State of the Onion

Alexander Færøy

November 27, 2022

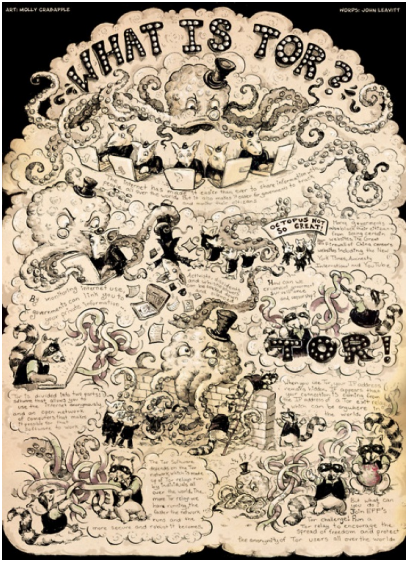
Cryptohagen

About Me

- Core Developer at The Tor Project since early 2017. Team Lead of the Network Team since late 2019.
- Free Software developer since 2006.
- Co-organizing the annual Danish hacker festival BornHack on Funen.

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.



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.
2007	Expansion to anti-censorship.
2008	Tor Browser development.
2010	The Arab spring.
2013	The summer of Snowden.
2018	Anti-censorship team created.
2019	Tor Browser for Android released.
2022	Mahsa Amini protests in Iran.

Network Team Summary of 2022

- Continue the ramping down on new client features in the C implementation of Tor.
- Ramping up on Rust development as part of the Arti project.
- VPN work with LEAP and Guardian Project!
- Work with friends that are integrating Tor into their applications.
- Denial of Service **:-(**
- Shadow simulations.

Arti

Focus on building a library to work with the entire Tor ecosystem:

- Embed the Arti client into your own application.
- Parsing different Tor related network objects.
- Onion Services ecosystem.

... while avoiding the spaghetti architecture of C Tor.

Arti

But, why rewrite Tor?

Writing "safe C" is costly, and prone to mistakes:

21 out of 34 of Tor's TROVEs were due to errors that would be impossible (or very unlikely) in Rust.

Most of the Network Team at Tor is very excited about Rust, and was interested in spending more time writing software in it.

Arti Roadmap

0.1.0	API stability. **Year I**
1.0.0	Usability, performance, and stability. **Year I**
1.1.0	Anti-censorship. **Year I**
1.2.0	Onion services. **Year II**
2.0.0	Ready to replace the C client. **Year II**
Future	Relay, bridge, directory authority, etc.

Arti and Legacy Tor

Currently, **3 out of 7 members of the Network Team are working full-time on Rust and Arti deliverables.** We aim to have the entire team work in this space as soon as possible.

We will **reduce feature additions in C Tor** drastically and will not be adding more Long-Term Support Tor releases.

We will **continue to support C Tor** until Arti can replace the currently used C Tor implementation.

Congestion Control

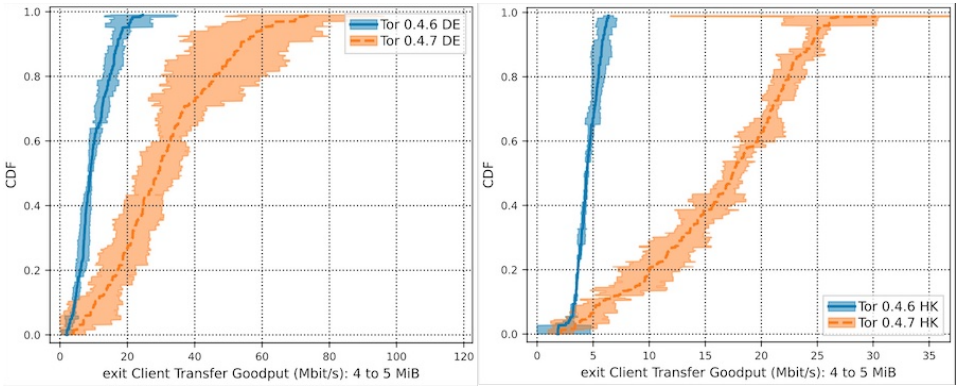
We implemented three congestion control algorithms: Tor-Westwood, Tor-Vegas, and Tor-NOLA. All of them are available in **Tor 0.4.7.**

Both Tor-Westwood and Tor-NOLA exhibited ack compression, which caused them to wildly overestimate the Bandwidth-Delay Product, which lead to runaway congestion conditions.

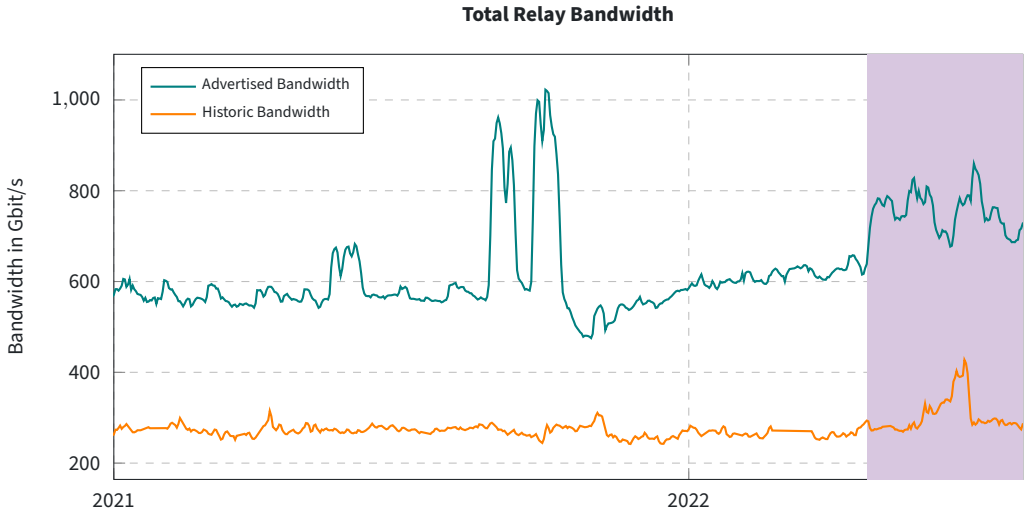
Google's BBR algorithm also suffers from these problems, and was not implemented in Tor.

Congestion Control

Tor-Vegas performed beautifully, almost exactly as the theory predicted, as seen in the results from **Shadow.**



Congestion Control



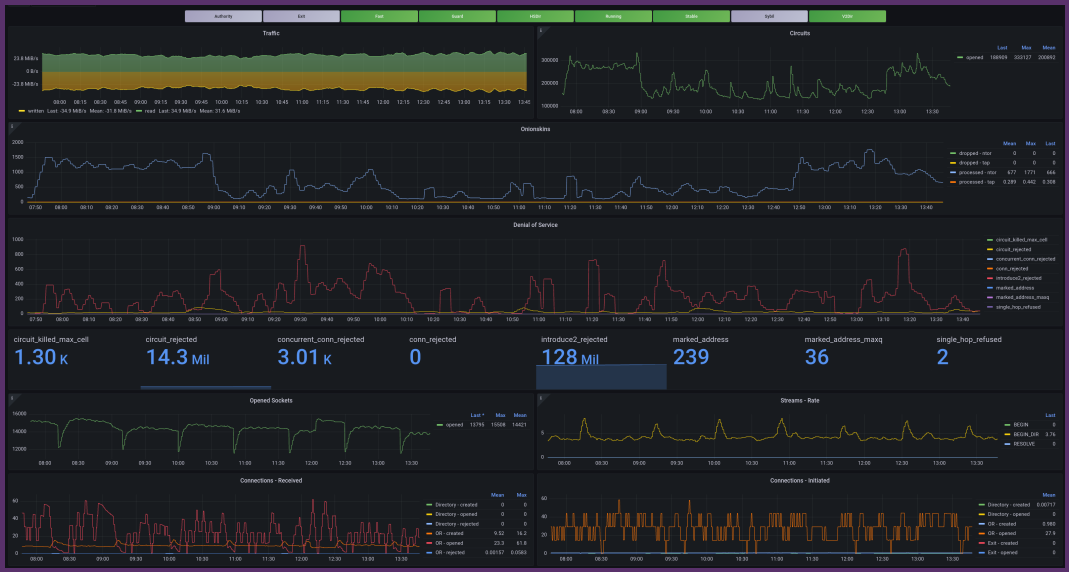
Source: metrics.torproject.org

Ongoing Denial of Service

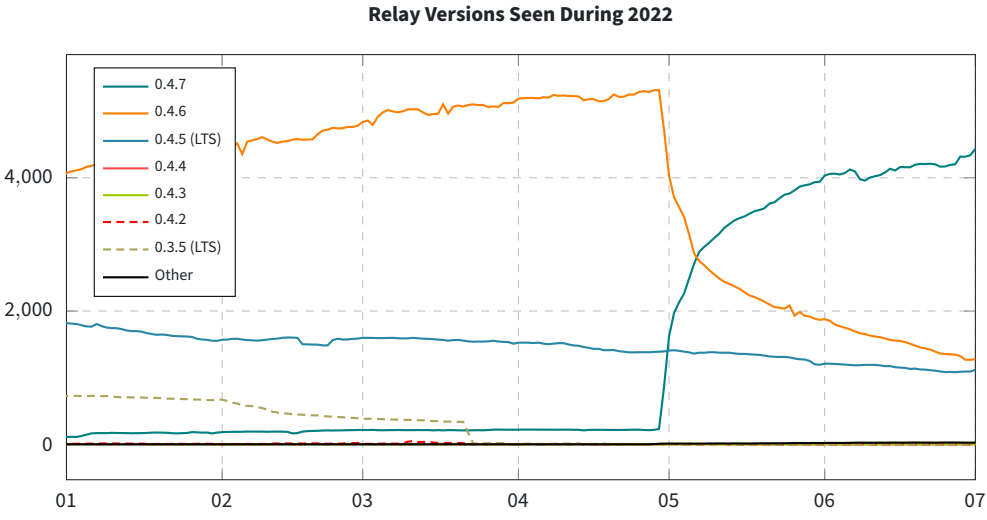
The ongoing Denial of Service against the Tor network in the last couple of months have made it drastically harder to analyse the impact and tuning opportunities related to the deployment of congestion control in the network.

Ongoing efforts to reduce the impact of Denial of Service attacks is helping, but it continues to be a bit of an arms race.

Better introspection tooling for Tor is also being integrated into C Tor via the **MetricsPort** feature.


Authority
Exit
Fast
Guard
Hsdir
Running
Stable
Valid
V3dir
Traffic
23.8 MiB/s
0 B/s
-23.8 MiB/s
written Last: -34.9 MiB/s Mean: -31.8 MiB/s
read Last: 34.9 MiB/s Mean: 31.8 MiB/s
Circuits
Last Max Mean
opened 188909 353127 206693
Onionskins
Mean Max Last
dropped - ntor 0 0 0
dropped - tap 0 0 0
processed - ntor 677 1771 666
processed - tap 0.291 0.442 0.308
Denial of Service
circuit_killed_max_cell
circuit_rejected
concurrent_conn_rejected
conn_rejected
introduce2_rejected
marked_address
marked_address_maxq
single_hop_refused
circuit_killed_max_cell
1.30 K
circuit_rejected
14.3 Mil
concurrent_conn_rejected
3.01 K
conn_rejected
0
introduce2_rejected
128 Mil
marked_address
239
marked_address_maxq
36
single_hop_refused
2
Opened Sockets
Last * Max Mean
opened 13795 15508 14421
Streams - Rate
Last
BEGIN 0
BEGIN_DIR 3.76
RESOLVE 0
Connections - Received
Mean Max
Directory - created 0 0
Directory - opened 0 0
Directory - rejected 0 0
OR - created 9.92 16.2
OR - opened 23.3 61.8
OR - rejected 0.00157 0.0583
Connections - Initiated
Mean
Directory - created 0.00717
Directory - opened 0
OR - created 0.988
OR - opened 27.9
Exit - created 0
Exit - opened 0

The Tor Network



Source: metrics.torproject.org

A massive thank you for upgrading to Tor 0.4.7 so quickly!

Congestion Control

Onion Service operators will also benefit from upgrading to **Tor 0.4.7.**

For more details, please read Mike Perry's blog post on Congestion Control at blog.torproject.org/congestion-contrl-047

Proof of Work for Onion Services

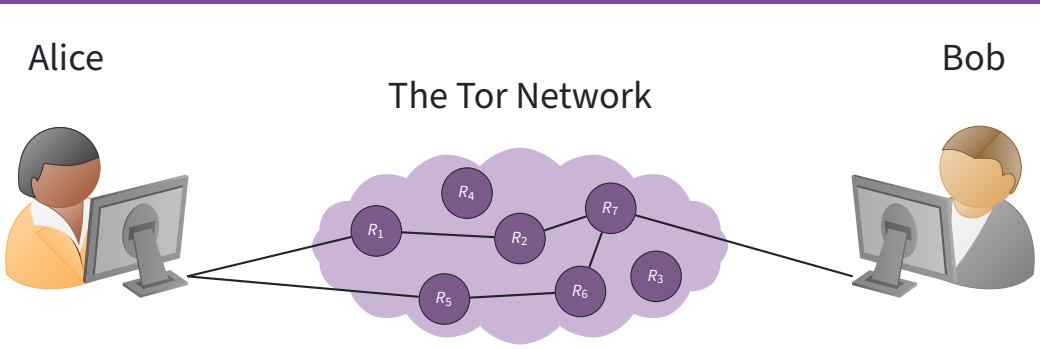
Implement PoW for Onion Services that can dynamically enable, disable, and adjust the difficulty of the system if pathological situations appears.

Make the cost of attacking an Onion Service higher.

A big thanks to **tevador** for all the help here!

See Proposal #327.

Conflux



UDP Support in the Tor Network

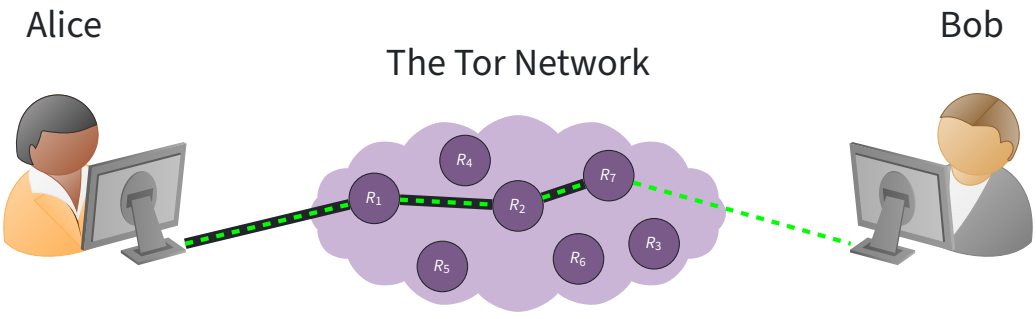
Support UDP for Tor clients and Exit nodes to allow support for modern internet applications such as: Crypto wallets, streaming, VoIP, and *hopefully* WebRTC-based applications.

Client and Exit nodes will require upgrades for deployment.

Use Tor's Congestion Control system to decide when to drop packets at the edges.

Specification work being tracked in torspec#73 on Tor's Gitlab.

UDP Support in the Tor Network



VPN using Tor

Allow users to use Tor with applications that are not necessarily Tor-aware.

The initial focus will be on the **Android** platform, but more platforms should become supported over time.

Our current **goal is to release the application in 2023.**

Onionmasq

Build a layer 3 packet engine library in Rust for handling:

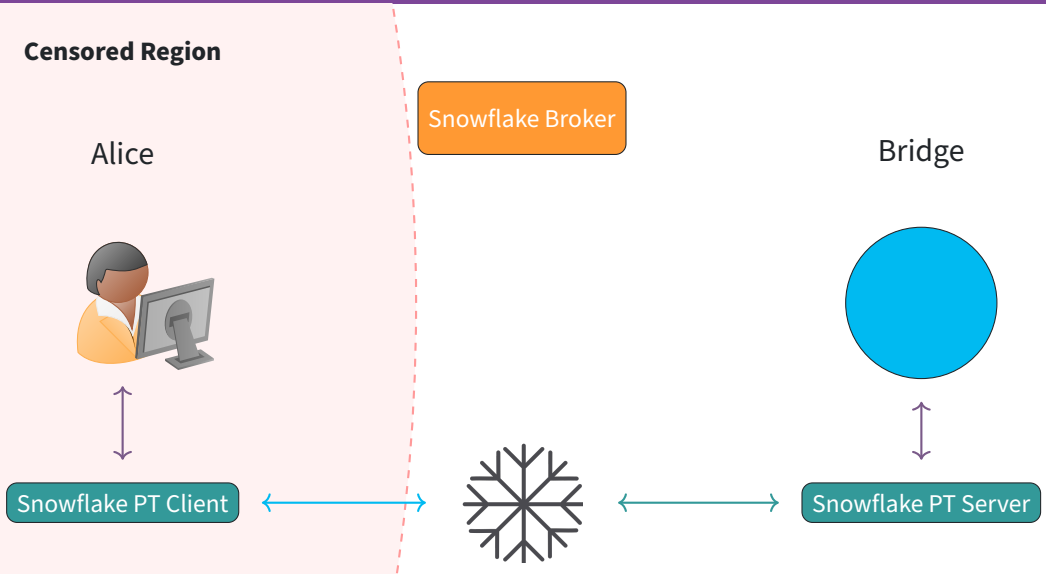
- Read and write IP packets from TUN devices.
- Multiplexing between TCP/UDP flows and Arti's TCP/UDP socket interface.
- Onion Service connectivity using cookie responses from DNS.
- Basic filtering mechanism for disallowing certain flows.

Onionmasq

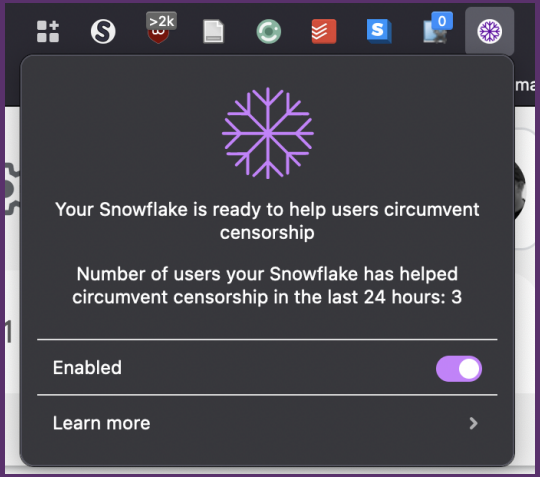
We need to expand the usual IP 5-tuple with additional flow metadata for isolation purposes:

- Application UUID (Unix User ID on Android) and its name.
- Hostname (if any).
- DNS cookie (for looking up cookie IP to Onion Service identifier).

Snowflake


Censored Region
Snowflake Broker
Alice
Bridge
Snowflake PT Client
Snowflake PT Server

Check out snowflake.torproject.org



Snowflake

We have seen over **100,000** Snowflakes online! Over **400** of them here in Denmark.

WebExtension	**94,000**.
Orbot	**8,000**.
Website	**4,000**.
Standalone	**4,000**.

Mahsa Amini situation in Iran

On 13th September 2022, Mahsa Amini, a 22-year-old Kurdish woman from the north-western city of Saqqez, visited Tehran with her family when she was arrested by morality police officers, who accused her of violating Iran's strict hijab rules.

Her family was told that she would be released after a "re-education session", but she died in custody three days later.

Mahsa Amini situation in Iran

OONI data shows new blocking events in Iran amid ongoing protests:

- Increased blocking of encrypted DNS.
- Blocking of WhatsApp and Instagram.
- Blocking of Google Play Store and Apple App Store.
- Blocking of Skype and Linkedin.

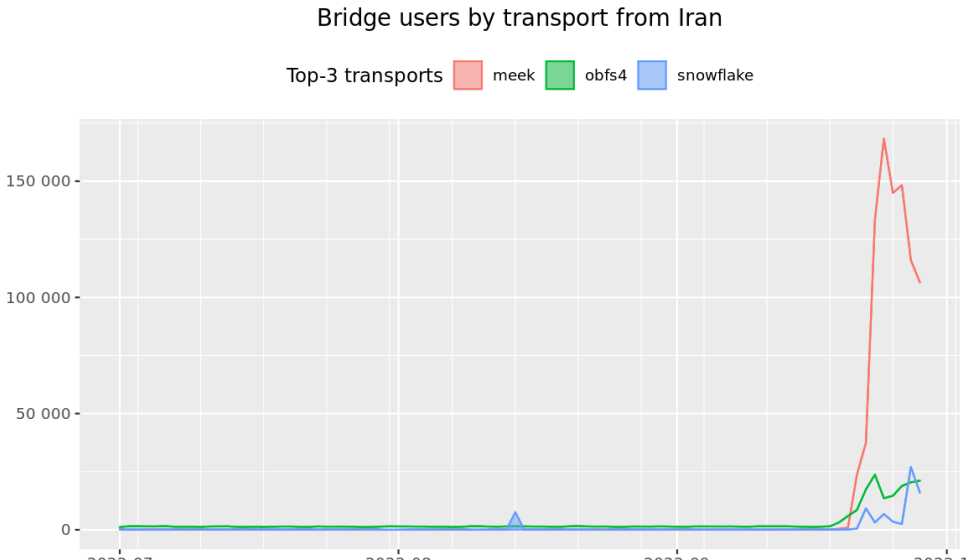
See OONI's report: Iran blocks social media, app stores and encrypted DNS amid Mahsa Amini protests

Mahsa Amini situation in Iran

In addition to the above blocks (and many other long-term blocks), Iran experienced multiple severe outages affecting mobile networks over the past week, which are visible in the IODA, Cloudflare Radar and Kentik datasets.

OONI data suggests that Psiphon and **Tor Snowflake work in Iran**, and can potentially be used for censorship circumvention. While our tests determine that it's possible to bootstrap these tools from Iran and use them to fetch a small webpage, we have no data regarding whether they are effective in providing circumvention for long periods of time.

Mahsa Amini situation in Iran



2023

- More attention to Onion Services.
- Hopefully, less DoS.
- VPN, Arti, CC, Conflux, and all the other things already mentioned.
- More hiring **:-)**

How can you help?

- Run a Tor relay, a bridge, or install the Snowflake browser extension!
- Teach others about Tor and privacy in general.
- Find, and maybe fix, bugs in Tor software.
- Test Tor on your platform of choice.
- Work on some of the many open research projects.
- Donate at donate.torproject.org

Questions?

ahf@torproject.org

@ahf@mastodon.social

@ahfaeroey

OpenPGP:
1C1B C007 A9F6 07AA 8152
C040 BEA7 B180 B149 1921