Tor and censorship circumvention

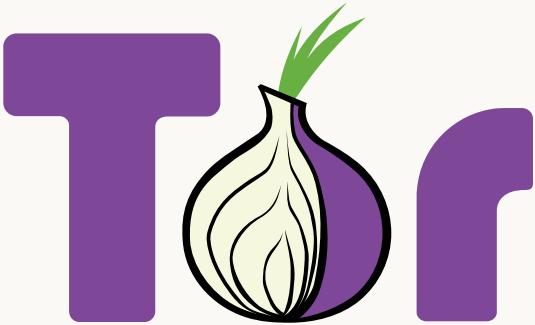
2024-03-14

Linus Nordberg, Glasklar Teknik AB

Outline

1. Tor crash course
2. Censorship circumvention
3. Wrap up

Who has heard of Tor?



Tor from a user perspective

A less insecure version of the web

(onion services)

Tor from a user perspective

A less insecure version of the web (onion services)
Consensual authentication (anonymous internet access)

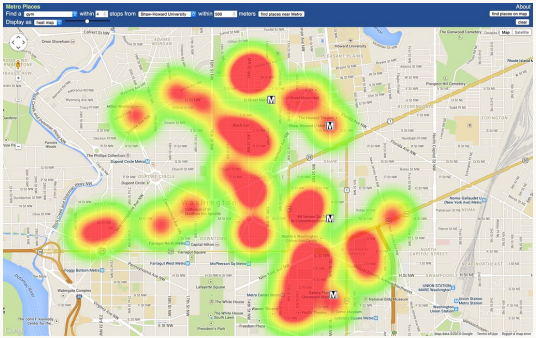
Tor from a user perspective

A less insecure version of the web (onion services)
Consensual authentication (anonymous internet access)
Internet access (censorship resistance)

Protecting communications metadata

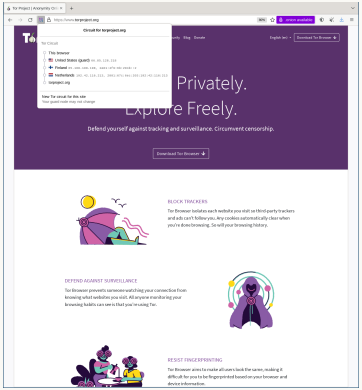
IPv4 Packet Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Version / IHL	DSCP / ECN	Total Length	
32	Identification		Flags	Fragment Offset
64	Time to Live	Protocol	Header Checksum	
96	Source IP Address			
128	Destination IP Address			
160	Options (if IHL > 5)			

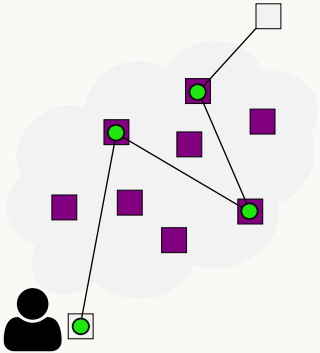


Metadata is data about data

Tor Project provides two things

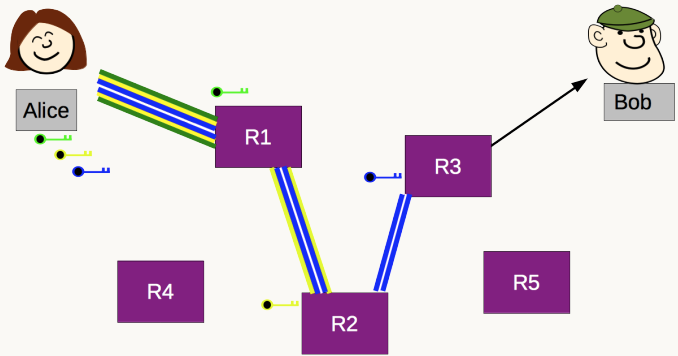


A web browser



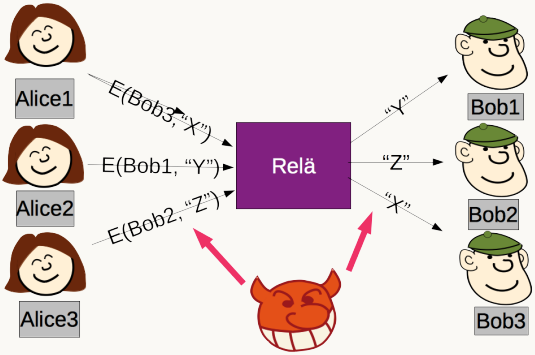
An overlay TCP network

Protection on the network layer



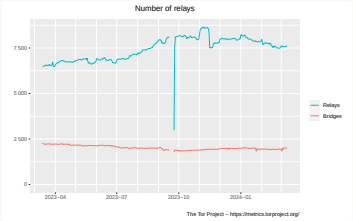
A three-hop proxy, aka Onion routing

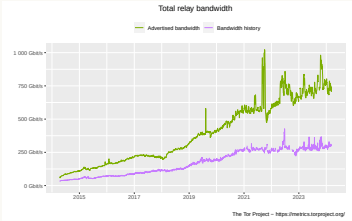
Less protection

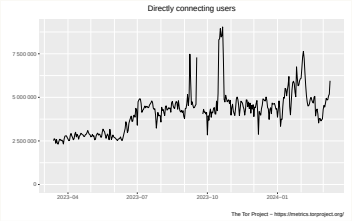


A one-hop proxy, aka a VPN

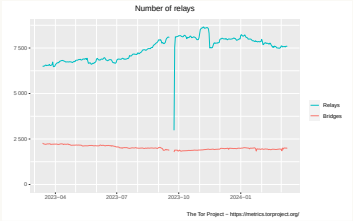
Who is providing Tor

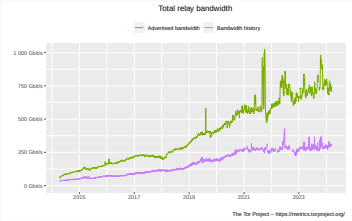


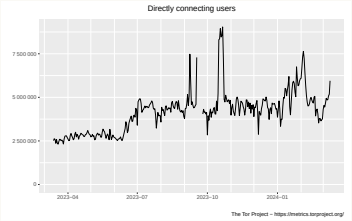


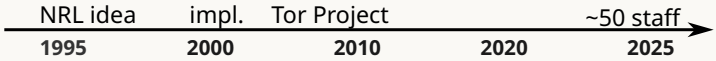


Who is providing Tor

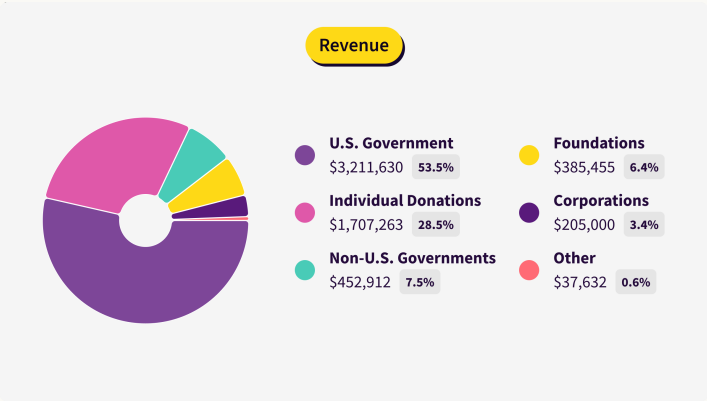








Who is funding Tor



Outline

1. ~~Tor crash course~~
2. Censorship circumvention
3. Wrap up

Censorship circumvention

Users get blocked based on...

Destination address

Protocol behaviour

Content

Censorship circumvention

Users get blocked based on...

Destination address

Protocol behaviour

Content

Censorship circumvention

Users get blocked based on...

Destination address

Protocol behaviour

Content

Active probing

Censor connects to suspected proxies, adding positives to block list

Active probing

Censor connects to suspected proxies, adding positives to block list

2010 SSH from .cn (Leif Nixon)
2011 Tor bridges get quickly blocked by GFW
2012 Tor probing research (KAU)
2014 Scramblesuit (KAU) and “obfs4” wire formats
2015 More research (Princeton, UCB, KAU)
2018 Active probing seen in .ru
...

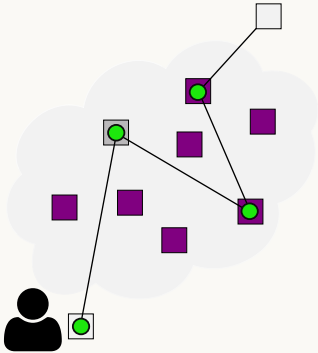
Do use an anonymity system

knowledge	the more a censor knows the easier they block
untrusted	there's no such thing as a trusted unblocked network (because of the proxy discovery problem)
tomorrow	situations can change

The proxy discovery problem: How can clients discover the proxies without having the censor discover and block these proxies?

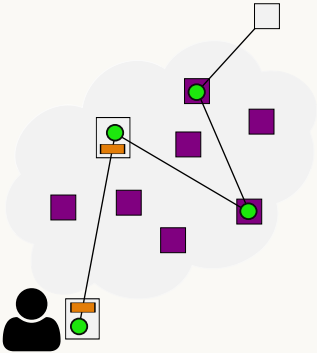
How do censored users reach Tor

Tor bridges



Unlisted first-hops

Pluggable Transports



Plugin programs

Tor Pluggable Transports

obfs4 meek Snowflake

New contender: WebTunnel, mimicking HTTPS

Tor Pluggable Transports

obfs4 **meek** **Snowflake**

New contender: WebTunnel, mimicking HTTPS

Tor Pluggable Transports

obfs4 **meek** **Snowflake**

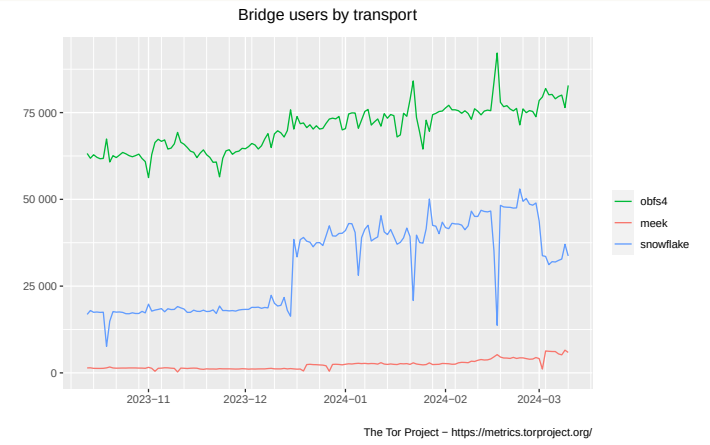
New contender: WebTunnel, mimicking HTTPS

Tor Pluggable Transports

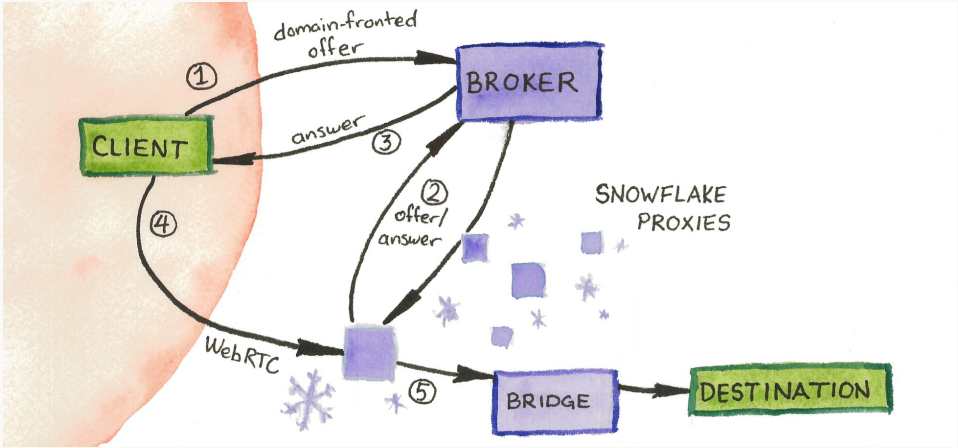
obfs4 **meek** **Snowflake**

New contender: WebTunnel, mimicking HTTPS

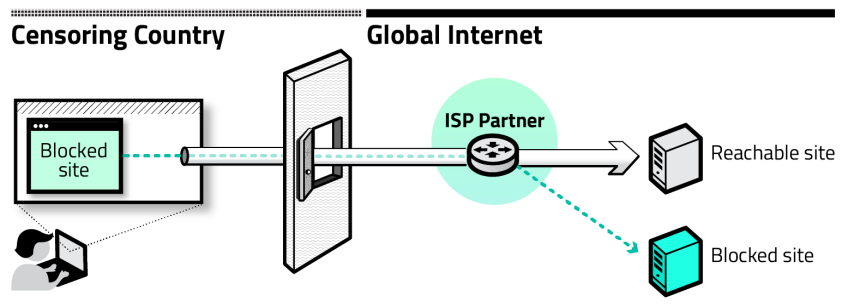
Pluggable transports



Snowflake

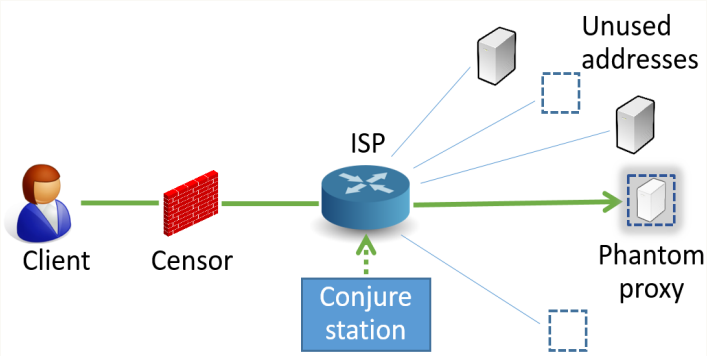

domain-fronted
offer
①
BROKER
CLIENT
answer
③
②
offer/
answer
SNOWFLAKE
PROXIES
④
WebRTC
⑤
BRIDGE
DESTINATION

Refraction networking



https://refraction.network/

Conjure



https://jhalderm.com/pub/papers/conjure-ccs19.pdf

How can network operators help censored users

- Deploy Conjure, making use of that unused address space
- Support Snowflake
  - Help people run proxies
  - Donate bandwidth, hardware...
  - ... or just money `https://opencollective.com/censorship-circumvention/projects/snowflake-daily-operations`
- Please don't disconnect

How can network operators help censored users

- Deploy Conjure, making use of that unused address space
- Support Snowflake
  - Help people run proxies
  - Donate bandwidth, hardware...
  - ... or just money https://opencollective.com/censorship-circumvention/projects/snowflake-daily-operations
- Please don't disconnect

How can network operators help censored users

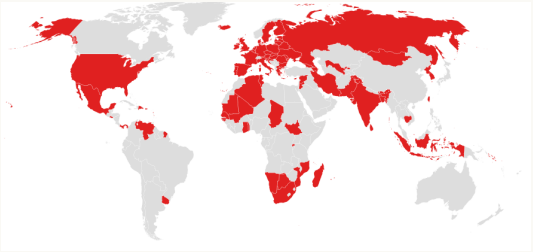
- Deploy Conjure, making use of that unused address space
- Support Snowflake
  - Help people run proxies
  - Donate bandwidth, hardware...
  - ... or just money https://opencollective.com/censorship-circumvention/projects/snowflake-daily-operations
- Please don't disconnect

Outline

1. ~~Tor crash course~~
2. ~~Censorship circumvention~~
3. Wrap up

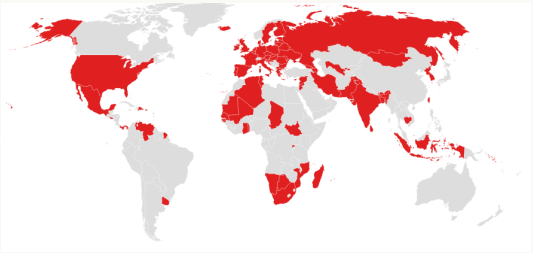
Wrap up

- What Tor provides and how it works
- How users get blocked
- Why using an anonymity system when circumventing censorship is important
- How censored users can reach Tor
- Refraction networking
- How to help



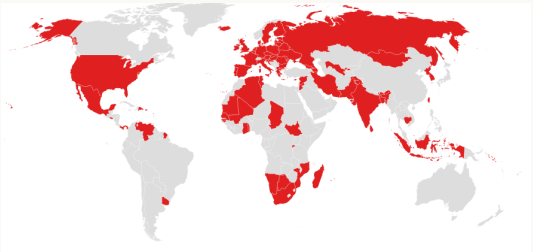
Wrap up

- What Tor provides and how it works
- How users get blocked
- Why using an anonymity system when circumventing censorship is important
- How censored users can reach Tor
- Refraction networking
- How to help



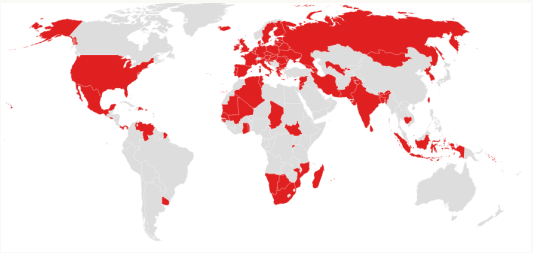
Wrap up

- What Tor provides and how it works
- How users get blocked
- Why using an anonymity system when circumventing censorship is important
- How censored users can reach Tor
- Refraction networking
- How to help



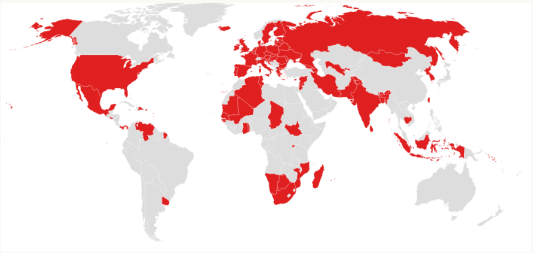
Wrap up

- What Tor provides and how it works
- How users get blocked
- Why using an anonymity system when circumventing censorship is important
- How censored users can reach Tor
- Refraction networking
- How to help



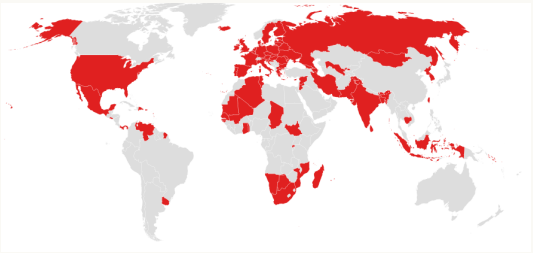
Wrap up

- What Tor provides and how it works
- How users get blocked
- Why using an anonymity system when circumventing censorship is important
- How censored users can reach Tor
- Refraction networking
- How to help



Wrap up

- What Tor provides and how it works
- How users get blocked
- Why using an anonymity system when circumventing censorship is important
- How censored users can reach Tor
- Refraction networking
- How to help



Thank you for listening

- Also, thanks to
  - Tor anti-censorship team for all the knowledge
  - David Fifield for the Snowflake figure
  - Ilja Hallberg for the Alice and Bob figure

Recommended reading

- Threat modeling and circumvention of Internet censorship
  https://www.bamsoftware.com/papers/thesis/
- A Worldwide View of Nation-state Internet Censorship
  https://censorbib.nymity.ch/#Master2023a
- Examining How the Great Firewall Discovers Hidden Circumvention Servers
  https://censorbib.nymity.ch/#Ensafi2015b
- TSPU: Russia's Decentralized Censorship System
  https://censorbib.nymity.ch/#Xue2022b
- The use of TLS in Censorship Circumvention
  https://censorbib.nymity.ch/#Frolov2019a
- Conjure: Summoning Proxies from Unused Address Space
  https://jhalderm.com/pub/papers/conjure-ccs19.pdf