The Tor Censorship Arms Race: The Next Chapter
- 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 to 8,000,000 daily Tor users
Threat model: what can the attacker do?

Alice

Anonymity network

Control part of the network!

Bob

watch Alice!

watch (or be!) Bob!
Anonymity isn't encryption: Encryption just protects contents.
Metadata

Data about data

"Metadata was traditionally in the card catalogs of libraries"
- Wikipedia

“We kill people based on metadata"
Anonymity serves different interests for different user groups.

“It's privacy!”

Private citizens
Anonymity serves different interests for different user groups.

Private citizens

“It's privacy!”

Anonymity

Businesses

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

“It's traffic-analysis resistance!”

Governments

Anonymity

Private citizens

“It's privacy!”

“It's network security!”

Businesses
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!”
How Tor Works: 2

Alice

Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.

Jane

Dave

Bob
Explore. Privately.

You're ready for the world's most private browsing experience.

Keep Tor strong. Donate Now »

Questions? Check our Tor Browser Manual »

Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »
Tails
the amnesic incognito live system
Explore Privately.

You're ready.

Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding will show you how.

START NOW

Travel a decentralized network.

Tor Browser connects you to the Tor network, a network of servers we call "relays," run by thousands of volunteers around the world. Unlike a VPN, there's no one point of failure or centralized entity you need to trust in order to...
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!
Tor censorship epochs

• Background / Phase 1 (2006-2011):
  Bridges, pluggable transports

• Phase 2 (2011-2019):
  Active probing, obfsproxy, domain
  fronting, many more countries

• Phase 3 (2019-?):
  Snowflake, obfs4, decoy routing, ...
Relay versus Discovery

There are two pieces to all these “proxying” schemes:

- a relay component: building circuits, sending traffic over them, getting the crypto right
- a discovery component: learning what relays are available
The basic Tor design uses a simple centralized directory protocol.

Relays publish self-signed descriptors.

Authorities publish a consensus list of all descriptors.

Alice downloads consensus and descriptors from anywhere.
Early blocking

• 2006: Thailand blocks our website by DNS
• 2007: Iran/Saudi Arabia/others use websense/smartfilter to block Tor’s http directory fetches.

The fix: put everything inside TLS.
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.

Access to this website is prohibited.

This site is blocked according to the government filtering policy. If you feel this page has been blocked in error, kindly fill out the form and we will investigate.

Thank You.
Iran throttles SSL (June 2009)

• We made Tor's TLS handshake look like Firefox+Apache.
• So when Iran freaked out and throttled SSL bandwidth by DPI in summer 2009, they got Tor for free
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)
How do you find a bridge?

1) [https://bridges.torproject.org/](https://bridges.torproject.org/) will tell you a few based on time and your IP address
2) Mail bridges@torproject.org from a gmail address and we'll send you a few
3) I mail some to a friend in Shanghai who distributes them via his social network
4) You can set up your own private bridge and tell your target users directly
Enter bridge information from a trusted source.

_type address:port (one per line)_
China (September 2009)

- China grabbed the list of public relays and blocked them
- They also enumerated+blocked one of the three bridge buckets (https://bridges.torproject.org/)
- But they missed the other bridge buckets.
Number of directory requests to directory mirror trusted

https://torproject.org

China
Chinese Tor users via bridges
China (March 2010)

• China enumerated the second of our three bridge buckets (the ones available at bridges@torproject.org via Gmail)

• We were down to the social network distribution strategy, and the private bridges
Iran (January 2011)

- Iran blocked Tor by DPI for SSL and filtering our Diffie-Hellman parameter.
- Socks proxy worked fine the whole time (the DPI didn't pick it up)
- DH p is a server-side parameter, so the relays and bridges had to upgrade, but not the clients
Directly connecting users from Egypt

The Tor Project - https://metrics.torproject.org/
Iran (September 2011)

- This time, DPI for SSL and look at our TLS certificate lifetime.
- (Tor rotated its TLS certificates every 2 hours, because key rotation is good, right?)
- Now our certificates last for a year
- These are all low-hanging fruit. Kind of a weird arms race.
Directly connecting users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
MESS WITH ONE OF US.
MESS WITH ALL OF US.

Supporting totalitarian regimes is our business. Sleep safe Assad, Blue Coat is here.
Tunisia (October 2011)

• First country to announce officially that they censor
• Using Smartfilter
• Outsourced to a foreign corporation
• And Tunisia got a discount!
Pluggable transports

![Diagram showing pluggable transports with obfsproxy client, CENSOR, obfsproxy server, Tor Client, and Tor Bridge]
The two currently successful PTs

- obfsproxy (2012): add a layer of encryption on top so there are no recognizable headers.
- meek (2014): “domain fronting” via Google, Azure, Amazon
Tor censorship epochs

- **Background / Phase 1 (2006-2011):**
  Bridges, pluggable transports

- **Phase 2 (2011-2019):**
  Active probing, obfsproxy, domain fronting, many more countries

- **Phase 3 (2019-?):**
  Snowflake, obfs4, decoy routing, ...
China (October 2011)

• Started its active probing campaign by DPIing on Tor’s TLS handshake, and later on obfs2 and obfs3
• Spoofed IP addresses from inside China
• The fix: obfs4 requires the client to prove knowledge of a secret, else it won’t admit to being an obfs4 bridge.
Directly connecting users from Ethiopia

The Tor Project - https://metrics.torproject.org/
China (March 2015)

- “Great Cannon” targets github
- Greatfire declaring war, “you can’t block us”
- Huge difference from previous “let them save face” approach
China (pre 2018)

• China also shifted to blackholing the entire IP address (not just the offending port).

• *Any* old probers are enough to get bridges blocked (0.2.9, ORPort, etc)
China (mid 2018)

• Lantern uses obfs4 proxies for its own circumvention tool

• After a while, the proxies they give their users don’t work so well.

^ another example of tough feedback loop
China (mid 2019)

- 0.3.2 Tor clients, talking to 0.3.5 Tor bridges, don’t trigger active probing anymore.
- We guess it has to do with changes in advertised ciphersuites on the client side.
Dozens of US spies killed after Iran and China uncovered CIA messaging service using Google
I CAN HAZ FREEDOM?
Tor censorship epochs

• **Background / Phase 1 (2006-2011):** Bridges, pluggable transports

• **Phase 2 (2011-2019):** Active probing, obfsproxy, domain fronting, many more countries

• **Phase 3 (2019-?):** Snowflake, obfs4, decoy routing, ...
New pluggable transport: Snowflake
1 client connected.

Your snowflake has helped 1 user circumvent censorship in the last 24 hours.

Turn Off

Learn more
What do the icons mean?

**Working:** if your status is light blue or dark blue, your proxy is running.

- A plain pink cupcake means the proxy is running but no one is using it right now.

- A happy cupcake means someone is using your proxy right now. Neat!

**Not working:** if your status is grey or black, there was a problem and your proxy is not running. Usually this is due to internet connection problems or firewall settings.

- A sad grey cupcake means that the badge has disabled itself. Try restarting your browser.
Streamlined obfs4 deployment

- https://community.torproject.org/relay/setup/bridge
- The future: “apt install tor-servers”?
BridgeDB needs a feedback cycle

- Measure how much use each bridge sees
- Measure bridge blocking
- Then adapt bridge distribution to favor efficient distribution channels
- Need to invent new distribution channels, eg Salmon from PETS 2015
Measuring bridge reachability

- Passive: bridges track incoming connections by country; clients self-report blockage (via some other bridge)
- Active: scan bridges from within the country; or measure remotely via indirect scanning
- Bridges test for duplex blocking
ooni.torproject.org
Other upcoming designs

- FTE/Marionette: transform traffic payloads according to a regexp or a state machine
- Decoy routing: run a tap at an ISP, look for steganographic tags, inject responses from the middle
Arms races

- Censorship arms race is bad
- Surveillance arms race is worse
  - And centralization of the Internet makes it worse still
How can you help?

• Run an obfs4 bridge, be a Snowflake
• Teach your friends about Tor, and privacy in general
• Help find – and fix – bugs
• Work on open research problems (petsymposium.org)
• donate.torproject.org