# Anonymity loves Diversity: The Case of Tor

Georg Koppen       Alexander Færøy

November 1, 2020

FOSS North

# About Georg

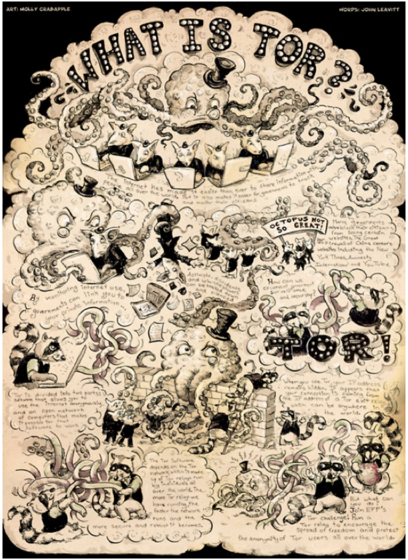
- Started volunteering around 2010
- Core Developer at The Tor Project since 2013
- Led the Tor Browser team from 2016-2019
- Transitioned to network health work in 2020

# About Alexander

- Core Developer at The Tor Project since early 2017.
- Free Software developer since 2006.
- Worked with distributed systems in the Erlang programming language, WebKit-based mobile web browsers, consulting, and firmware development.
- Co-organizing the annual Danish hacker festival BornHack.

# What is Tor?

- Online anonymity, and censorship circumvention.
  - Free software.
  - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.

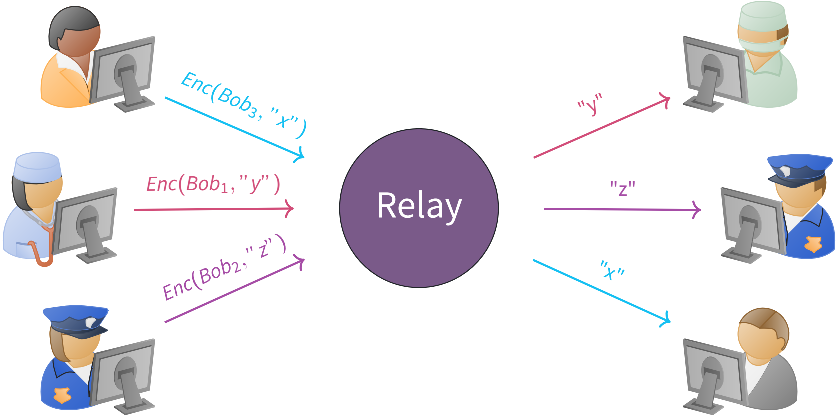

ART: MOLLY CRABAPPLE
WORDS: JOHN LEAVITT
WHAT IS TOR?
The Internet has made it easier than ever to share information with people all over the world. But it also makes it easier for governments to track and monitor their citizens
OCTOPUS NOT SO GREAT!
Many governments also block their citizens from seeing certain websites. The Great Firewall of China censors websites including the New York Times, Amnesty International and YouTube.
By monitoring internet use, governments can link you to your private information...
Activists, dissidents and whistleblowers can be tracked down and silenced
How can we circumvent government surveillance and censorship?
TOR!
Tor is divided into two parts: software that allows you to use the Internet anonymously and an open network of computers that makes it possible for that software to work.
When you use Tor, your IP address remains hidden. It appears that your connection is coming from the IP address of a Tor exit relay which can be anywhere in the world.
The Tor Software depends on the Tor network, which is made up of Tor relays run by individuals all over the world. The more Tor relays we have running, the faster the network runs and the more secure and robust it becomes.
But what can you do? Join EFF's Tor challenge! Run a Tor relay to encourage the spread of freedom and protect the anonymity of Tor users all over the world.

# History

| | |
|---|---|
| **Early 2000s** | Working with the U.S. Naval Research Laboratory. |
| **2004** | Sponsorship by the Electronic Frontier Foundation. |
| **2006** | The Tor Project, Inc. became a non-profit. |
| **2008** | Tor Browser development. |
| **2010** | The Arab spring. |
| **2013** | The summer of Snowden. |
| **2018** | Anti-censorship team created. |
| **2019** | Tor Browser for Android released. |
| **2020** | Network Health team created. |

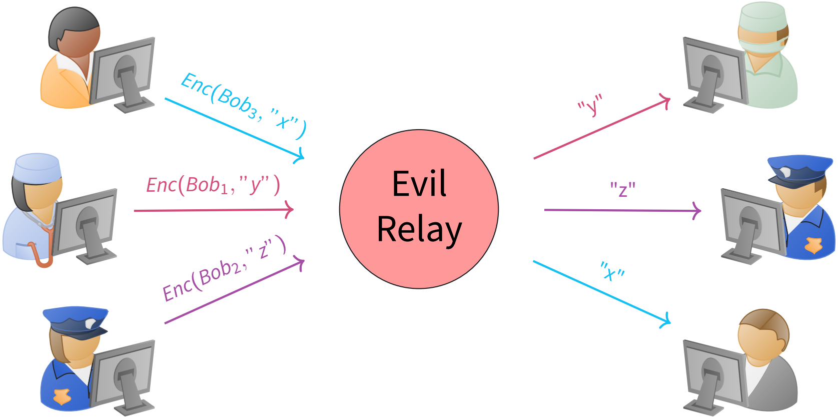
Somewhere between 2,000,000 and 8,000,000 daily users.

# A Simple Design

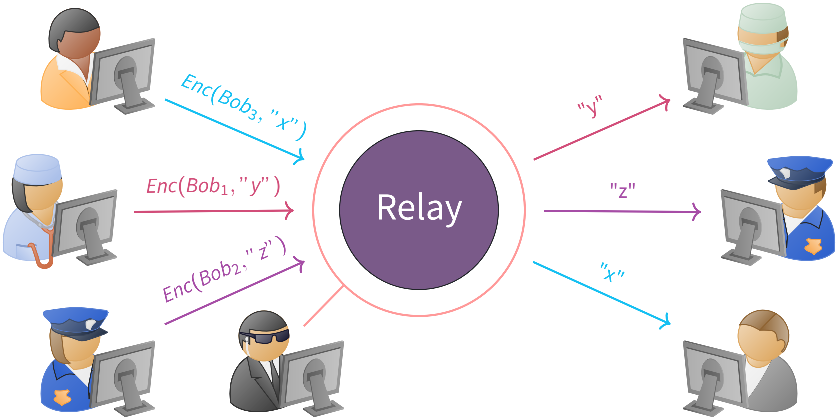


Equivalent to some commercial proxy providers.

# A Simple Design

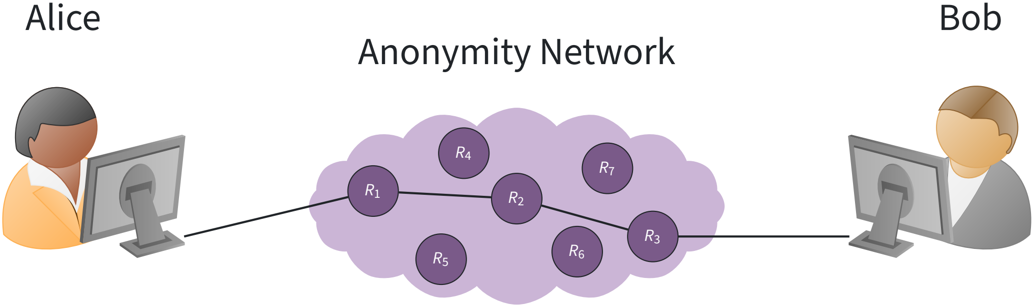


# A Simple Design



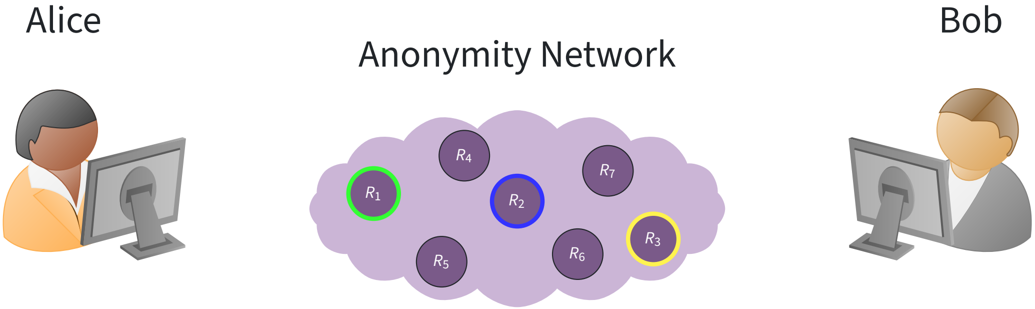
Timing analysis bridges all connections going through the relay.

# The Tor Design



Add multiple relays so that no single relay can betray Alice.

# The Tor Design



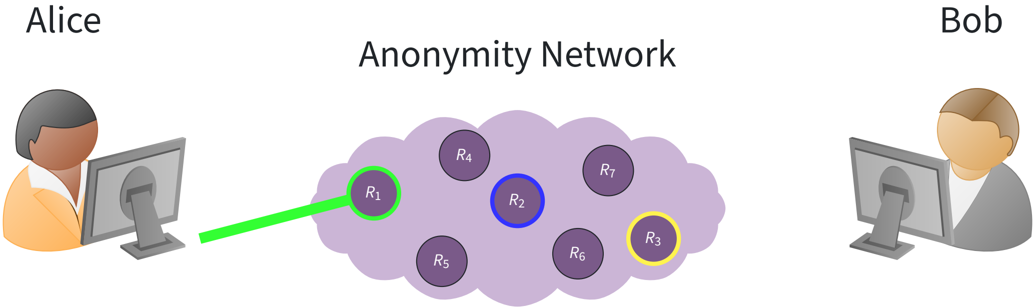
Alice

Anonymity Network

Bob

Alice picks a path through the network: $R_1$, $R_2$, and $R_3$ before finally reaching Bob.

# The Tor Design



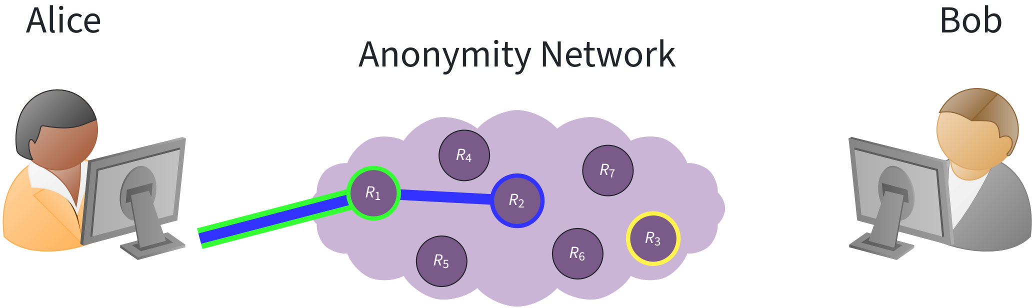
Alice

Anonymity Network

Bob

Alice makes a session key with $R_1$.

# The Tor Design



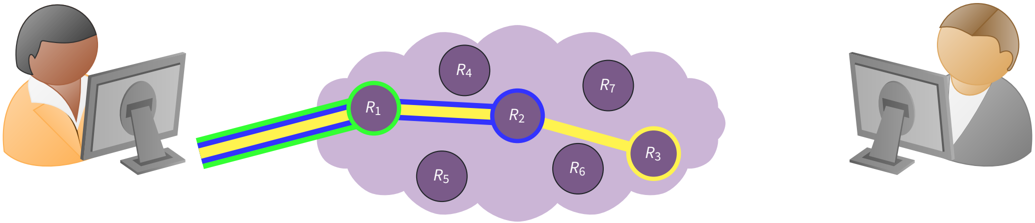
Alice asks $R_1$ to extend to $R_2$.

# The Tor Design

Alice

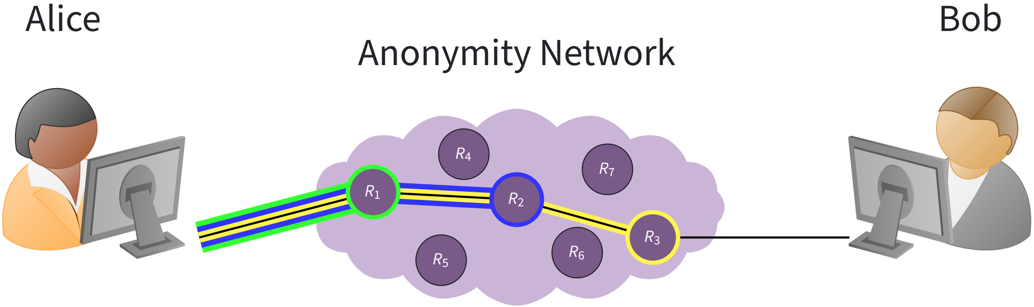
Anonymity Network

Bob



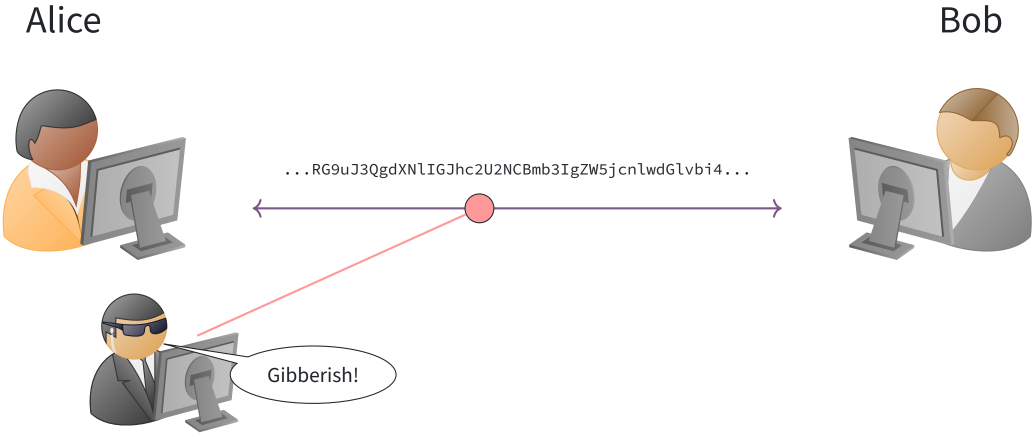
Alice asks $R_2$ to extend to $R_3$.

# The Tor Design



Alice finally asks $R_3$ to connect to Bob.

# Anonymity isn’t Encryption



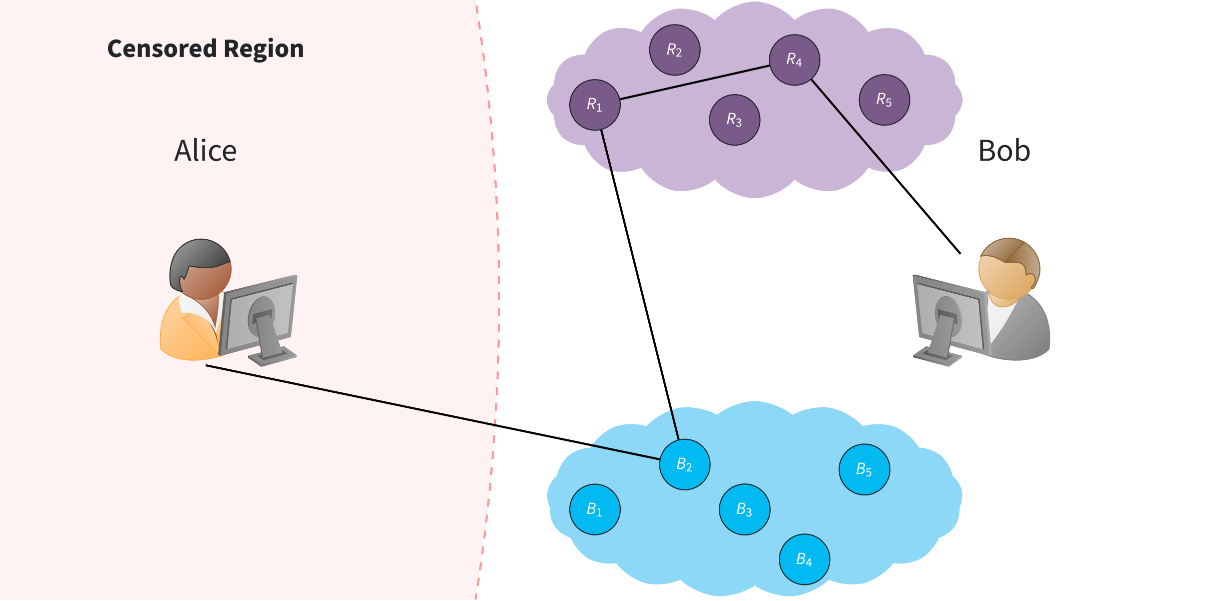
Encryption just protects contents.

# Metadata

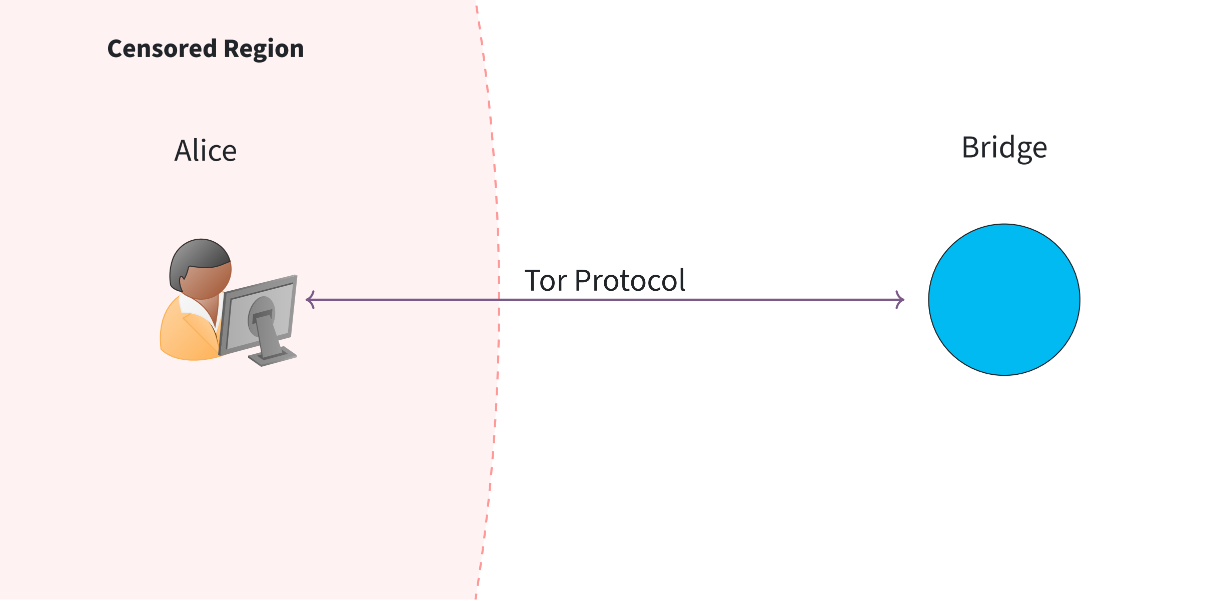
*"We Kill People Based on Metadata."*

*—Michael Hayden, former director of the NSA.*

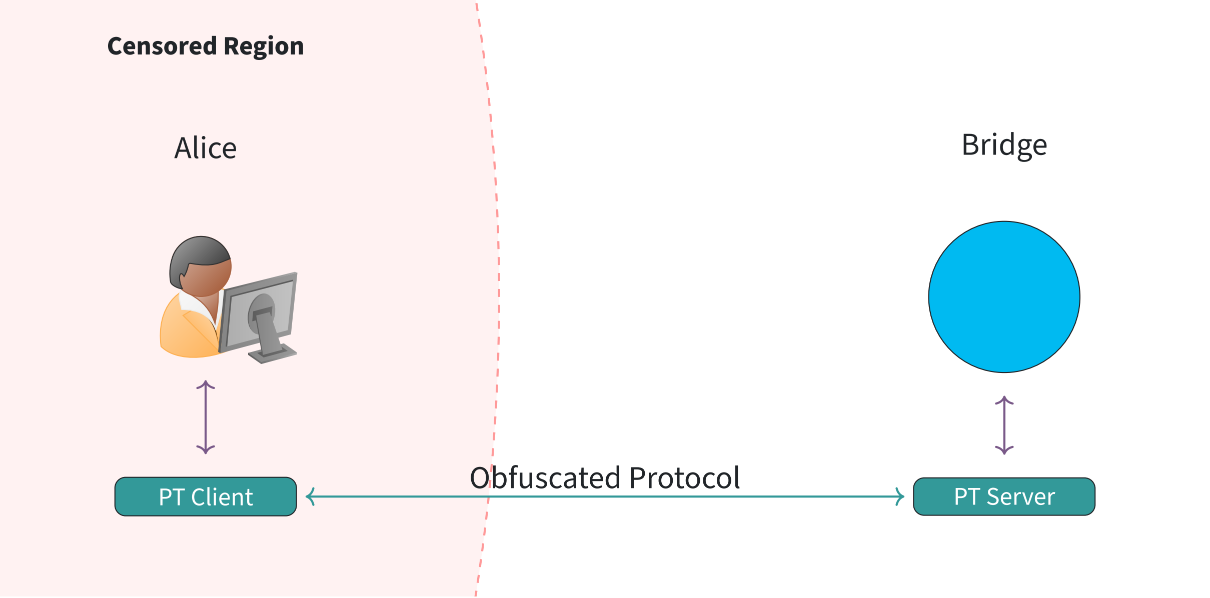
# Bridges



# Bridges



# Bridges and Pluggable Transports



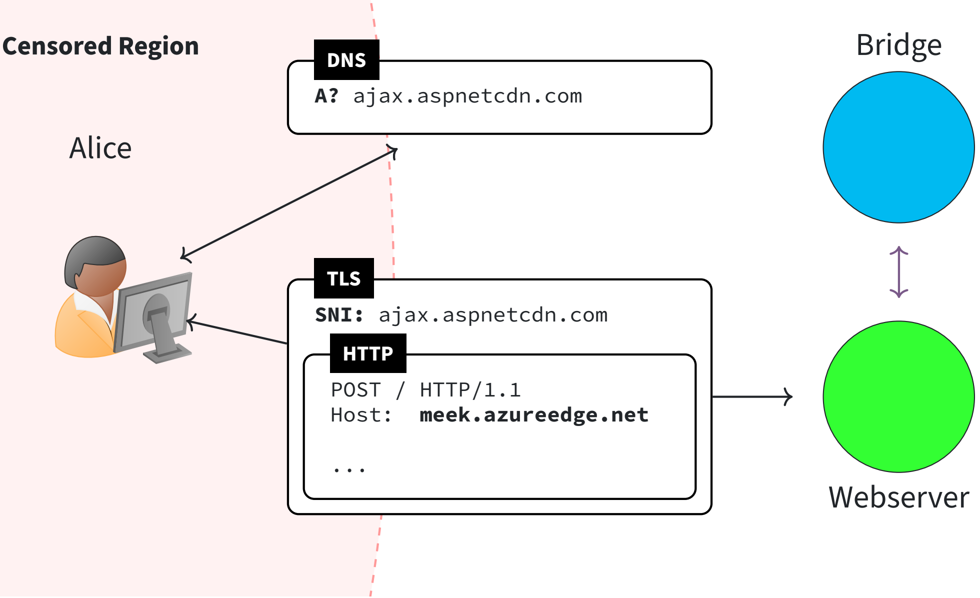
# Pluggable Transports

- Allows people to easily build, experiment, and deploy their own obfuscation technology without having to modify the Tor source code itself.
- The specification for Pluggable Transports is open and allows other vendors to implement support for PTs in their own products.
- Allows people to experiment with different transports for Tor that might not be doing any anti-censorship related obfuscation.

# Obfourscator (obfs4)

- Makes it hard for passive DPI to verify the presence of the obfs4 protocol unless the adversary knows the bridge parameters.
- Makes active probing hard unless the adversary knows the bridge parameters.
- Uses Tor's ntor handshake (x25519), but uses Elligator2 to encode the elliptic-curve points to be indistinguishable from uniform random strings. The link layer encryption uses NaCl secret boxes (XSalsa20 and Poly1305).

# SNI Domain Fronting using Meek



**Censored Region**

Alice

Bridge

Webserver

**DNS**

```
A? ajax.aspnetcdn.com
```

**TLS**

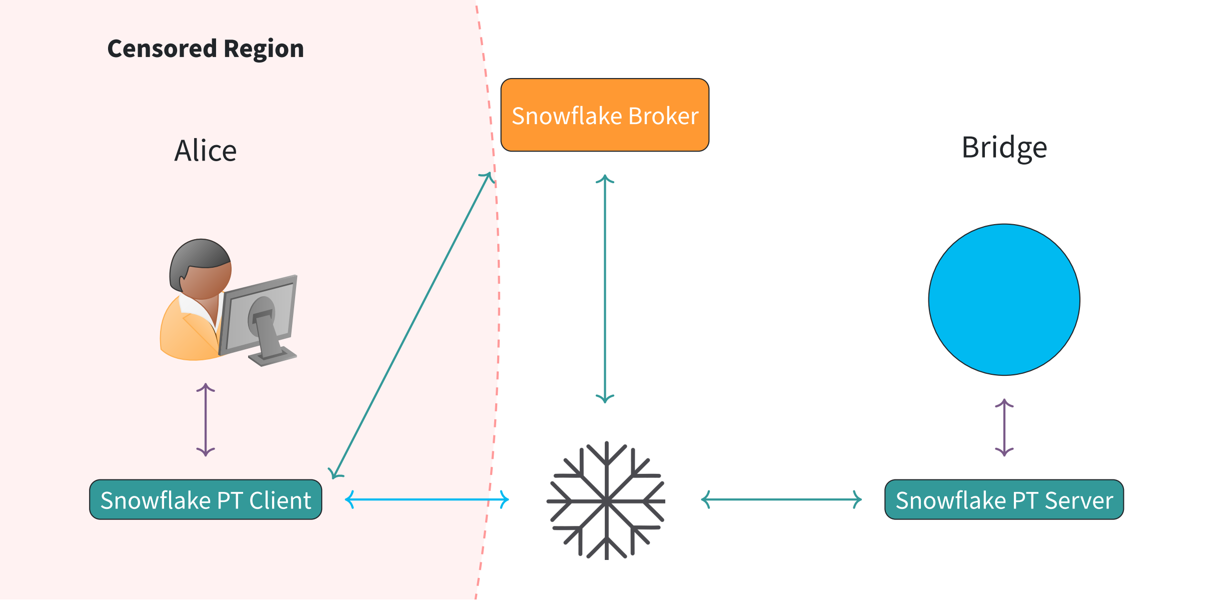
```
SNI: ajax.aspnetcdn.com
```

**HTTP**

```
POST / HTTP/1.1
Host:  meek.azureedge.net

...
```

# Snowflake



Censored Region

Alice

Snowflake Broker

Bridge

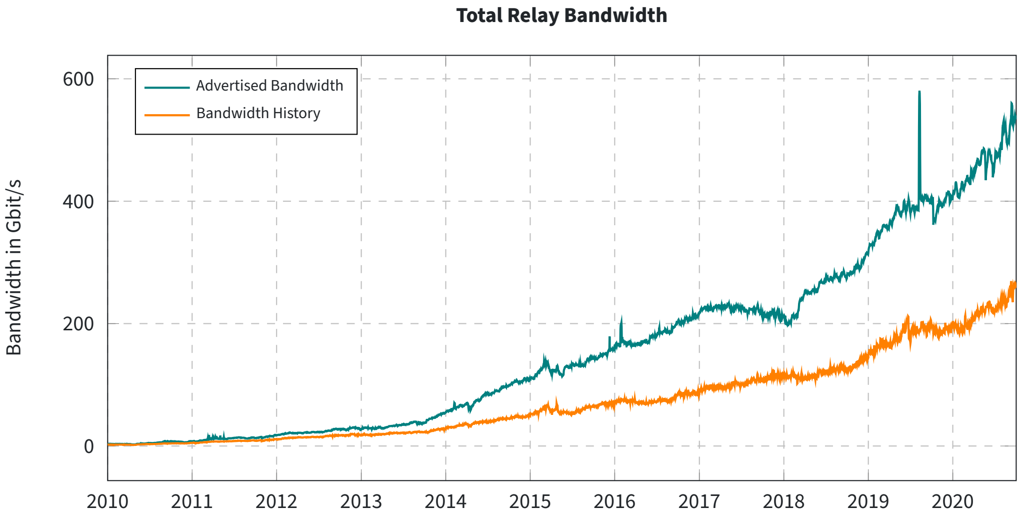
Snowflake PT Client

Snowflake PT Server

# The Tor Network

- An open network – everybody can join!
- Between 6000 and 7000 relay nodes.
- Kindly hosted by various individuals, companies, and non-profit organisations.
- 9 Directory Authority nodes and 1 Bridge Authority node.

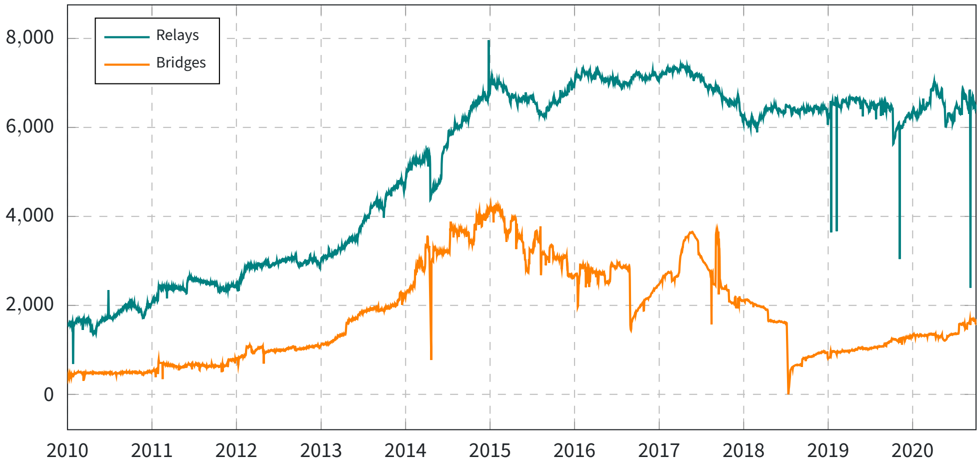
# The Tor Network



Source: metrics.torproject.org

# The Tor Network

## Number of Relays



Source: metrics.torproject.org

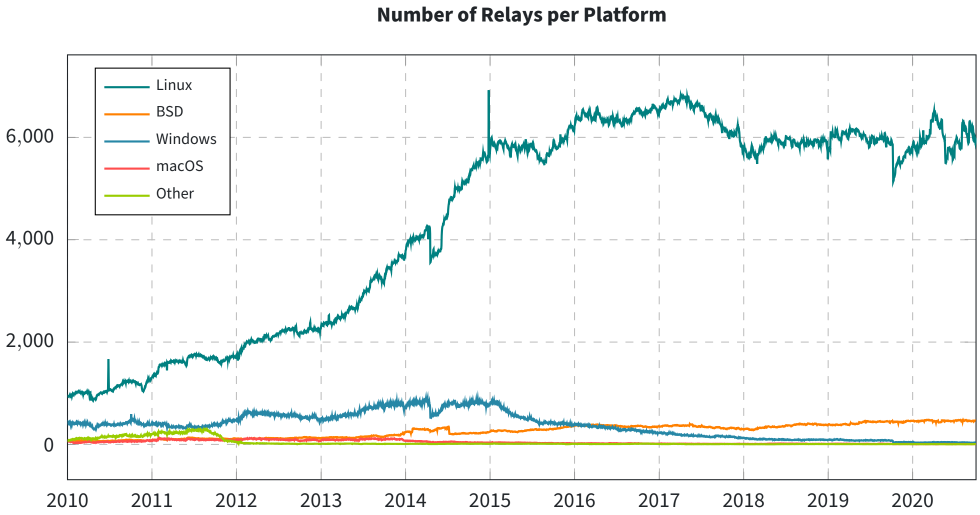
# The Tor Network

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.
2. Diversity of users and reasons to use it. 50,000 users in Iran means almost all of them are normal citizens.

**Research problem**: How do we measure diversity over time?

# The Tor Network

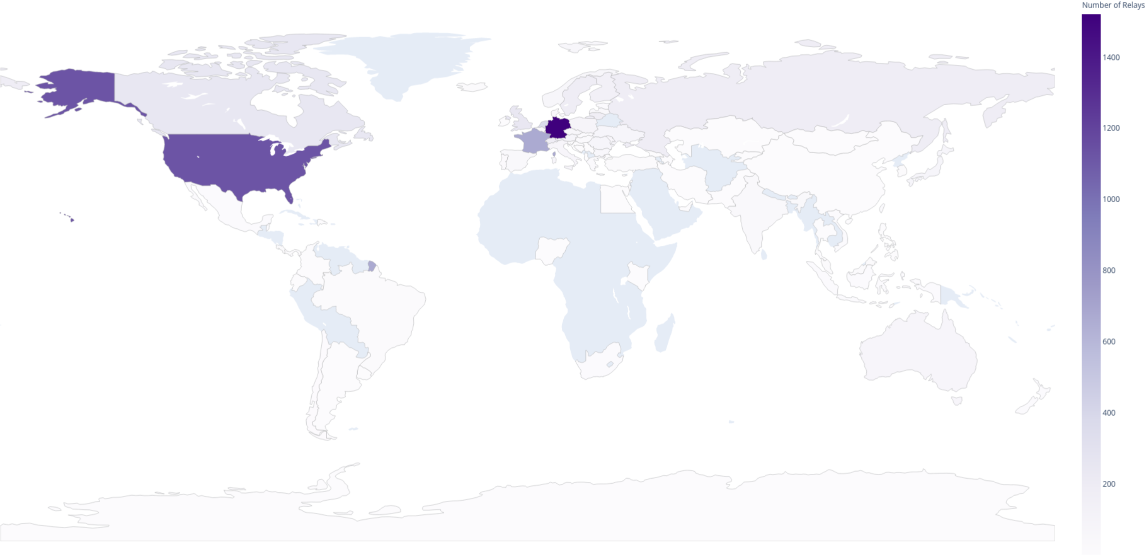


Source: metrics.torproject.org

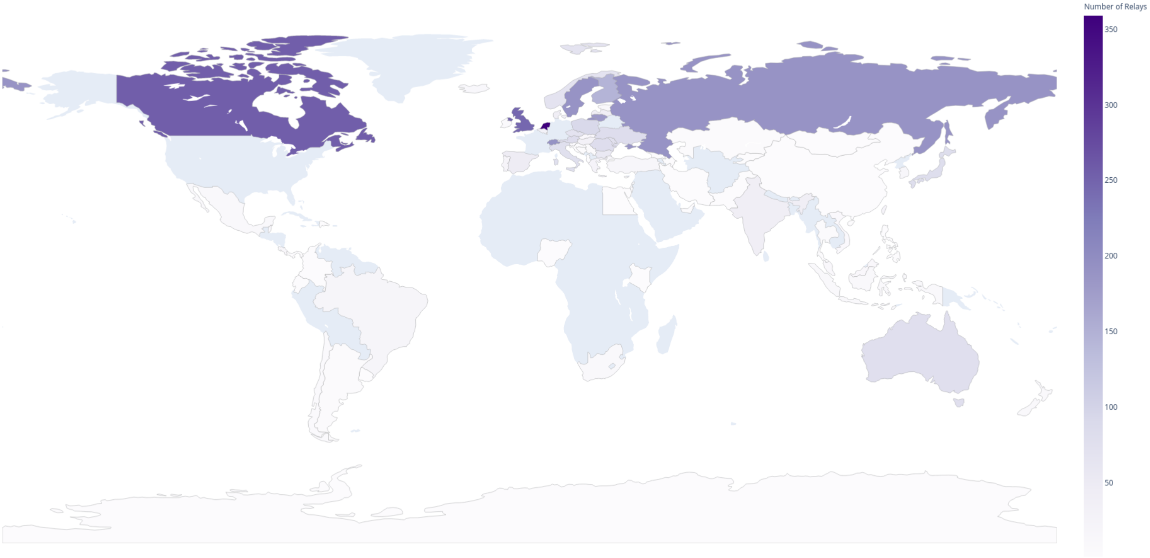
# The Tor Network

| # | Country | Relays |
|---|---|---:|
| 1 | Germany | 1517 |
| 2 | United States | 1114 |
| 3 | France | 677 |
| 4 | Netherlands | 359 |
| 5 | Canada | 256 |
| 6 | United Kingdom | 246 |
| 7 | Switzerland | 193 |
| 8 | Sweden | 191 |
| 9 | Russian Federation | 187 |
| 10 | Lithuania | 179 |
| 22 | Norway | 69 |
| 27 | Denmark | 44 |

Number of Relays per Country (2020)



Number of Relays per Country (2020)



# The Tor Network

| Network | Relays |
|---|---:|
| 185.220.0.0/16 | 216 |
| 51.81.0.0/16 | 97 |
| 51.15.0.0/16 | 87 |
| 185.150.0.0/16 | 68 |
| 163.172.0.0/16 | 59 |
| 172.105.0.0/16 | 57 |
| 95.216.0.0/16 | 56 |
| 195.189.0.0/16 | 55 |
| 51.195.0.0/16 | 49 |
| 51.91.0.0/16 | 40 |

# The Tor Network

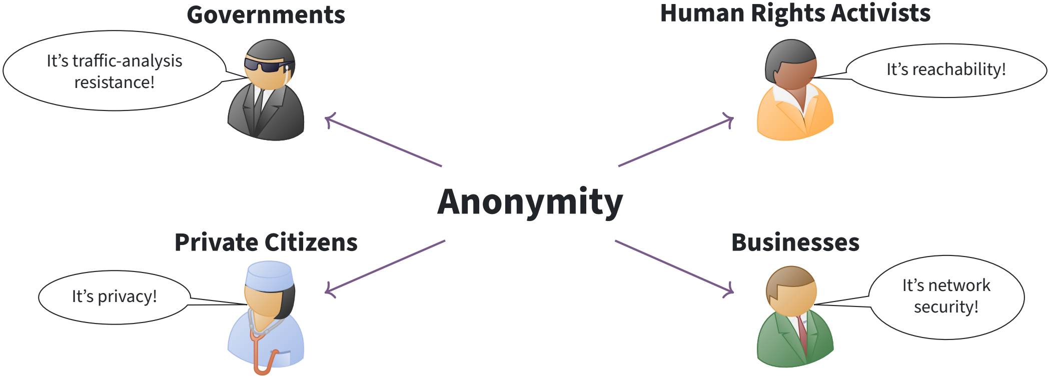
| AS Number | Name | Relays |
|---|---|---:|
| AS 16276 | OVH, FR | 770 |
| AS 24940 | HETZNER-AS, DE | 403 |
| AS 12876 | Online SAS, FR | 263 |
| AS 63949 | LINODE-AP Linode, LLC, US | 240 |
| AS 14061 | DIGITALOCEAN-ASN, US | 166 |
| AS 208294 | ASMK, NL | 140 |
| AS 197540 | NETCUP-AS netcup GmbH, DE | 138 |
| AS 53667 | PONYNET, US | 136 |
| AS 3320 | DTAG Internet service provider operations, DE | 118 |
| AS 16125 | CHERRYSERVERS1-AS, LT | 104 |

# The Tor Network

Malicious relays and what we (plan to) do about them:

- Malicious guard+exit relays (Guard pinning, MyFamily settings)
- Malicious exit relays
  - Exit scanning (e.g. against SSL strip attacks)
  - Blacklisting found relays (but: that’s an uphill battle)
  - Application-level improvements (HTTPS-only mode)
  - Limit weight/influence of unknown relays

# Applications



Governments

It’s traffic-analysis resistance!

Human Rights Activists

It’s reachability!

Anonymity

Private Citizens

It’s privacy!

Businesses

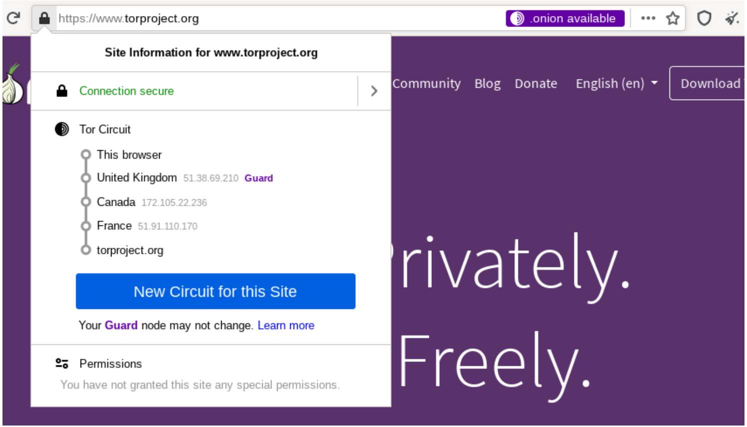
It’s network security!

# Applications

- Many users with different backgrounds helps against singling individuals out
- But how do we prevent all those users from getting fingerprinted due to their different computers?
  - Make everyone look the same
  - Obscure real values by spoofing/faking them

# Applications

- Many users with different backgrounds helps with usability, privacy protections, and security



https://www.torproject.org

Site Information for www.torproject.org

Connection secure

Tor Circuit

This browser

United Kingdom 51.38.69.210 Guard

Canada 172.105.22.236

France 51.91.110.170

torproject.org

New Circuit for this Site

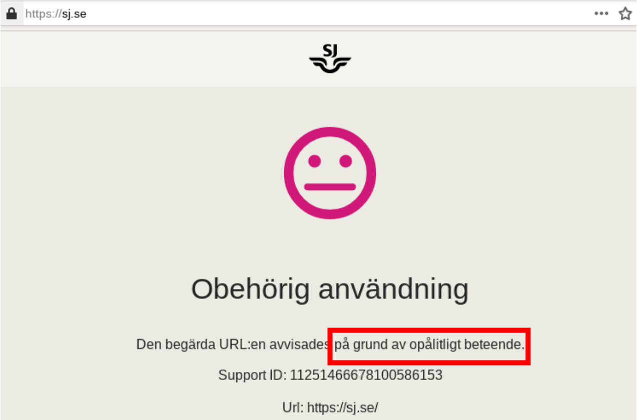
Your Guard node may not change. Learn more

Permissions

You have not granted this site any special permissions.

# Applications

- There are downsides we have to deal with, e.g. user blocking or CAPTCHAs



Obehörig användning

Den begärda URL:en avvisades på grund av opålitligt beteende.

Support ID: 11251466678100586153

Url: https://sj.se/

# Applications

Possible mitigations to Tor blocking:

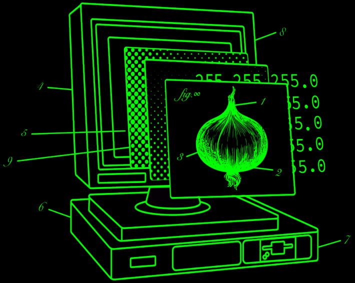
- Outreach? (but that does not scale)
- PoW schemes? (might help against onion service DoS, too, see: proposal 327)
- Anonymous credentials?
- Paid exit relays?

# How can you help?

- Hack on some of our cool projects.
- Find, and maybe fix, bugs in Tor.
- Test Tor on your platform of choice.
- Work on some of the many open research projects.
- Run a Tor relay or a bridge!
- Teach others about Tor and privacy in general.

# USE A MASK, USE TOR.

Resist the surveillance pandemic.



Donate at donate.torproject.org

# Questions?