State of the Onion

Alexander Hansen Færøy

November 26, 2023

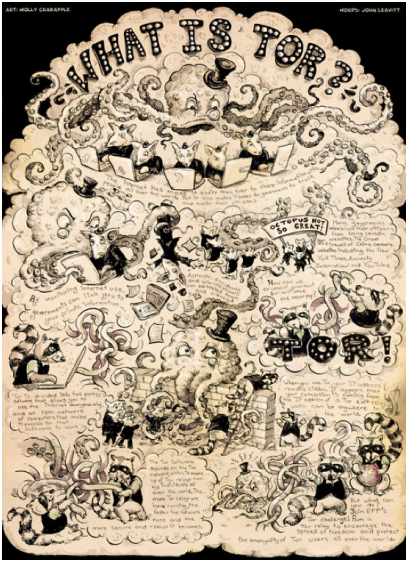
Cryptohagen

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.



Congestion Control

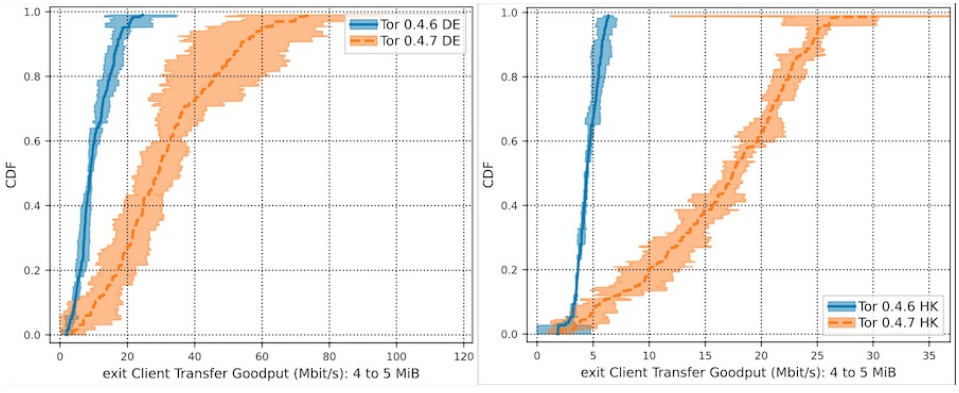
We implemented three congestion control algorithms: Tor-Westwood, Tor-Vegas, and Tor-NOLA. All of them are available in **Tor 0.4.7.**

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.**

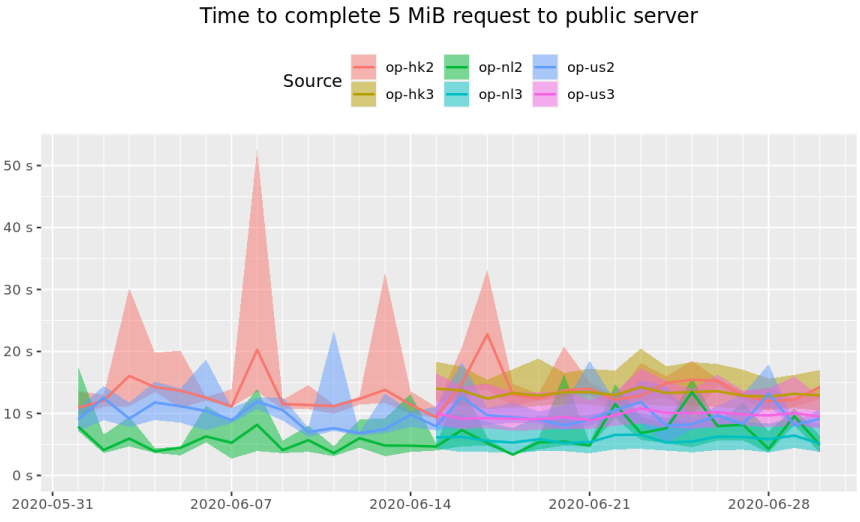


Congestion Control

Experimental algorithms have been removed from 0.4.8.x; Vegas left as the winner.

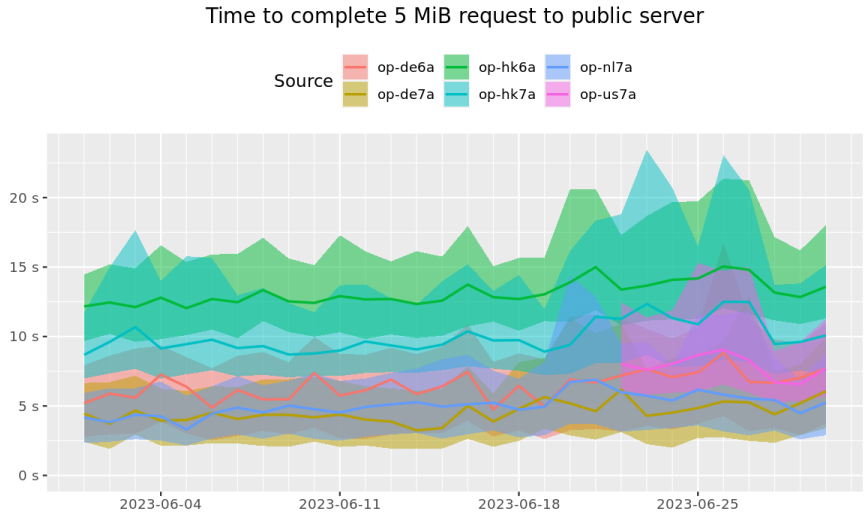
Continued tuning efforts will happen over time using consensus parameters.

Congestion Control



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

Congestion Control



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

A massive thank you for upgrading to Tor 0.4.8 so quickly!

Tor 0.4.9 may be a while!

Proof of Work for Onion Services

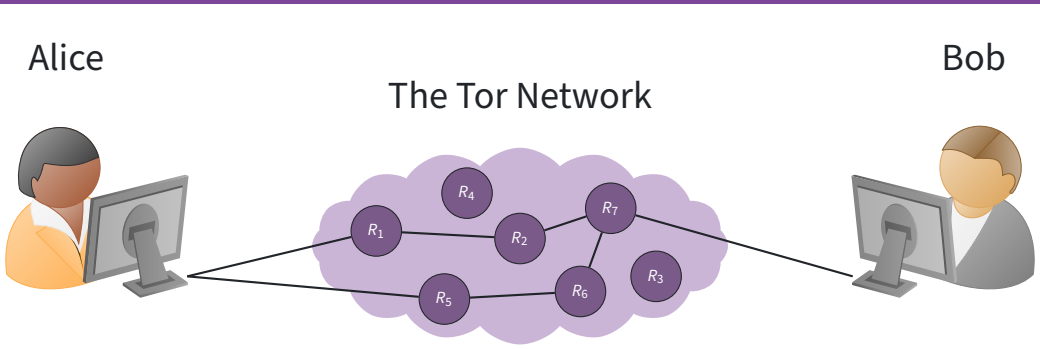
We implemented PoW for Onion Services that can dynamically enable, disable, and adjust the difficulty of the system if pathological situations appears.

Make the cost of attacking an Onion Service higher.

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

See Proposal #327. And as an Onion Services operator, here is how you can enable it: Community portal - Onion Services - DoS.

Conflux



Methodologies

Testing and tuning happens using a number of tools:

- Chutney
- Shadow

UDP

UDP, packed, and fragmented cells making progress.

Denial of Service

Multiple concurrent Denial of Service attacks significantly impacted the User Experience of the Tor ecosystem.

Funding for continued mitigation work when pathological situations arise. Work tracked under the Sponsor 112 and Denial of Service labels on Gitlab.

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

... we recently spend 2.5 people for almost 8 days for security auditing due to two Denial of Service issues ...

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 Relay!

Arti and Legacy Tor

Currently, **the majority 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.

Tracking Arti Engineering Efforts

All Arti development is free software and development happens in the public:

- Day-to-day development happens over IRC at **#tor-dev @ OFTC** and via Matrix **#tor-dev:matrix.org**.
- Gitlab is used for engineering work at gitlab.torproject.org/tpo/core/arti.
- We are encouraging contributions from upcoming Tor hackers! Rust knowledge useful – you will learn about Tor as you progress.

Tor Browser and Mullvad

Onionmasq and VPN Status

Tor Relay Operator Community

Tor is an open community

- Relay operators run the backbone infrastructure of the Tor network. Part of what makes the Tor network successful or unsuccessful is this community.
- Working to improve the health of this community improves the network as a whole.

Combating malicious relays

- Previously we talked about fighting bad relays by using tools, scanners, and the implementation of technical solutions. This is one strategy.
- Another strategy that we're working on is the community building/social approach: writing policies, meeting with operators, and helping to organize the relay operators community.
- It's harder to infiltrate in a more united community. Attackers will need to expend more effort.

Removing bad relays and adversaries

- Over the past years, we have seen adversaries trying some techniques to infiltrate the Tor community and pushing back on our community building work. For example, some accused us of trying to implement a Know Your Customer (KYC) process.
- This is absurd because we do not require or ask a copy of your passport, ID, legal name, home address, bank account, phone number, etc.
- However, as member of a community, an operator needs to be reachable, not only by the The Tor Project, but also to other members of this community.

Tor is a public network

Running a relay is an act of transparency (even though being a Tor user is an act of privacy), because the way to strengthen trust in relays is by having a stronger community."

There are many adversaries

But these two extreme positions aren’t helpful:

- Underestimating of the problem: "Everything is fine! Please don’t remove my super sketchy nodes, they are just happy relays."
- Overestimation of the problem: "The NSA/CIA is running Tor exit nodes, so let’s use this sketchy solution instead." This is an obvious tactic of FUD (Fear Uncertainty and Doubt).

Tor Relay Operators Policies and Processes

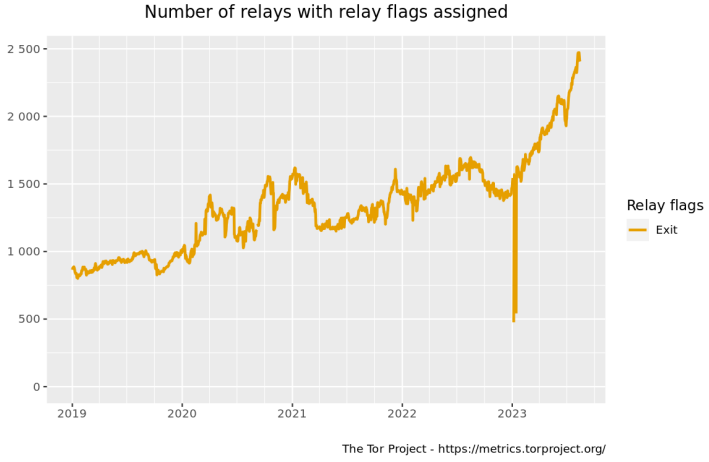
- We have started the process of improving the network health by calling on operators to submit proposals and ideas. Also we're collecting previous ideas that have been shared here and there.
- There is now a meta-policy explaining how proposals are to be submitted, approved and implemented in relay operators community.

Examples of Proposals

- Guidelines for maximum consensus weight fraction per Tor operator
- Allow limiting total consensus exit fraction by family
- Guidelines for conducting open source investigations when hunting malicious relays

Another Example

Bumping the limit relays per IPv4 from 2 to 4, 4 to 8 relays.



Join the Tor Relay Operator Community!

- tor-relays mailing list (main communication channel) - lists.torproject.org.
- Tor Forum: forum.torproject.org.
- Matrix/IRC: **tor-relays:matrix.org** or tor-relays @ irc.oftc.net.
- Regular online meetups announced on the tor-relays mailing list.
- Official docs: https://community.torproject.org/relay/
- Or if you can’t run a relay, please run a Tor snowflake proxy: https://snowflake.torproject.org.

- Metrics pipeline.
- Anti-censorship technology.
- Growing "the company."
- Bandwidth scanning.
- EFF Tor University Challenge.

Upcoming Relay Operator Events

Tor will be present at the following upcoming events in Europe:

- 37C3 in Hamburg (December, 2023).
- FOSDEM 2024 in Brussels (February, 2024).

Questions?

ahf@torproject.org

Signal: +1 (703) 420-1337

@ahf@mastodon.social

@ahfaeroey

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