugin

to Tor

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Snowflake Options

This page enables you to use your web browser as a proxy to help other Internet users in censored places. When you click yes, your browser will act as a censorship circumvention proxy as long as you are viewing a page with the snowflake badge.

For more information on this system click here.

Do you want your browser to act as a proxy?

Yes  No

Snowflake Proxy is ACTIVE

Thank you for contributing to internet freedom!
Arms races

- Censorship arms race is bad
- Surveillance arms race is worse
  - And centralization of the Internet makes it worse still
Step 5: Bob connects to the Alice’s rendezvous point and provides her one-time secret.
Welcome to Riseup Black

This is the home of the Riseup "Black" services, our new enhanced security VPN and (soon) Encrypted Mail application.

Important: To avoid possible issues, you will need to create a new account (this means a new username) for Riseup Black services. But don't fear, you will be later able to use your current username if you want.

Download Bitmask

Log in to change your account settings or create support tickets for Riseup Black services.

Log in

Create a new user account for Riseup Black. For greater security, we strongly recommend you create your account via the Bitmask application instead. Remember: to avoid possible issues, you cannot use your current riseup.net username at this stage. But don't fear, you will be able to do it later.

Sign Up
Total relay bandwidth

- Advertised bandwidth
- Bandwidth history

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

Note: All slides are made public by the authors who created the slides. The slides may be downloaded for informational purposes only. The reproduction, reuse or reposting of these slides is expressly prohibited.
Total relay bandwidth

- Advertised bandwidth
- Bandwidth history

The Tor Project - https://metrics.torproject.org/
Onion-service traffic in Mbit/s

The Tor Project - https://metrics.torproject.org/
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.
Today, 30+ organizations use SecureDrop

https://securedrop.org/directory
Ricochet

Salut Korben !

ça fonctionne, c'est cool. A qui ai je l'honneur ?

Oui, c'est cool. Je suis un lecteur de ton site, Paul.

enchante !

j'ai commenté qu'une fois un article sur Mario64 porté sur plateforme x86
Tor isn't foolproof

- Opsec mistakes
- Browser metadata fingerprints
- Browser exploits
- Traffic analysis