Anonymity Loves Resilience: The Case of Tor

Georg Koppen Alexander Hansen Færøy

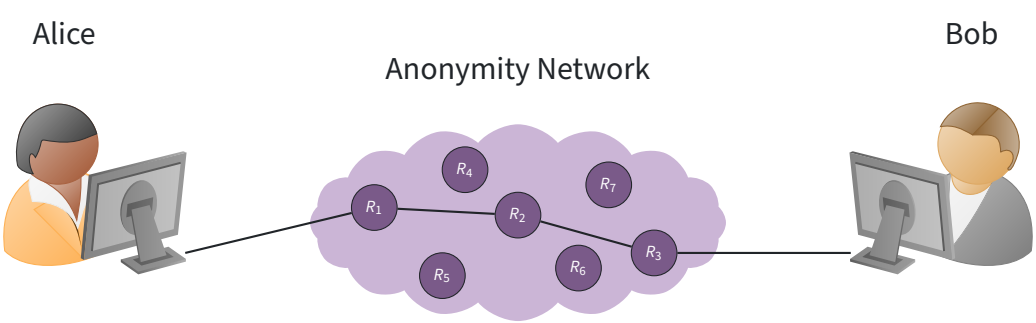
April 14, 2025

FOSS North 2025

What is Tor?

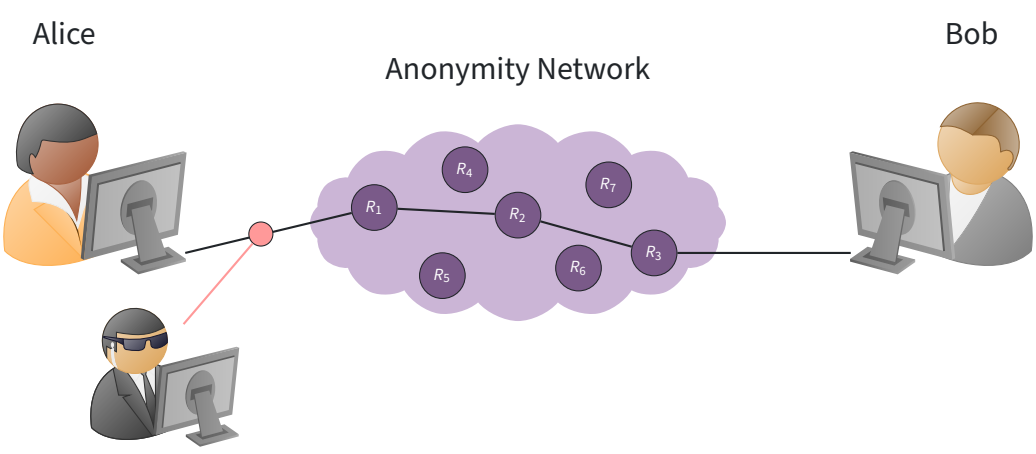
- Online anonymity, and censorship circumvention.
  - Free software.
  - Open network.
  - Open specifications.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.

Threat Model

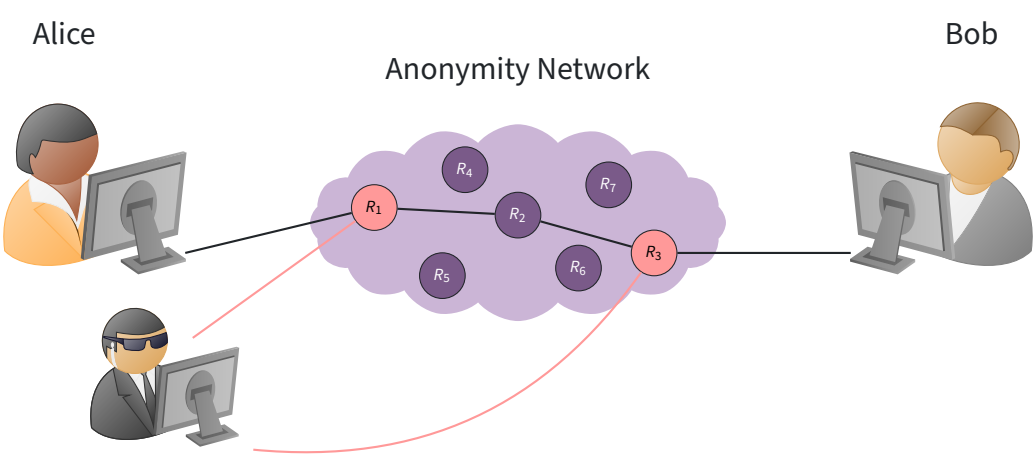


What can the attacker do?

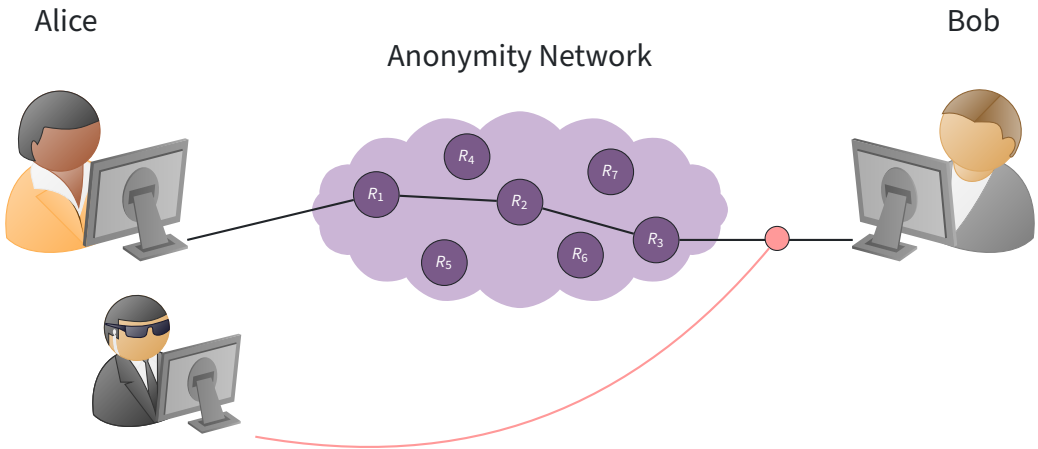
Threat Model



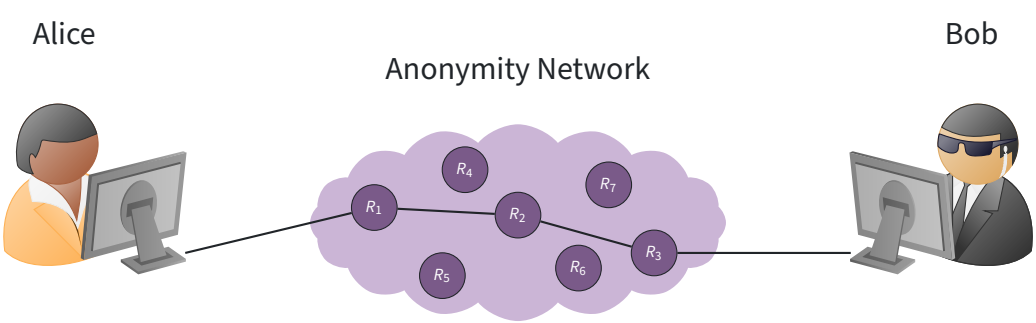
Threat Model



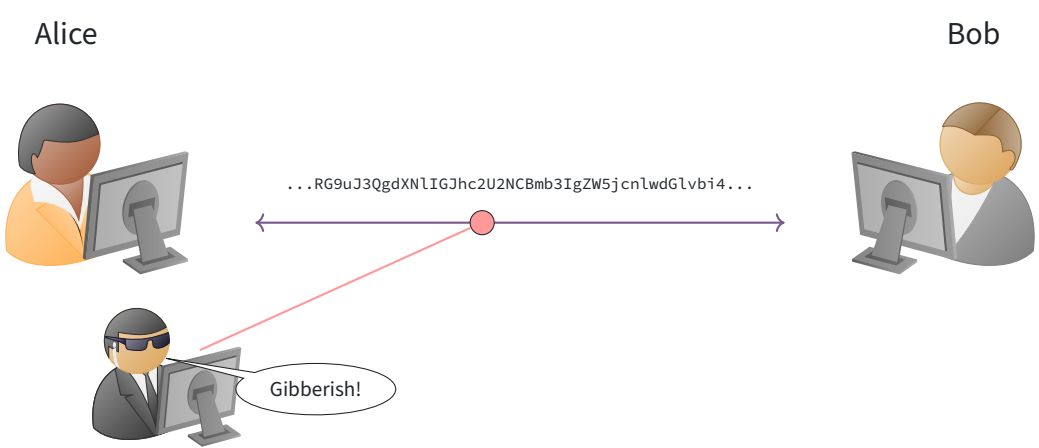
Threat Model



Threat Model



Anonymity isn’t Encryption

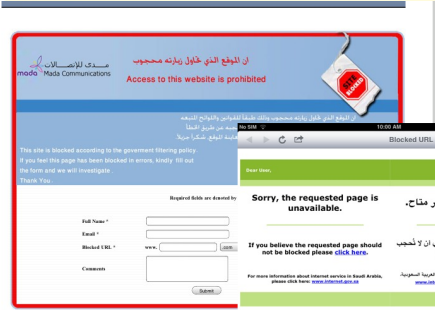


Encryption just protects contents.

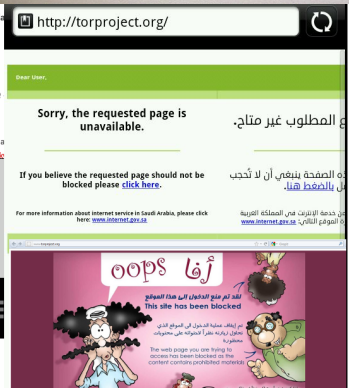

يالله بالستر ...!
تصفح بأمان!
عذراً، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الانترنت وسيلة لتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي تريد بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.
إذا كانت لديك وجهة نظر مختلفة، الرجاء النقر هنا.
Surf Safely!
This website is not accessible in the UAE.
The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates.
If you believe the website you are trying to access does not contain any such content, please click here.
© 2009 zammitcre FZ LLC.


خطر!
تصفح بأمان!
تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي تريد بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.
إذا كانت لديك وجهة نظر مختلفة، الرجاء النقر هنا.
Surf Safely!
This website is not accessible in the UAE.
BOMB
Site is now TRUSTED


هذا الموقع محظور
This site is blocked
الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.
إذا كنت ترغب في إضافة النظر في تصنيف هذا الموقع، يرجى التفضل بتعبئة استمارة الملاحظات
If you would like the classification on this site to be reviewed, please fill in and submit the Feedback Fo


Access Denied
our request was denied because of its content categorization: "Computers/Internet;Proxy Avoida


عزيزي العميل : تم حجب هذا الموقع بناء على القوانين والقوانين
بأن هناك خطأ يرجى إرسال رسالة على البريد الالكتروني unblock.kw@kw.zain.com مع ذكر عنوان الموقع الذي تم حجبه.
Dear Customer: This site has
categorizing this site, please


http://torproject.org/
Dear User,
Sorry, the requested page is unavailable.
If you believe the requested page should not be blocked please click here.
For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa
عزيزي المستخدم،
عفواً، الموقع المطلوب غير متاح.
إذا كنت ترى أن هذه الصفحة ينبغي أن لا تُحجب تفضل بالضغط هنا.
مزيد من المعلومات عن خدمة الإنترنت في المملكة العربية السعودية: www.internet.gov.sa

مدى للاتصالات
mada Mada Communications
ان الموقع الذي حاول زيارته محجوب
Access to this website is prohibited
This site is blocked according to the government filtering policy.
If you feel this page has been blocked in errors, kindly fill out the form and we will investigate.
Thank You
Required fields are denoted by
Full Name *
Email *
Blocked URL *
Comments
Submit

9:28 AM
Site Blocke...
http://torproject.org/
Dear User,
Site Blocked
This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.
If you believe the requested page should Not be blocked please click here.
الموقع محظور
هذا الموقع مغلق لمخالفته الأنظمة والقوانين في مملكة البحرين.
إذ كنت ترى أن هذه الصفحة ينبغي أن لا تحجب تفضل بالضغط هنا.

oops! أوقا
This site has been blocked
The web page you are trying to access has been blocked as the content contains prohibited materials

Du var på vej ind på en ulovlig hjemmeside

Vi vil meget gerne hjælpe dig med at finde den film eller serie, du søger.

Søg med FilmFinder →

Hvis du er på udkig efter musik, bøger eller møbler

Gå til SHARE WITH CARE →

SHARE WITH CARE

Hjemmesiden er blevet blokeret, fordi den er dømt ulovlig ved en dansk domstol. Brug Share With Care til at finde det, du leder efter, lovligt. På den måde passer du både på dig selv og på kulturen. **Læs mere om Share With Care**

Metadata

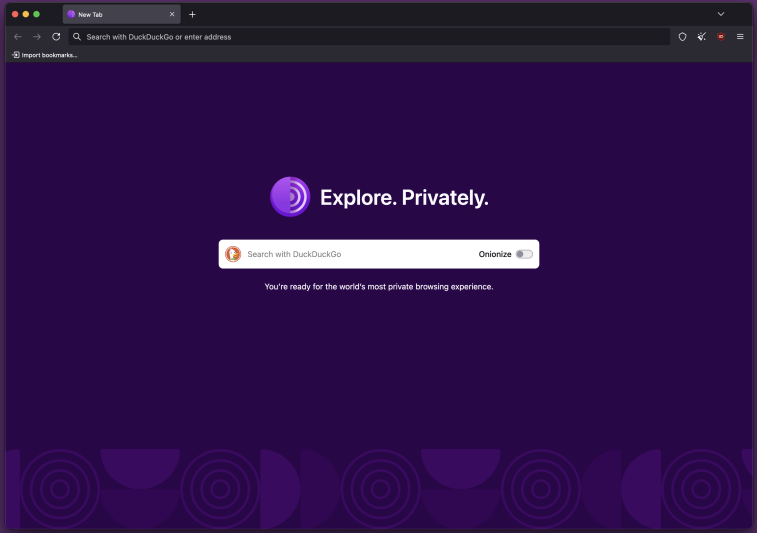
"We Kill People Based on Metadata."

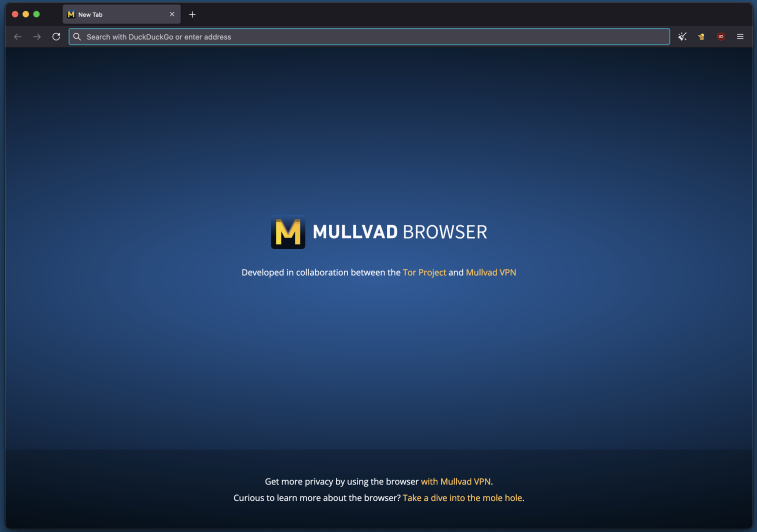
—Michael Hayden, former director of the NSA.

Unfortunately, network anonymity is often not enough on its own.

Application-specific integration and protection is often needed to ensure a more uniform fingerprint of the application's users.

Tails is our live operating system project that gives you a stateless operating system that uses Tor by default to access the internet.


New Tab
Search with DuckDuckGo or enter address
import bookmarks...
Explore. Privately.
Search with DuckDuckGo
Onionize
You're ready for the world's most private browsing experience.


New Tab
Search with DuckDuckGo or enter address
MULLVAD BROWSER
Developed in collaboration between the Tor Project and Mullvad VPN
Get more privacy by using the browser with Mullvad VPN.
Curious to learn more about the browser? Take a dive into the mole hole.

Building a Community and an Ecosystem

But the Tor application ecosystem is larger than just "browsing". Onion Services is an important piece of the ecosystem too.

OnionShare is used for easy, anonymous, file-sharing.

SecureDrop is used for source and whilsteblower handling in various media settings.

We host our own Onion Services, including our Debian mirror, too. See onion.torproject.org for more information.

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.

Development Process

Development work takes place via IRC/Matrix on various public channels on the OFTC IRC network.

All development happens in our self-hosted Gitlab instance at gitlab.torproject.org.

Anonymous ticket interaction is available via anonticket.torproject.org.

Effective collaboration tooling, such as audio/video meetings, was adopted during the 2020-2022 period.

Protocol Specification Process

We have our own process for handling protocol changes over time. Work begins as a proposal and ends as part of a specification.

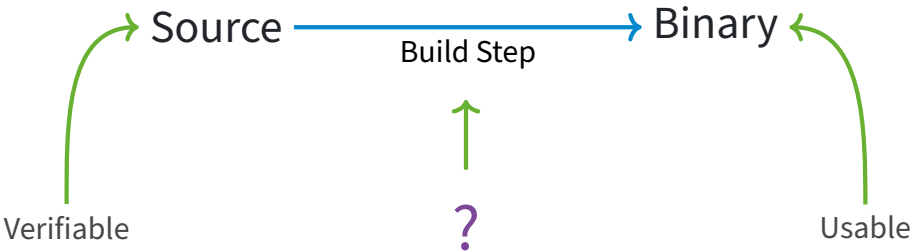
Specification work largely happens in gitlab.torproject.org/tpo/core/torspec.

Protocol specifications can be found on spec.torproject.org, but discussions often take place on the tor-dev mailing list.

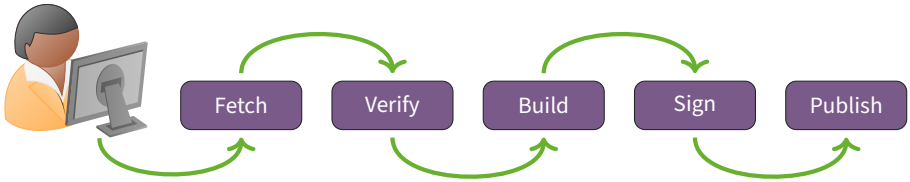
We heavily depend upon feedback from both community and the greater Tor research community.

Reproducible Builds

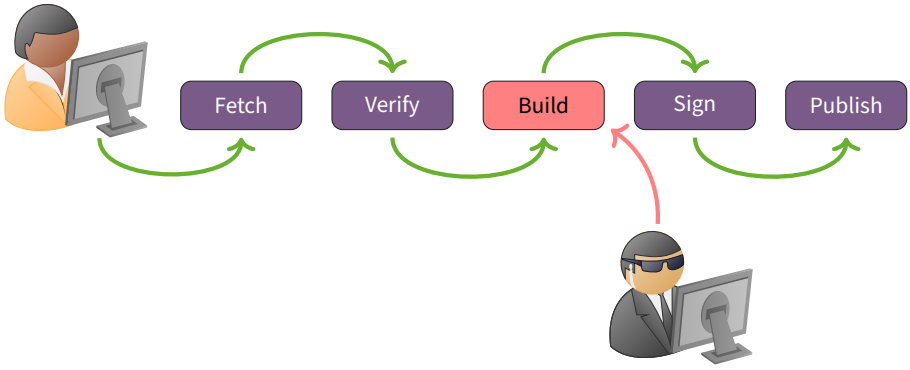
Reproducible Builds



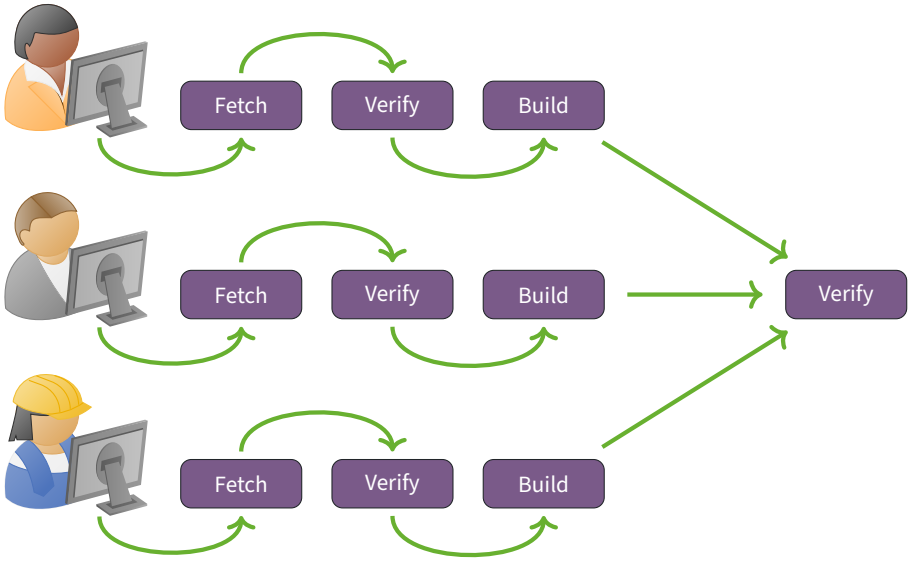
Build Process



Build Process



Build Process



Reproducible Releases

For the Tor component of our software stack, we also build our source tarballs reproducibly.

Requires at least 2 out of 3 release engineers + CI to be able to do a release.

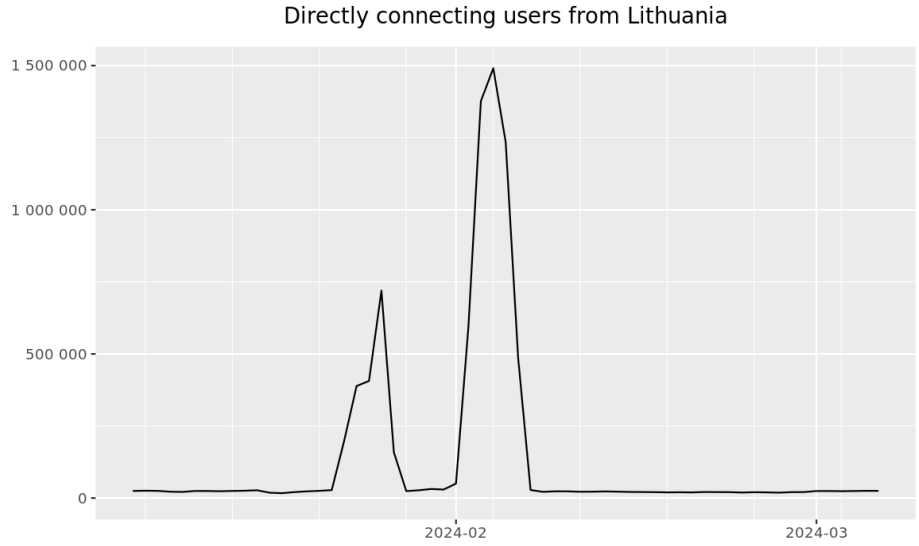
Same hash generated from multiple people allows us to have multiple people signing our releases using PGP.

Tor network resilience - Overview

What do we mean when we talk about network resilience?

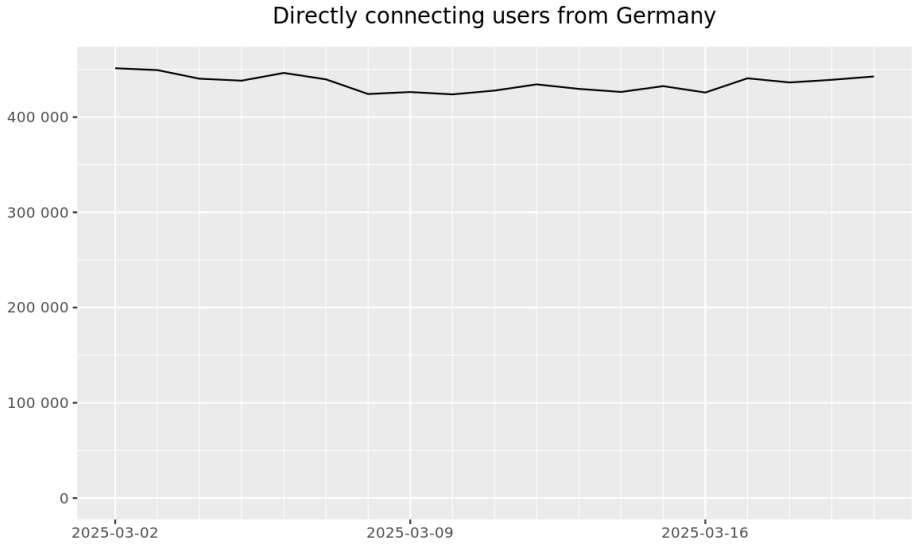
- the Tor network is not going down or getting unreliable in the face of potential disruptions
  - when is the Tor network behaving "normal"?
  - potential disruptions have to be detected quickly (pre-emptively)
  - disruptions need to get mitigated early on
- the Tor network is diverse
  - distributed trust
  - diverse set of relay operators
  - diverse set of relay locations (operating systems etc.)

Tor network resilience - Disruptions



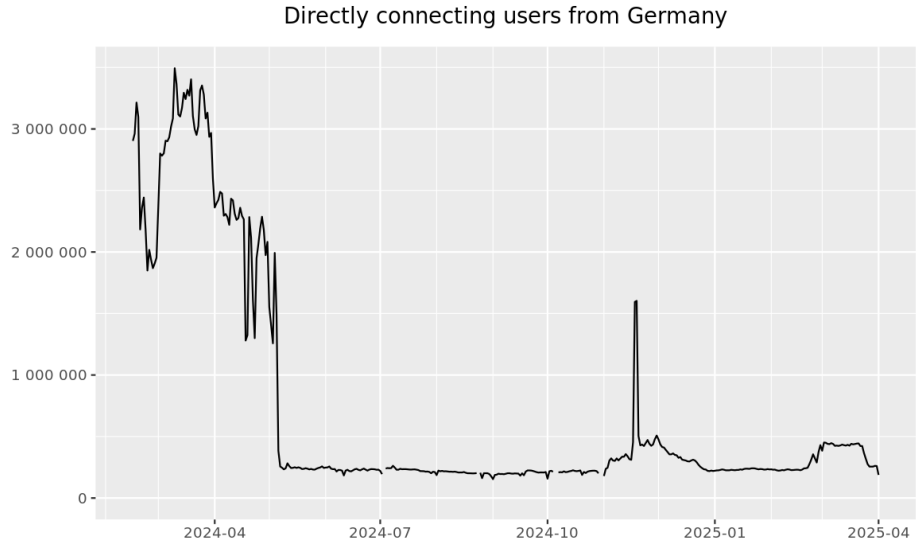
The Tor Project - https://metrics.torproject.org/

Tor network resilience - Disruptions



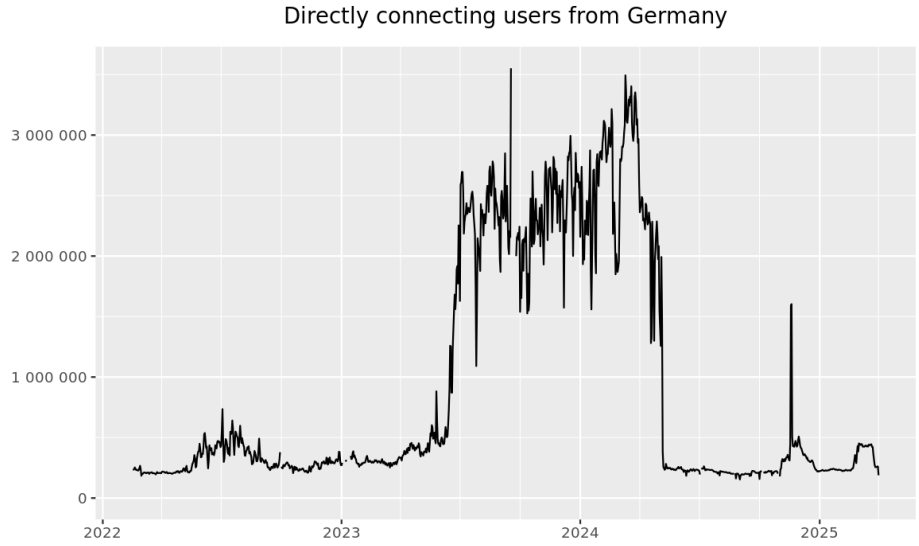
The Tor Project - https://metrics.torproject.org/

Tor network resilience - Disruptions



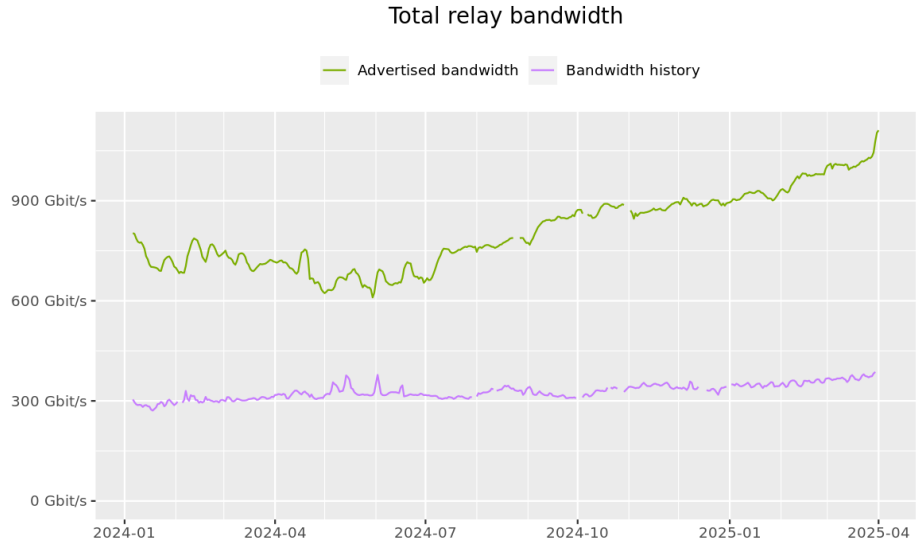
The Tor Project - https://metrics.torproject.org/

Tor network resilience - Disruptions



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

Tor network resilience - Disruptions



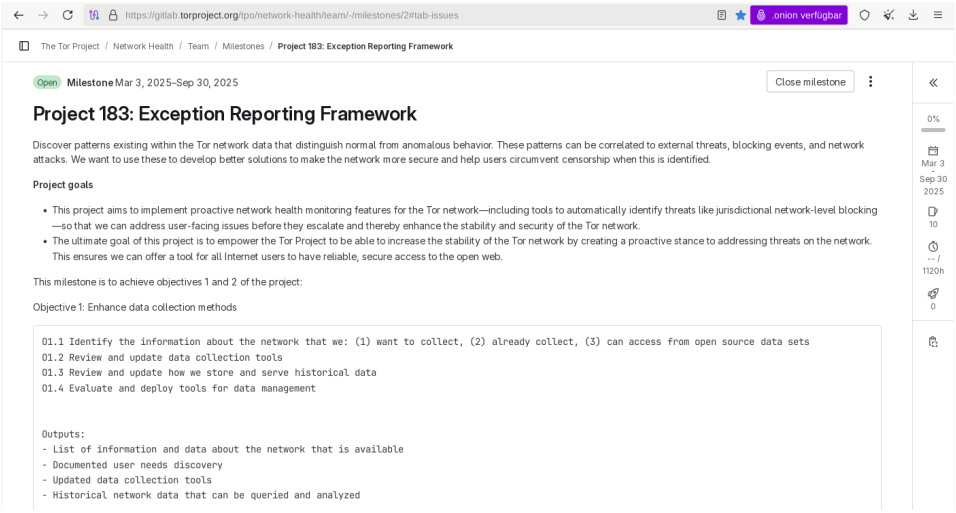
The Tor Project - https://metrics.torproject.org/

Tor network resilience - Disruptions

Exception Reporting Framework - Analysis:

- powered by "sensors" in the network doing data collection
- establishment of baseline metrics
- anomaly analysis and reporting
- categorization according to profiles of past incidents

Tor network resilience - Disruptions



Exception Reporting Framework milestone

Tor network resilience - Disruptions

Exception Reporting Framework - Mitigations:

- the network-health team sits at the center of coordinating the mitigations
- other stakeholders need to get included (network, community, bad-relay teams, potentially Directory Authorities)
- evaluation of responses and mitigation strategy

Tor network resilience - Distributed trust

Relay Search

flag:authority

flag:authority

Show 10 entries

Nickname†	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
faravahar (1)	8 MiB/s	6d 19h		216.218.219.41	2001:470:164:2::2		v3	443	80	Relay
dannenberg (1)	100 KiB/s	38d 15m		193.23.244.244	2001:678:558:1000::244		v3	443	80	Relay
Serge (3)	100 KiB/s	1d 20h		66.111.2.131	2610:1c0:0:5::131		v3	9001	9030	Relay
dizum (1)	88 KiB/s	12d 5h		45.66.35.11	2a09:61c0::1337		v3	443	80	Relay
tor26 (1)	75 KiB/s	4d 3h		217.196.147.77	2a02:16a8:662:2203::1		v3	443	80	Relay
bastet (1)	50 KiB/s	6d 11h		204.13.164.118	2620:13:4000:6000::1000:118		v3	443	80	Relay
maatuska (3)	50 KiB/s	4d 23h		171.25.193.9	2001:67c:289c::9		v3	80	443	Relay
moria1 (1)	40 KiB/s	6d 17h		128.31.0.39	-			9201	9231	Relay
gabelmoo (1)	40 KiB/s	4d 22h		131.188.40.189	2001:638:a000:4140::ffff:189		v3	443	80	Relay
longclaw (1)	38 KiB/s	1d 23h		199.58.81.140	-			443	80	Relay

https://metrics.torproject.org/rs.html#search/flag:authority

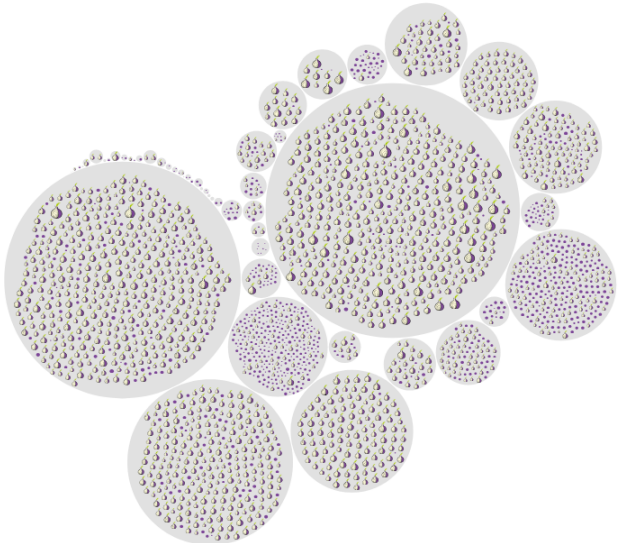
Tor network resilience - Distributed trust

The 9 Directory Authorities make and maintain the consensus which involves:

1. Keeping the service *available*.
2. Being *responsive* as an operator.
3. Having *integrity*.
4. Balancing maximizing network capacity and excluding *bad relays*.

More details can be found in the Directory Authority expectations document.

Tor network resilience - Diversity



54 countries with 2454 exits (2330 visible)
2025-04-11 12:00:00

Tor network resilience - Diversity

Research question: How do we tune the diversity dial for maximum network resilience?

- How should we measure diversity?
- Do we have some reasonable baselines?
- Should we focus on operator diversity or relay country diversity or...?

We start working on answers during our exception reporting framework project and continue afterwards.

Tor network resilience - Diversity

We help the relay operator community helping the network by:

- outlining relay operator expectations
- providing a proposal process for network-health improvements with relay operators as key stakeholders
- holding regular relay operator meet-ups (virtual and in-person)
- encouraging interaction *within* the operator community

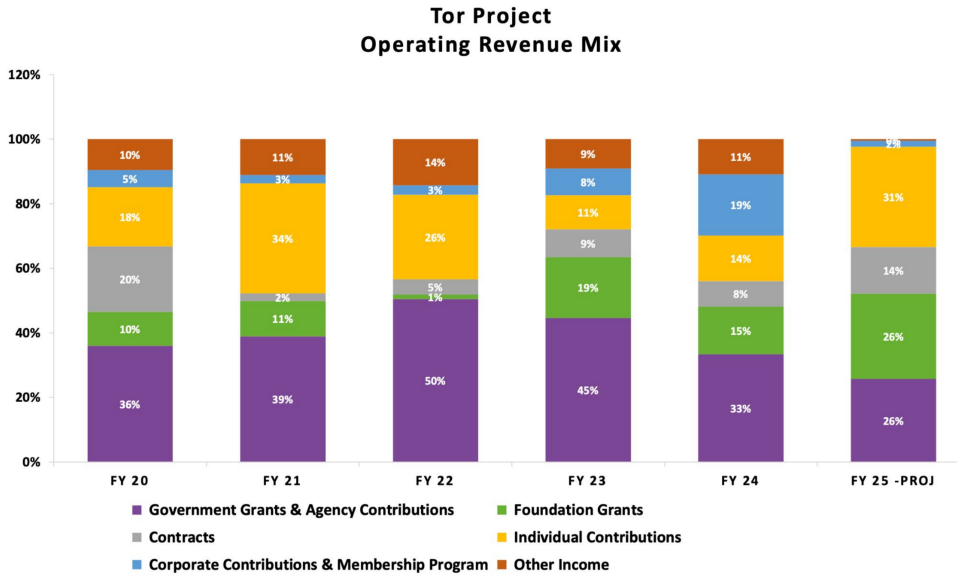
For the relay operator expectations, see:
https://community.torproject.org/policies/relays/expectations-for-relay-operators/

Tor project resilience

Resilience measures, which we already talked about in a software/code and community context, apply to the project itself as well:

- Diversity
- Openness and Transparency
- Community-building
- Trust

Tor project resilience - Funding



Tor project resilience - Funding

As a 501(c)(3) non-profit organization we are committed to financial transparency via:

- financial audit reports
- IRS 990 forms

Those transparency documents can be found on https://www.torproject.org/about/reports/.

Tor project resilience - Funding

There are indirect threats for non-profits to (funding) security as well:

- "foreign agent"-style laws around the world
- "nonprofit killer" plans in the US (aka bill H.R. 9495) (see: https://theintercept.com/2024/11/15/nonprofits-trump-bill-gop-republicans/)

Tor is not affected by those threats yet but we need to be wary and prepare for scenarios like that.

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.

Questions?