State of the Onion

Alexander Hansen Færøy

November 24, 2024

Cryptohagen

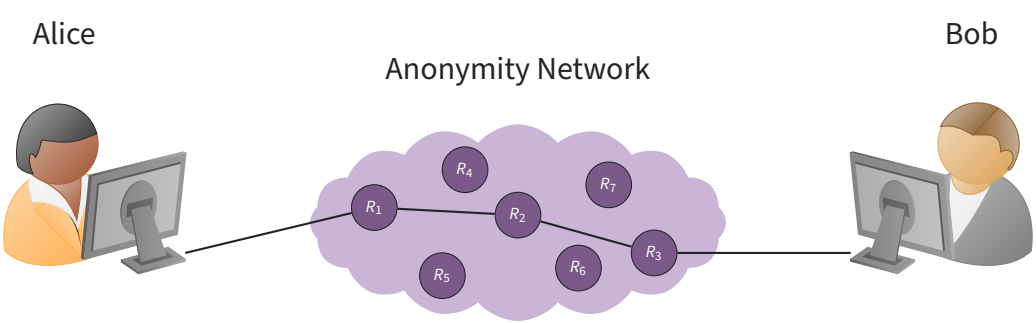
About Me

- 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.

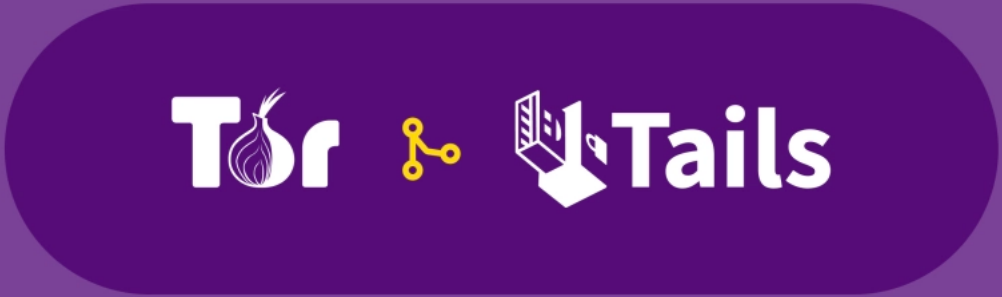
What is Tor?

- 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 with 69 members of staff.

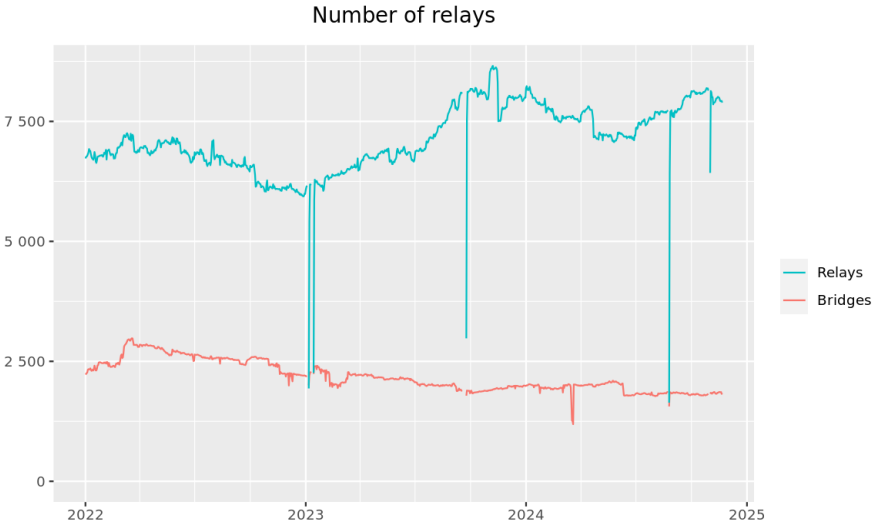
Threat Model



What can the attacker do?

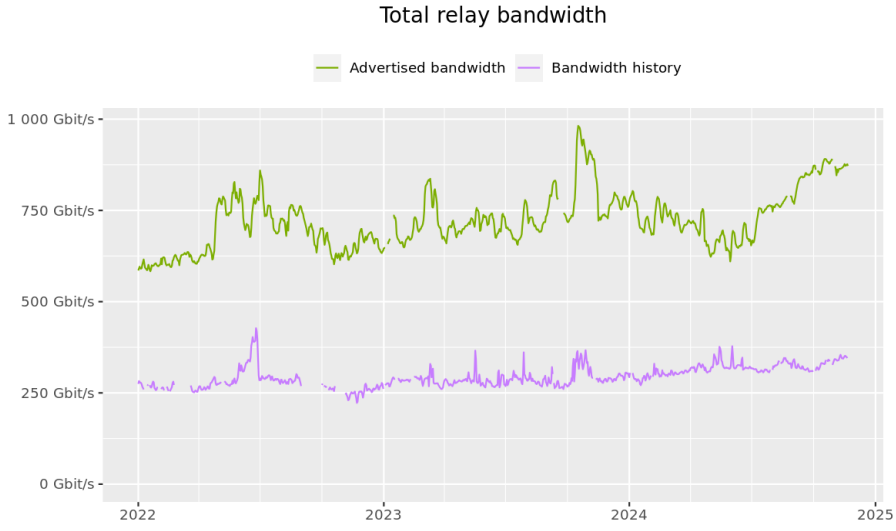

Tor
Tails

Network Size



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

Network Size



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

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 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.

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.

What is Arti?

- Standalone application (SOCKS proxy)

```
$ arti proxy

 INFO arti::subcommands::proxy:  Starting Arti 1.3.0 in
    SOCKS
 proxy mode on localhost port 9150 ...
```

What is Arti?

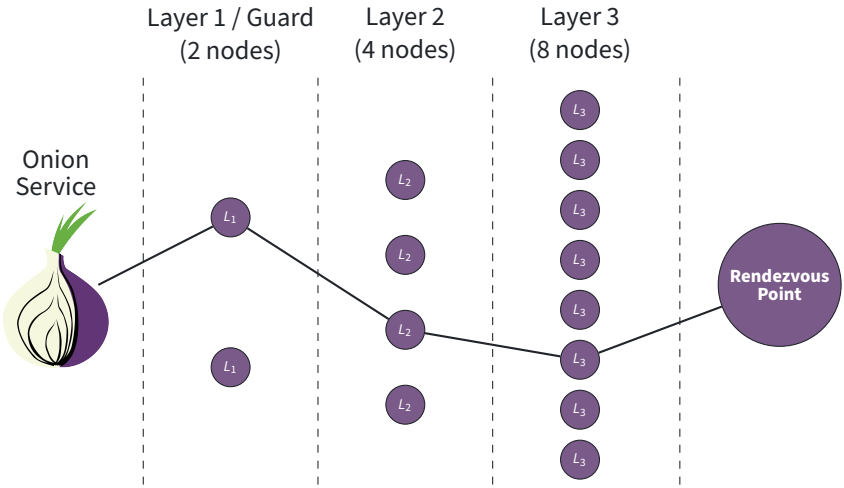
- Standalone application (SOCKS proxy)
- Embeddable library

```
// Initiate a connection over Tor to example.com, port 80.
let mut stream = tor_client.connect(("example.com", 80)).
    await?;

// Write out an HTTP request.
stream
    .write_all(b"GET / HTTP/1.1\r\nHost: example.com\r\n\r
        \n")
    .await?;
stream.flush().await?;

// Read and print the result.
let mut buf = Vec::new();
stream.read_to_end(&mut buf).await?;

println!("{}", String::from_utf8_lossy(&buf));
```

2024 Progress Update

- Onion Services development
- Progress on RPC system
- Started work on adding relay support to Arti
- Many less visible changes, bug fixes, and quality of life improvements

Security features: Vanguards

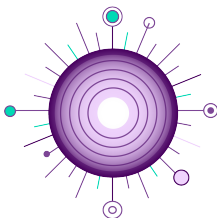


blog.torproject.org/announcing-vanguards-for-arti

DoS mitigations: memory DoS resistance

Arti's new subsystem for **preventing memory DoS**

- Tracks memory consumption for each stream and circuit
- Tracks total memory consumption for all streams and circuits.
- Tracks the age of data on streams and circuits.
- Kills streams and circuits if low on memory, starting with the ones with the oldest data



DoS mitigations: Proof of Work

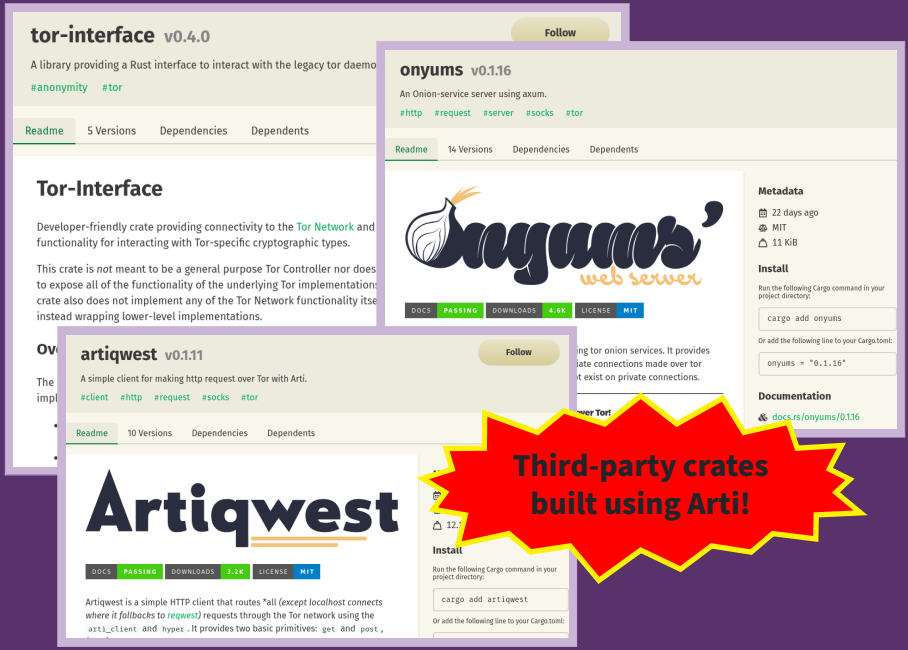
Experimental client-side **Proof of Work** support

- Clients have to solve a puzzle before they can connect to onion services using PoW
- **Not** a captcha
- Increases the cost of attacking Onion Services

blog.torproject.org/introducing-proof-of-work-defense-for-onion-services

RPC subsystem developments

- Well-defined encoding inspired by JSON-RPC (but we may define other encodings in the future)
- Capability-based: privilege separation, app isolation
- Library support
- Currently under heavy development


tor-interface v0.4.0
Follow
A library providing a Rust interface to interact with the legacy tor daemo
#anonymity #tor
Readme 5 Versions Dependencies Dependents
Tor-Interface
Developer-friendly crate providing connectivity to the Tor Network and
functionality for interacting with Tor-specific cryptographic types.
This crate is not meant to be a general purpose Tor Controller nor does
to expose all of the functionality of the underlying Tor implementations
crate also does not implement any of the Tor Network functionality itse
instead wrapping lower-level implementations.
onyums v0.1.16
An Onion-service server using axum.
#http #request #server #socks #tor
Readme 14 Versions Dependencies Dependents
onyums'
web server
DOCS PASSING DOWNLOADS 4.6K LICENSE MIT
Metadata
22 days ago
MIT
11 KiB
Install
Run the following Cargo command in your project directory:
cargo add onyums
Or add the following line to your Cargo.toml:
onyums = "0.1.16"
Documentation
docs.rs/onyums/0.1.16
artiqwest v0.1.11
Follow
A simple client for making http request over Tor with Arti.
#client #http #request #socks #tor
Readme 10 Versions Dependencies Dependents
Artiqwest
DOCS PASSING DOWNLOADS 3.2K LICENSE MIT
Artiqwest is a simple HTTP client that routes *all (except localhost connects
where it fallbacks to reqwest) requests through the Tor network using the
arti_client and hyper. It provides two basic primitives: get and post,
Install
Run the following Cargo command in your project directory:
cargo add artiqwest
Or add the following line to your Cargo.toml:
Third-party crates
built using Arti!

Arti Relay

The work to build a relay implementation has begun.

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

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.

Here is where **you** come in

We need your help!

- Have you built something using **Arti**? We'd love to hear about it!
- Try out **arti**, or the **arti-client** crate
- Open source contributions (code, docs, etc.)
- Bug reports, feature requests, feedback on our APIs

Protocol Work

- (344) Prioritizing Protocol Information Leaks in Tor.
- (347) Domain separation for certificate signing keys.
- (353) Requiring secure relay identities in EXTEND2.

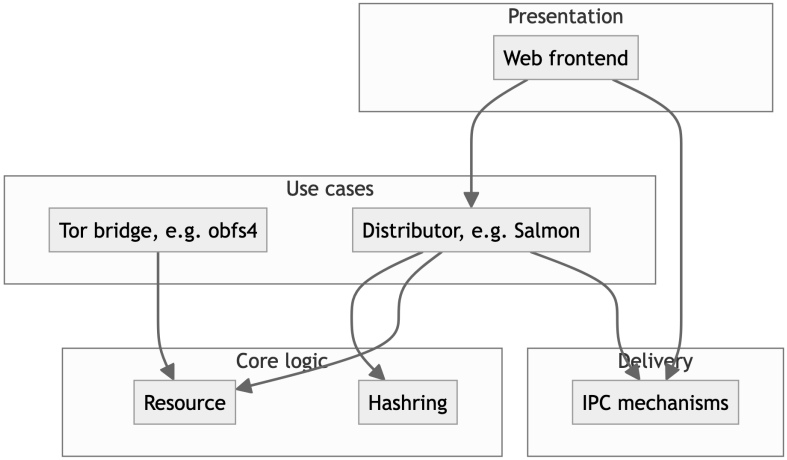
spec.torproject.org

Onionmasq and VPN Status!

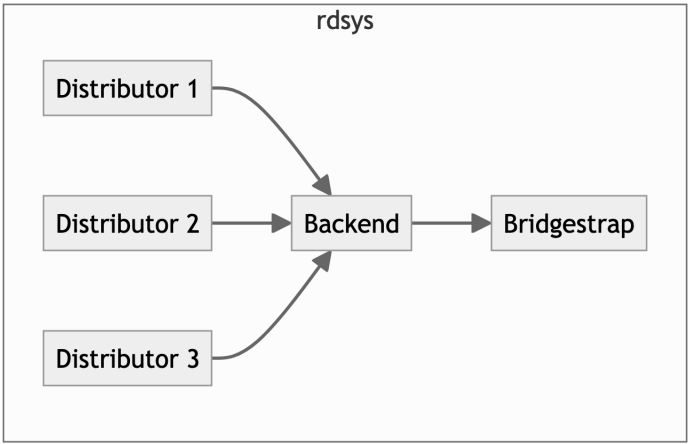
Anti-censorship Status

- Snowflake Status.
- Russia.

Bridge Distribution and rdsys



Bridge Distribution and rdsys



WebTunnel Pluggable Transport

WebTunnel is a censorship-resistant pluggable transport designed to mimic encrypted web traffic (HTTPS) inspired by HTTPT. It works by wrapping the payload connection into a WebSocket-like HTTPS connection, appearing to network observers as an ordinary HTTPS (WebSocket) connection.

For an onlooker without the knowledge of the hidden path, it just looks like a regular HTTP connection to a webpage server giving the impression that the user is simply browsing the web.

Upcoming Tor Events

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

- 38C3 in Hamburg (December, 2024).
- FOSDEM in Brussels (February, 2025).
- BornHack in Gelsted (July, 2025).
- What Hackers Yearn 2025 in Geestmerambacht (August, 2025).
- 39C3 in Hamburg (December, 2025).

2025

- Continue the strategy to move to Arti everywhere.
- Continue work on anti-DoS.

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

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

Signal: +1 (703) 420-1337

@ahf@mastodon.social

@ahf.me