Tor Relay Operators Meetup

Alexander Hansen Færøy

2025-12-30

39C3

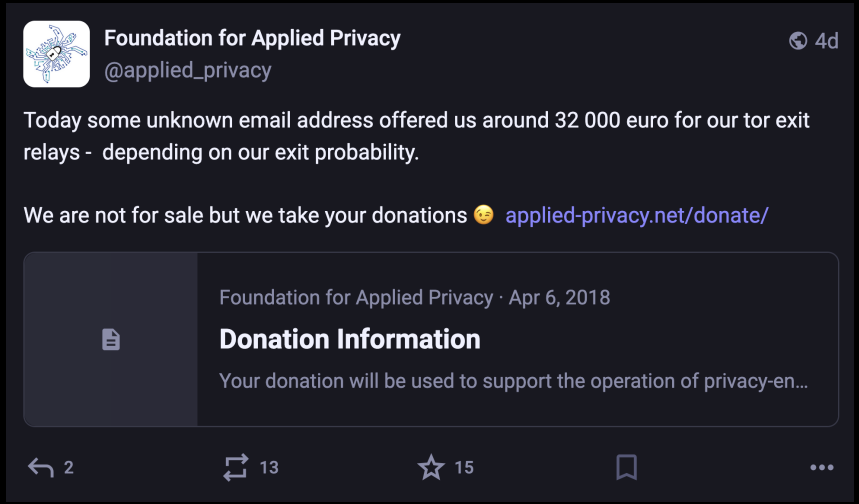
Updates

- Lots of updates to Tor Browser, Mullvad Browser, and Tails.
- Continued work on better anti-censorship technology.
- Continued development on replacing C Tor with Arti: flow control, conflux, onion services, relay, metrics, RPC, and resilience.
- New support portal at https://support.torproject.org/.
- 2025 User Survey.
- Growth and resilience of the organization.
- VPN Android App entered beta.

Post-Quantum Cryptography

- With the release of OpenSSL 3.5.0, we can now finally start seeing PQ in our TLS layer in Tor. This is the most important layer to upgrade for this specific use-case. Big thanks to the OpenSSL team here!
- Supported in the Arti layer too via some of the crypto providers we support there.
- BoringSSL integration not needed anymore. Phew.
- Debian 13 (Trixie) got OpenSSL 3.5.0 in before the release freeze. Big thanks to Kurt Roeckx!
- But what about LibreSSL?

Network Health



Context and problem: Old family system is causing us trouble:

- Poor UX for Relay Operators: Each time they add a new relay, they need to update all their other relays with information about the new relay.

  This issue is fortunately largely mitigated by our relay operators using various shared tooling for configuration management.

- Our relay operators are really good at what they are doing. They seem to have a lot of resources, and a lot of computation power. This leads to them being hungry to run more and more relays as network bandwidth and computation power increases.

- Unfortunately, the C implementation of Tor doesn't scale very well with modern multi-core CPU's. This leads to people running multiple instances of C Tor per computer.

  The Network Team believes Arti will solve this, and it's one of the many reasons we are currently working on Project 141 (Arti Relays).

- Memory and storage space size issues (particularly bad for Apple iOS users):

  23.58 MB of cached micro descriptors consists of 19.29 MB (82%) family info.

Context and problem: Old family system is causing us trouble:

- Because of many requests from our relay community, we decided to allow more relays per IP. This is generally good for the network, but it made our space issues more problematic due to $O(n^2)$ behaviour of our current family system.

  Timeline:

  2023-01-31 AuthDirMaxServersPerAddr was bumped from 2 to 4 relays per IP.

  2023-06-28 AuthDirMaxServersPerAddr was bumped from 4 to 8 relays per IP.

Solution: Proposal 321: Better performance and usability for MyFamily

- Proposal written by Nick Mathewson during 2020 as part of the work on ”Walking Onions”.
- Gives each relay operator a new identity key: the family identity key.

  This key gives us some new opportunities: we can now both validate ownership of an individual relay, but also a set of relays (a family).
- Makes analysis work a lot easier: you already have a 256-bit public key that you can use for “group by”-like operations on relay data.

  Before this, we would have to build a set of relays from the family value, add the relay ID itself, and hash the set together to create a “group by” identifier.
- But Network Team, when can we have this shiny new piece of technology?

  Happy Families got implemented in 2025-Q1:

  - Arti 1.4.1 (released 3rd of March, 2025);
  - C Tor 0.4.9.2-alpha (released 2nd of April, 2025).

  See also: https://blog.torproject.org/happy-families/

Counter Galois Onion

- Enhancing Tor's relay encryption to prevent a number of problems:

  Problem 1: Tagging attacks.

  Problem 2: Forward secrecy begins when a circuit closes.

  Problem 3: Insufficient 4-byte authentication tag.

- Research carried out by Jean Paul Degabriele, Alessandro Melloni, Jean-Pierre Münch, and Martijn Stam.

- Supported in both Arti and C Tor.

See also: https://blog.torproject.org/introducing-cgo/

Stronger Padding

- A couple of years ago, we introduced the Web Traffic Fingerprinting (WTF) padding framework as part of our C Tor development cycle to mitigate attacks where an observer can identify some HTTP flows happening in an encrypted data stream.
- VPN providers are starting to be interested in this problem space as well, which benefits Tor.
- We integrated the MaybeNot Rust framework (https://github.com/maybenot-io/maybenot) in Arti. This work is developed by Tobias Pulls.
- Arti-only and will remain that way. There are no good alternatives to MaybeNot for C Tor without embedding Rust into C Tor.

Threat Model Update: Proposal 344

- Mike Perry published Proposal 344: Information Leak Hazards for Tor Implementations.
- Revisiting the old Tor Threat Model: The world is different today than it was when Tor got out.
- Main gaps: Internal Covert Channel Vectors, Zero-Click Behavior Manipulation Primitives, and Augmented Observation Primitives.
- We conducted an audit of Arti to look for protocol leaks and fixed a number of issues in our protocol state machines.
- This proposal gives us internally in Tor, and our community, a helping hand when it comes to prioritize problems. This is often a source of frustration in our community where some people think all issues are equal.
- See State of the Onion or wait the upcoming blog post on this topic.

Arti Relay

The work to build a relay implementation continues.

- Directory Authority support.
- Core Relay functionality (guard, middle, exit, and bridges).
- Performance analysis and simulation.
- Testing.

Tor Community Gathering in Denmark

- Took place at Hylkedam from 2025-10-03 to 2025-10-05.
- We were around 16 participants from SE, US, IT, NL, DE, and DK.
- Not funded by ”Tor Project, Inc.”, but everybody pooled together for rental of the space and food. Cost ended up around 170 EUR per person (excluding traveling of course).
- Managed to cover a lot of different topics related to the Tor community spaces.
- Will happen again in 2026 and we are looking at building something similar to Mozilla’s Mozfest concept at a bigger venue in late 2026.
- See more: https://tcg2025.4711.se/
- Upcoming event likely around 2026-03-13 to 2026-03-16.

2026

- Recent Arti release blog posts are mentioning ORPort support. Once this is starting to work, we will be unblocked on test network, performance analysis, etc.
- Continued work on client integration of Arti with Tails and Tor Browser.
- 3rd party integration of Arti: Building a development ecosystem for others to build safe, censorship resistant, anonymous communication in their software.
- Paying attention to some of the community efforts: stateless relays, TPM usage, transparency logs, etc.
- Navigating a chaotic world...

Questions?

Email: ahf@torproject.org

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

Mastodon: @ahf@mastodon.social

Bluesky: @ahf.me