Network Anonymity with Tor

Alexander Færøy

March 11, 2020

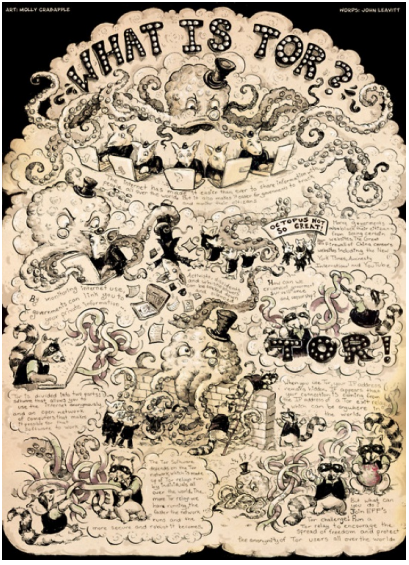
University College Lillebaelt

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.
- Worked with distributed systems in the Erlang programming language, WebKit-based mobile browsers, embedded development, and software development consulting.
- Co-organizing the annual Danish hacker festival BornHack on Funen.

What is Tor?

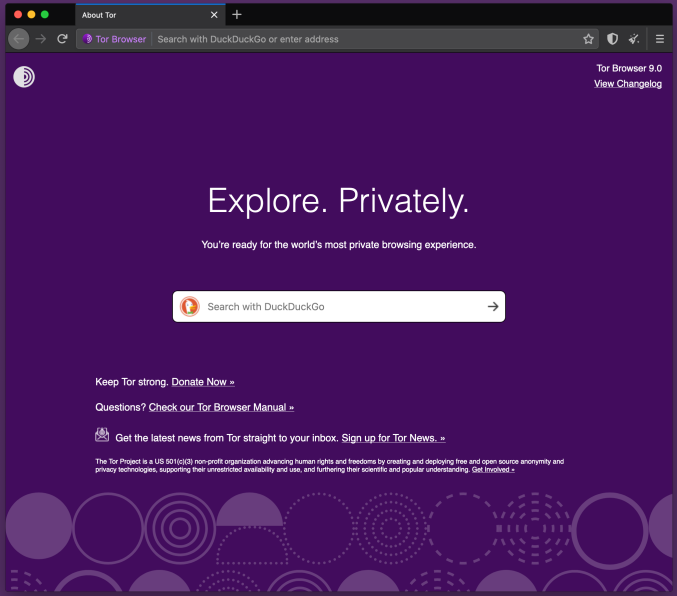
- Online anonymity, and censorship circumvention.
  - Free software.
  - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.

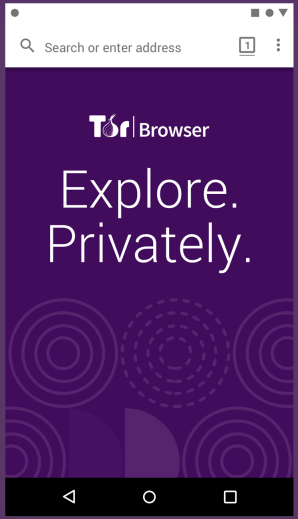


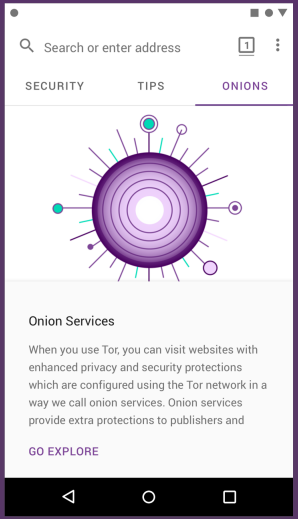
History

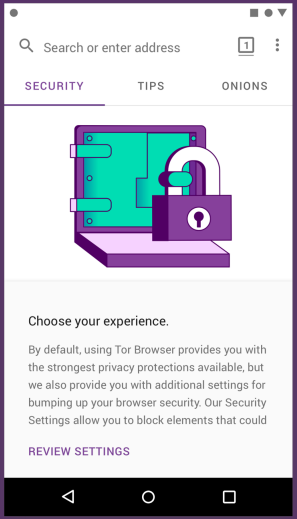
Early 2000s	Working with the U.S. Naval Research Laboratory.
2004	Sponsorship by the Electronic Frontier Foundation.
2006	The Tor Project, Inc. became a non-profit.
2007	Expansion to anti-censorship.
2008	Tor Browser development.
2010	The Arab spring.
2013	The summer of Snowden.
2018	Anti-censorship team created.
2020	Network Health team created.

Somewhere between 2,000,000 and 8,000,000 daily users.

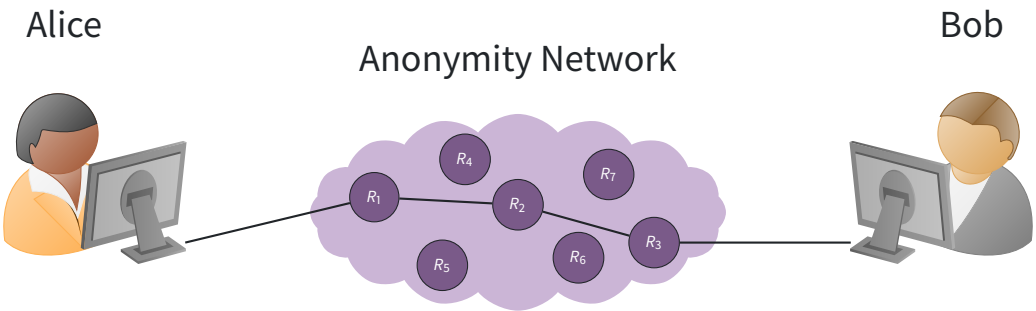

About Tor
Tor Browser
Search with DuckDuckGo or enter address
Tor Browser 9.0
View Changelog
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Keep Tor strong. Donate Now »
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »


Search or enter address
Tor Browser
Explore.
Privately.


Search or enter address
SECURITY
TIPS
ONIONS
Onion Services
When you use Tor, you can visit websites with enhanced privacy and security protections which are configured using the Tor network in a way we call onion services. Onion services provide extra protections to publishers and
GO EXPLORE

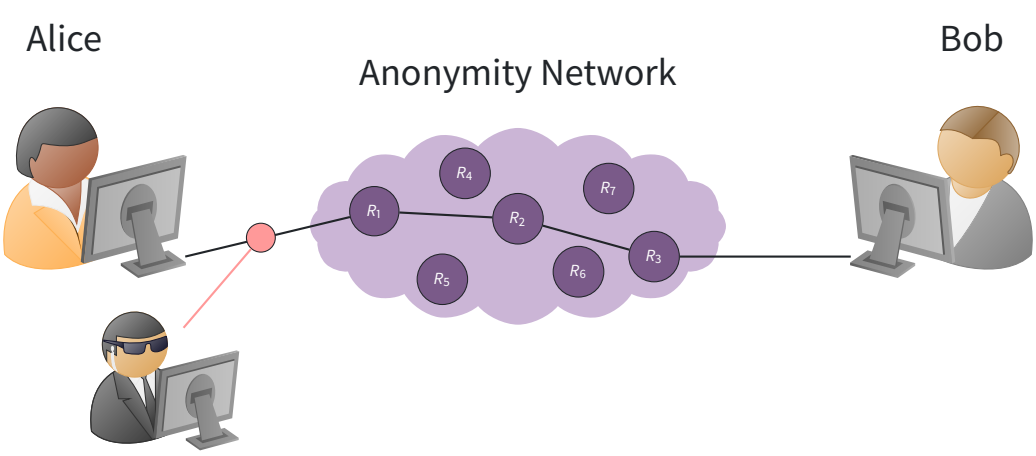

Search or enter address
SECURITY
TIPS
ONIONS
Choose your experience.
By default, using Tor Browser provides you with the strongest privacy protections available, but we also provide you with additional settings for bumping up your browser security. Our Security Settings allow you to block elements that could
REVIEW SETTINGS

Threat Model

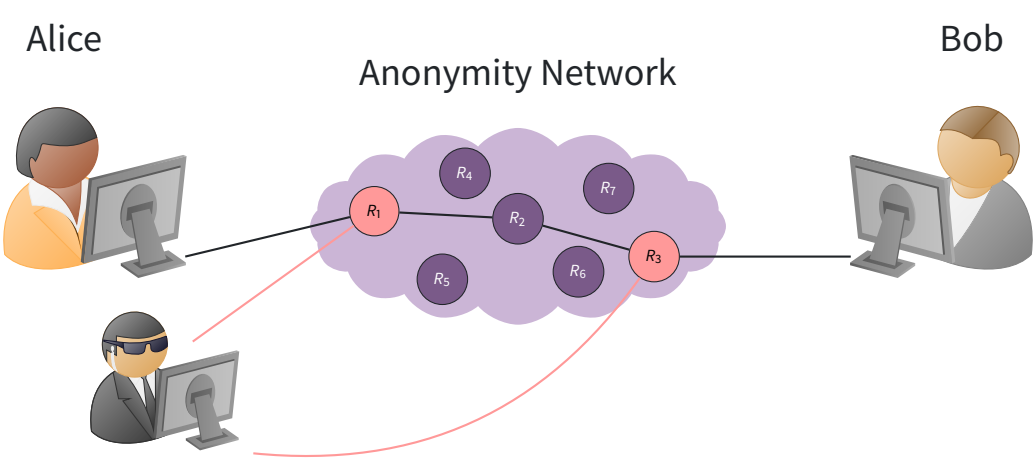


What can the attacker do?

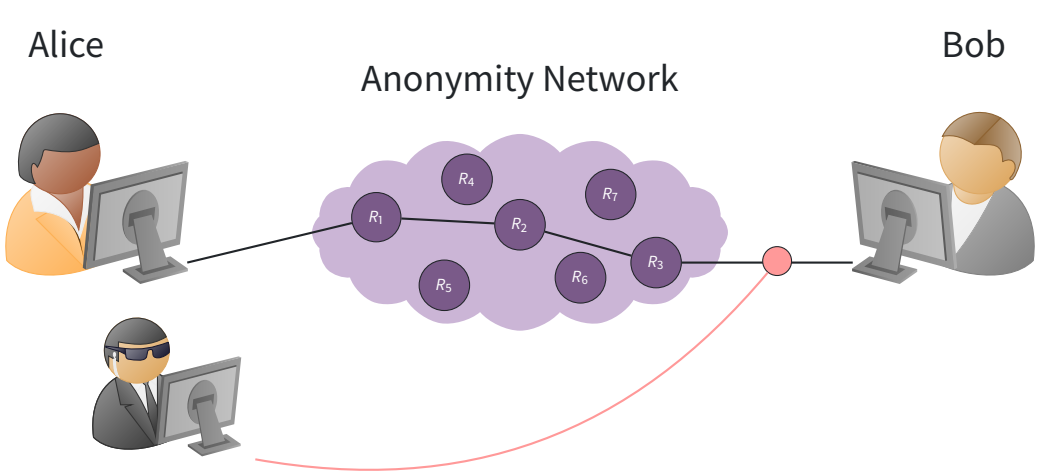
Threat Model



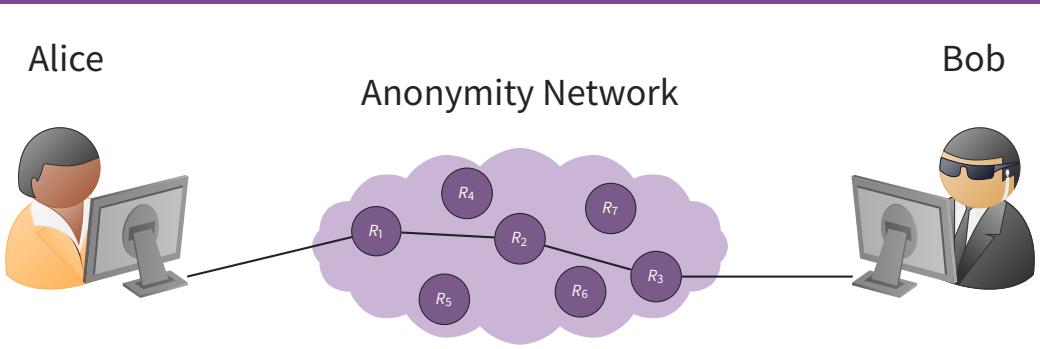
Threat Model



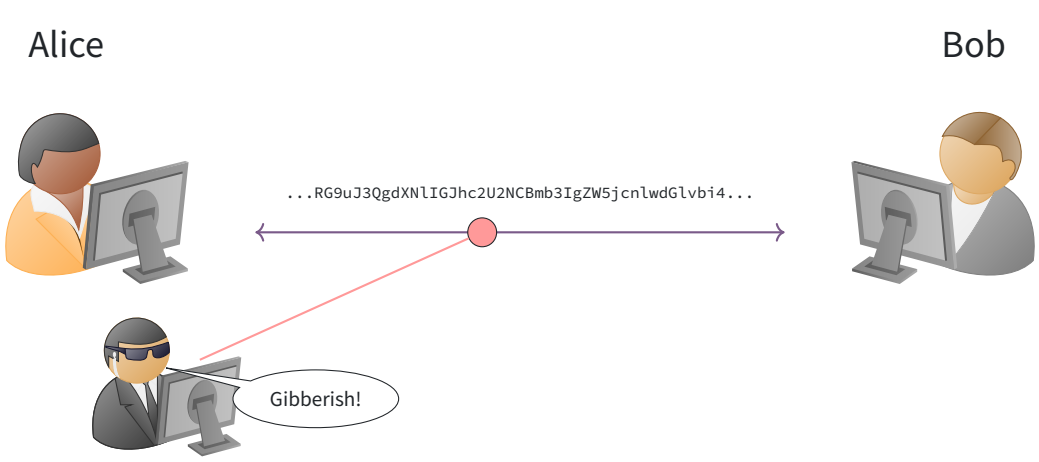
Threat Model



Threat Model



Anonymity isn't Encryption



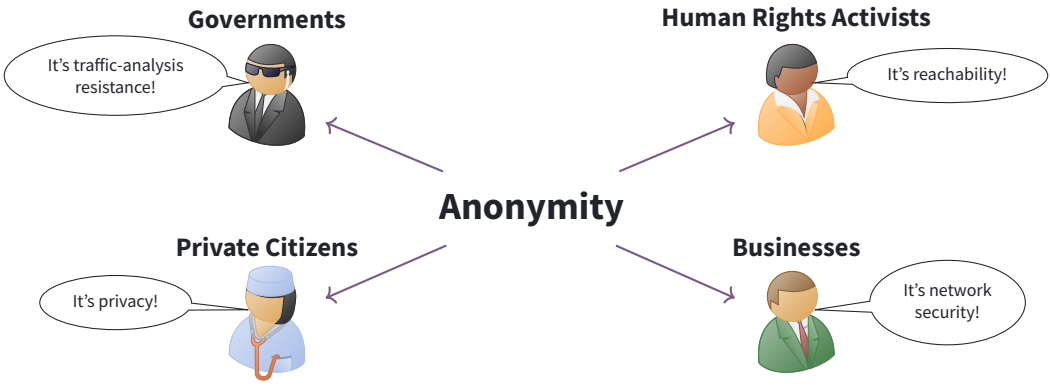
Encryption just protects contents.

Metadata

"We Kill People Based on Metadata."

—Michael Hayden, former director of the NSA.

Different Purposes of Anonymity



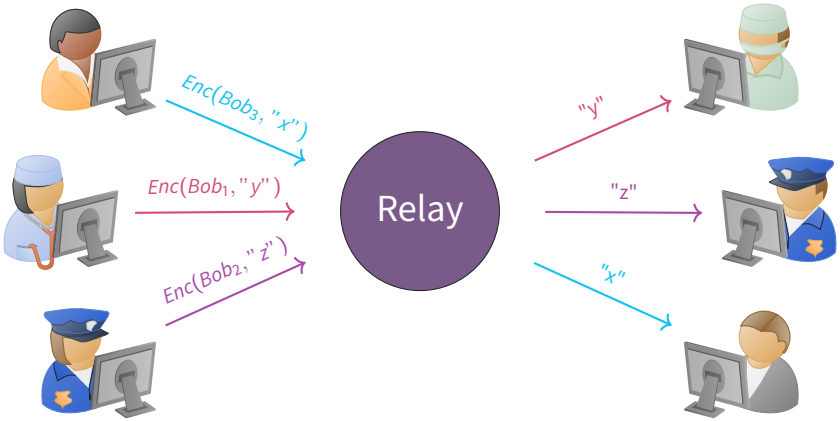
I'm a political activist, part of a semi-criminalized minority. In my younger years I entered the public debate openly, and as a result got harassed by government agencies. I later tried to obfuscate my identity, but I found that my government has surprisingly broad powers to track down dissidents.

Only by using anonymizing means, among which Tor is key, can I get my message out without having police come to "check my papers" in the middle of the night. **Tor allows me freedom to publish my message to the world without being personally persecuted for it.**

Being a dissident is hard enough, privacy is already heavily curtailed, so anonymized communication is a godsend.

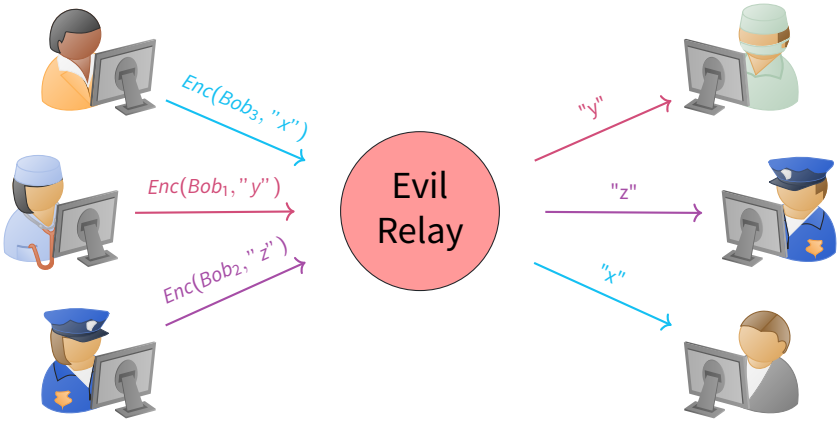
—Anonymous Tor User.

A Simple Design

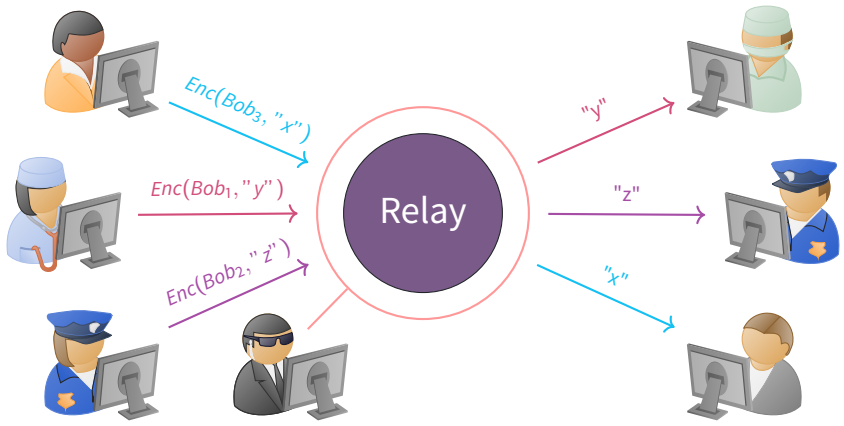


Equivalent to some commercial proxy providers.

A Simple Design

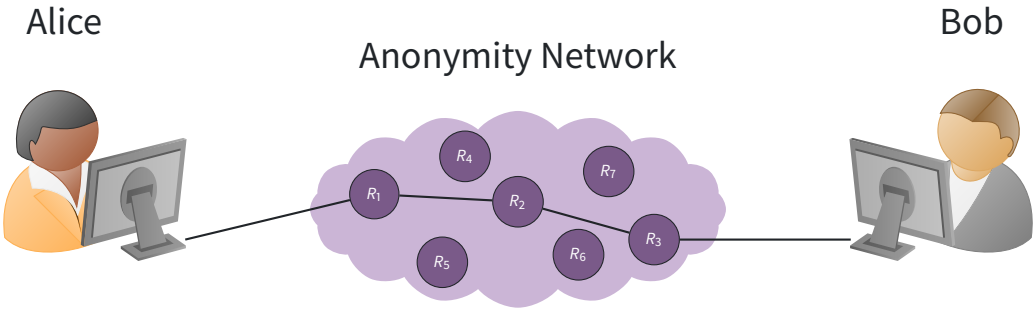


A Simple Design



Timing analysis bridges all connections going through the relay.

The Tor Design



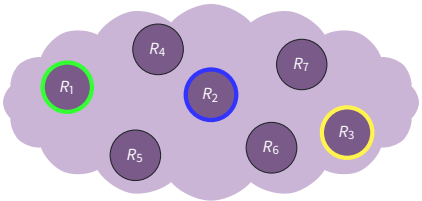
Add multiple relays so that no single relay can betray Alice.

The Tor Design

Alice

Anonymity Network

Bob



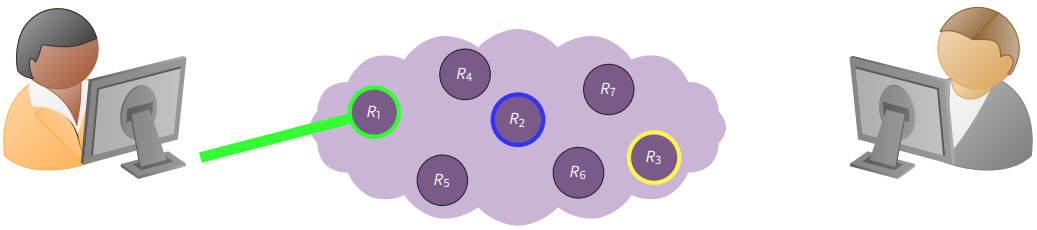
Alice picks a path through the network: R_1, R_2, and R_3 before finally reaching Bob.

The Tor Design

Alice

Anonymity Network

Bob



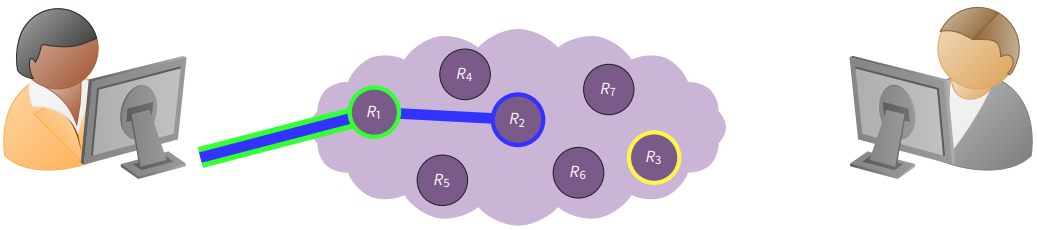
Alice makes a session key with R_1.

The Tor Design

Alice

Anonymity Network

Bob



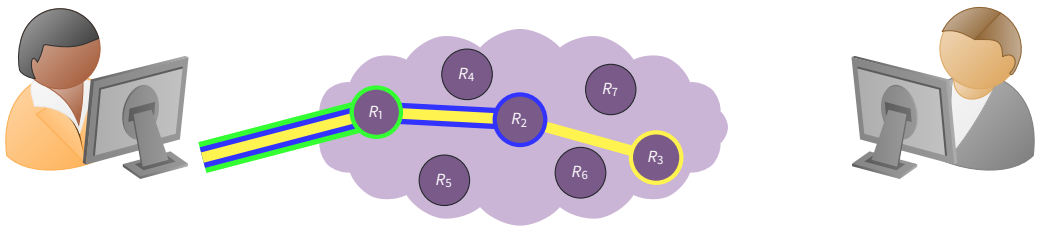
Alice asks R_1 to extend to R_2.

The Tor Design

Alice

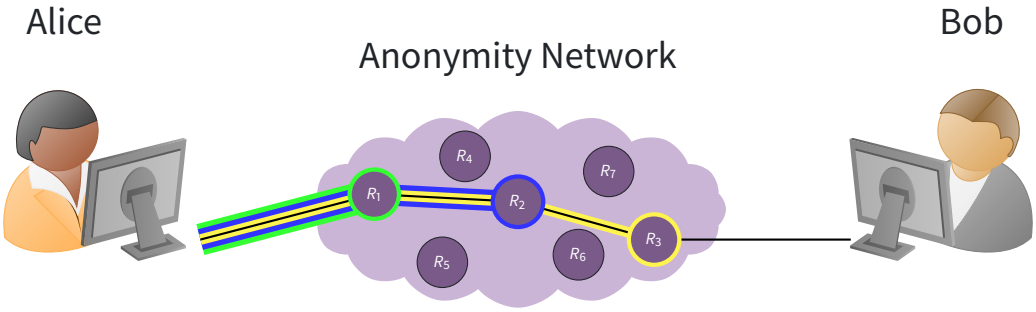
Anonymity Network

Bob



Alice asks R_2 to extend to R_3.

The Tor Design

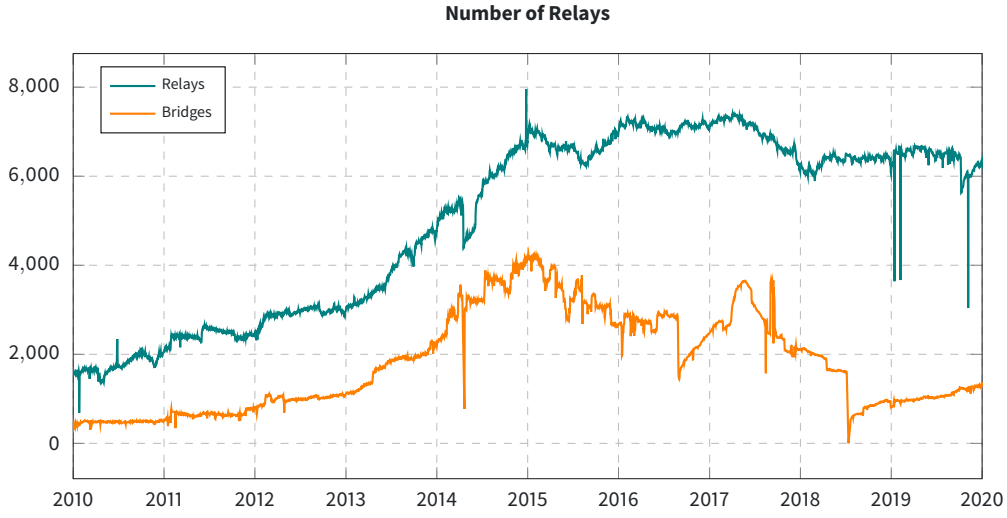


Alice finally asks R_3 to connect to Bob.

The Tor Network

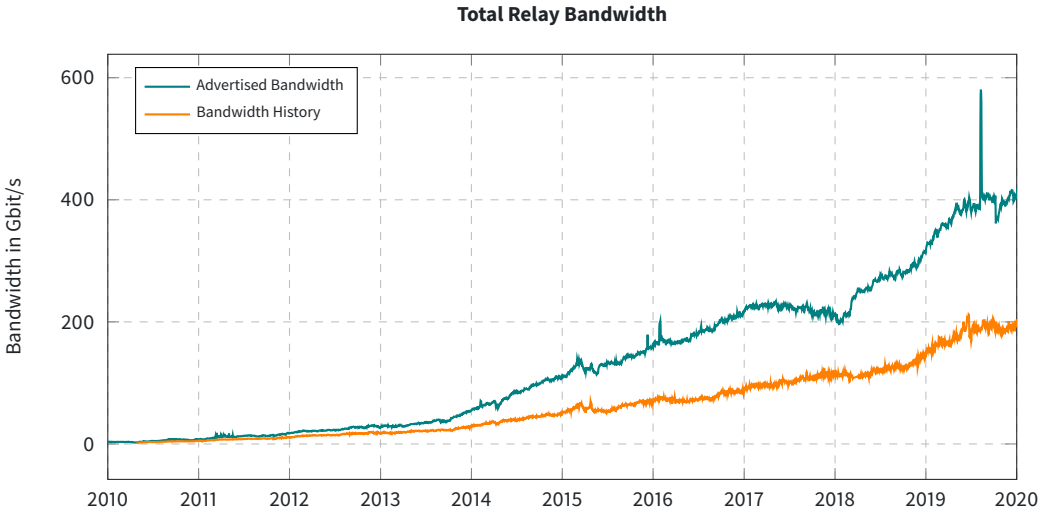
- An open network – everybody can join!
- Between 6000 and 7000 relay nodes.
- Kindly hosted by various individuals, companies, and non-profit organisations.
- 9 Directory Authority nodes and 1 Bridge Authority node.

The Tor Network



Source: metrics.torproject.org

The Tor Network



Source: metrics.torproject.org

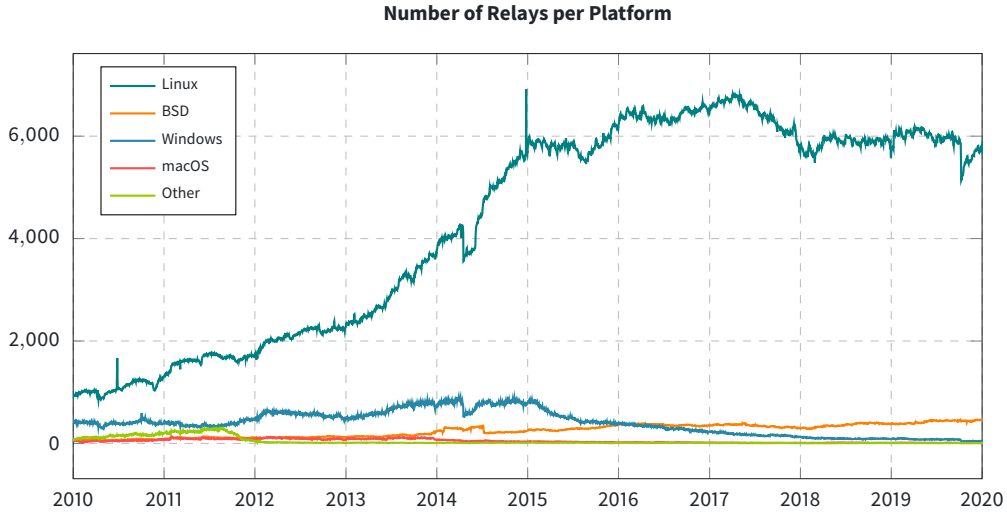
The Tor Network

Tor's **safety** comes from **diversity**:

1. Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation.
2. Diversity of users and reasons to use it. 50,000 users in Iran means almost all of them are normal citizens.

Research problem: How do we measure diversity over time?

The Tor Network



Source: metrics.torproject.org

I live in Iran and I have been using Tor for censorship circumvention. During political unrest while the government tightens grip on other censorship circumvention alternatives, **Tor with obfuscation plugins remains the only solution.**

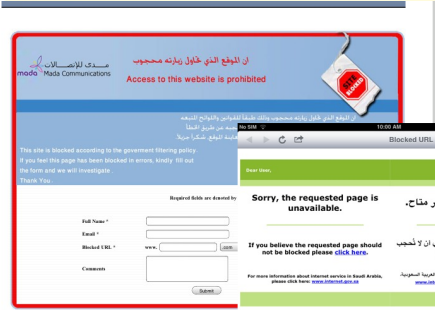
Tor changed my personal life in many ways. **It made it possible to access information on Youtube, Twitter, Blogger and countless other sites.** I am grateful of Tor project, people working on it as well as people running Tor nodes.

—Anonymous Tor User.

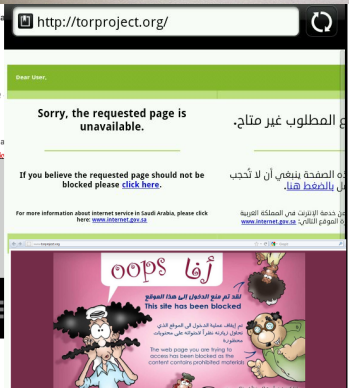

يالله بالستر ...!
تصفح بأمان!
عذراً، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الانترنت وسيلة لتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي تريد بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة 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

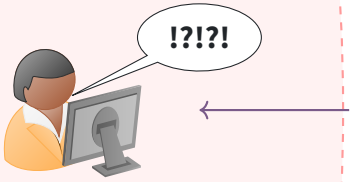
Hjemmesiden er blevet blokeret, fordi den er dømt ulovlig ved en dansk domstol. Brug Share With Care til at finde det, du leder efter, lovligt. På den måde passer du både på dig selv og på kulturen. **Læs mere om Share With Care**

Introduction to Censorship

Censored Region

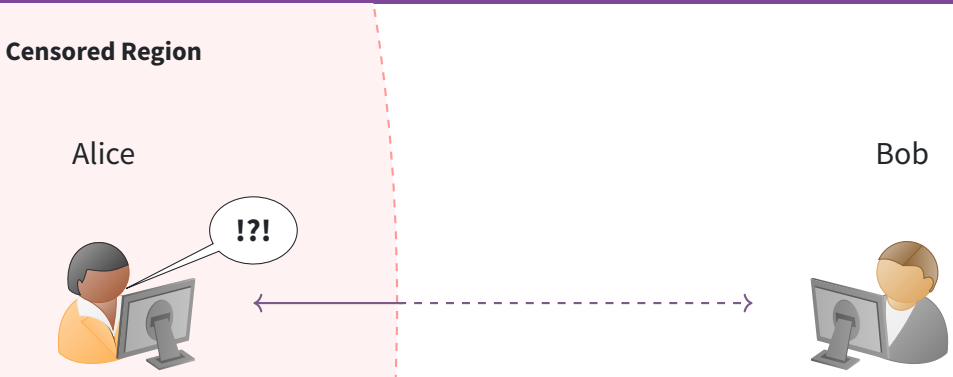
Alice

Bob



Alice is unable to reach Bob.

Introduction to Censorship



Alice can reach Bob, but their connection is throttled.

Introduction to Censorship

Censored Region

Alice

Bob

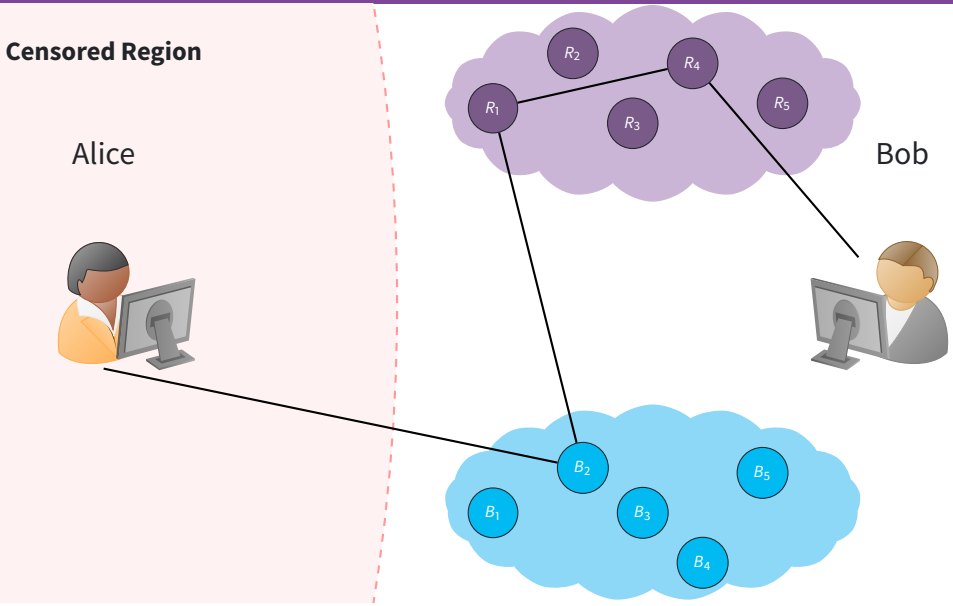
Alice can reach Bob because the censor thinks Bob is fine.

Anti-censorship Strategies

1. Censors will apply censorship to **all** relays in the network and effectively block access to the Tor network.
2. Censors will apply censorship to **known** bridges.

Solution: We make it difficult to find and block bridges and we make it difficult to learn if a given connection is between a Tor user and an entry-point into the Tor network.

Bridges



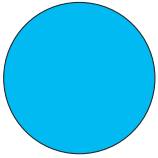
Bridges

Censored Region

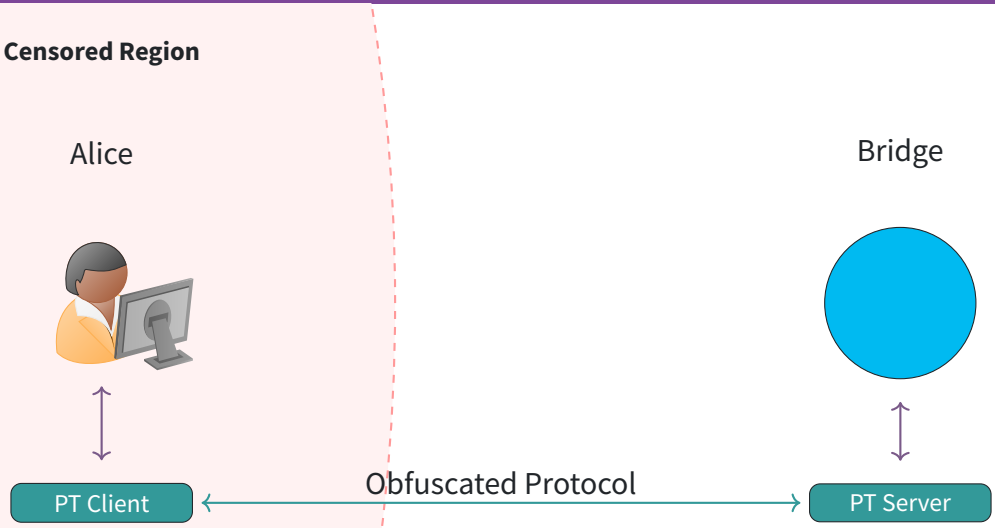
Alice

Tor Protocol

Bridge



Bridges and Pluggable Transports



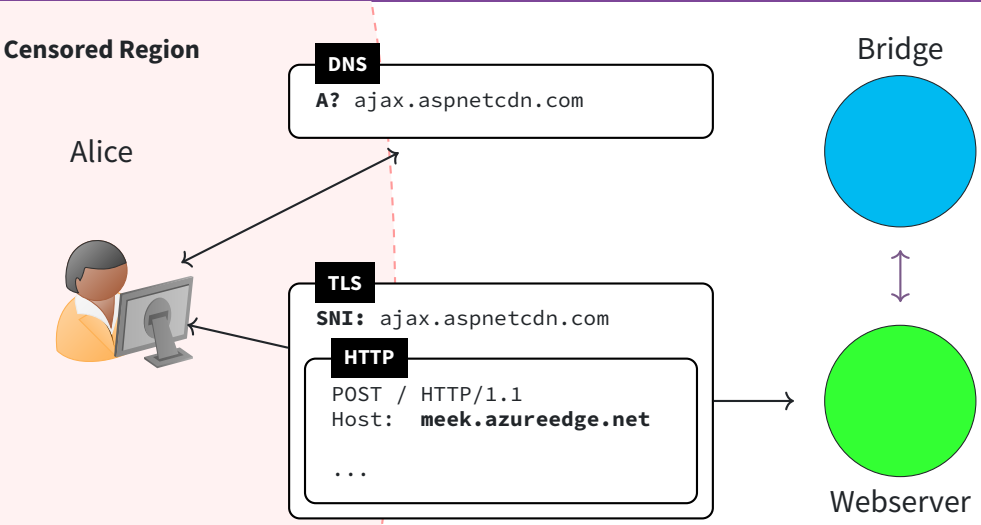
Pluggable Transports

- Allows people to easily build, experiment, and deploy their own obfuscation technology without having to modify the Tor source code itself.
- The specification for Pluggable Transports is open and allows other vendors to implement support for PTs in their own products.
- Allows people to experiment with different transports for Tor that might not be doing any anti-censorship related obfuscation.

Obfourscator (obfs4)

- Makes it hard for passive DPI to verify the presence of the obfs4 protocol unless the adversary knows the bridge parameters.
- Makes active probing hard unless the adversary knows the bridge parameters.
- Uses Tor's ntor handshake (x25519), but uses Elligator2 to encode the elliptic-curve points to be indistinguishable from uniform random strings. The link layer encryption uses NaCl secret boxes (XSalsa20 and Poly1305).

SNI Domain Fronting using Meek



SNI Domain Fronting using Meek

Very **efficient**, but **expensive** :-(

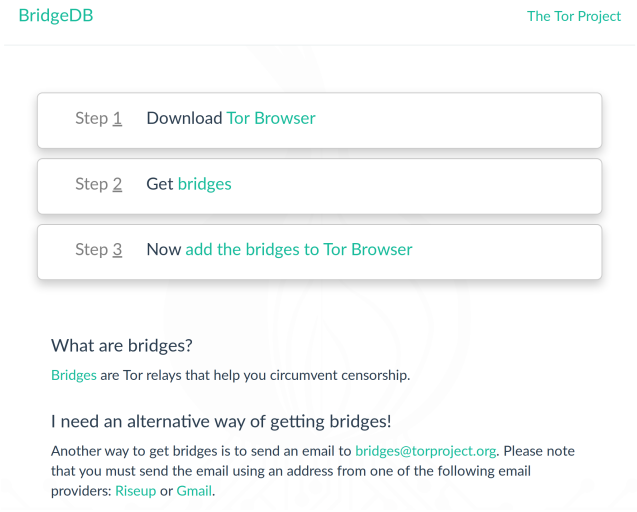
Unpopular with the cloud providers:

Google	Never been a supported feature of Google.
Amazon	Already handled as a breach of AWS ToS.

Domain Fronting in the Future?

- Use Encrypted SNI?
- Use message queue services hosted by the different cloud providers?
- Generally continue to use centralized services to give people in censored areas access.

Bridge Distribution



Source: bridges.torproject.org

Bridge Distribution using Moat

Snowflake

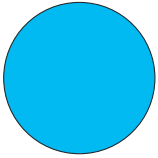
Censored Region

Alice

Snowflake PT Client

Snowflake Broker

Bridge



Snowflake PT Server

Snowflake

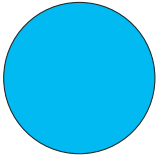
Censored Region

Alice

Snowflake PT Client

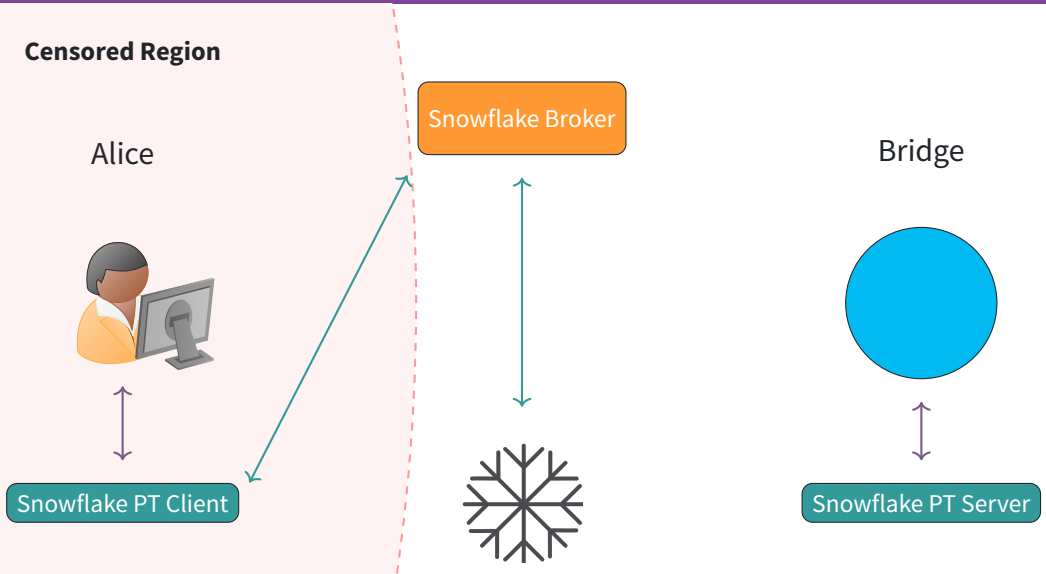
Snowflake Broker

Bridge

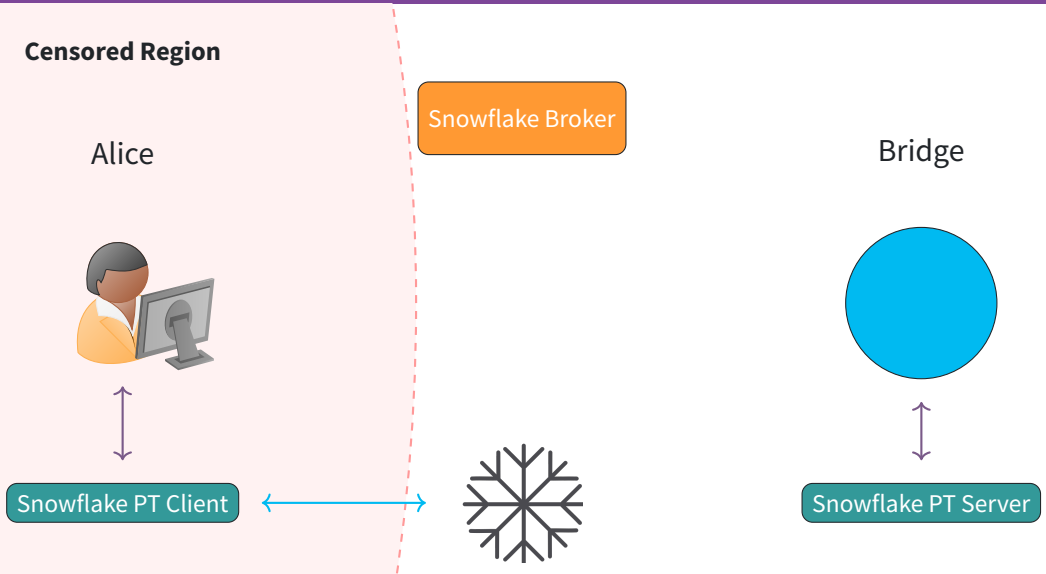


Snowflake PT Server

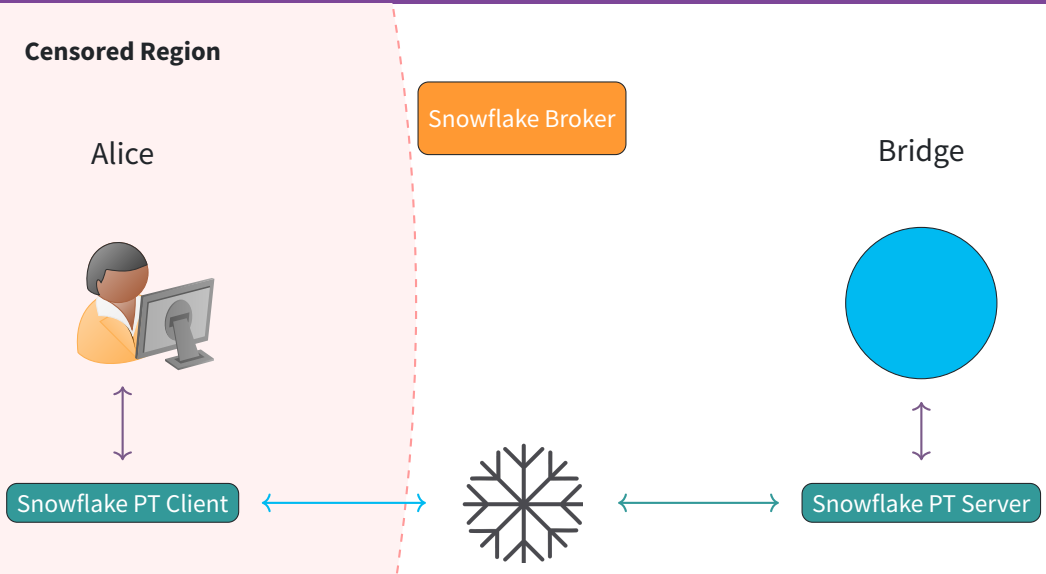
Snowflake


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

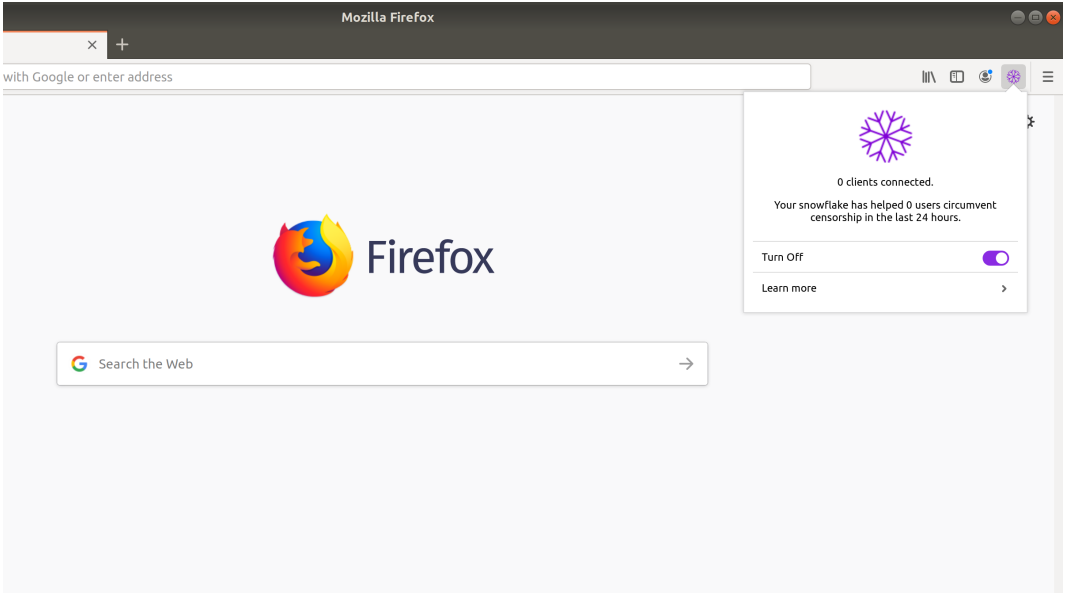
Snowflake


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

Snowflake

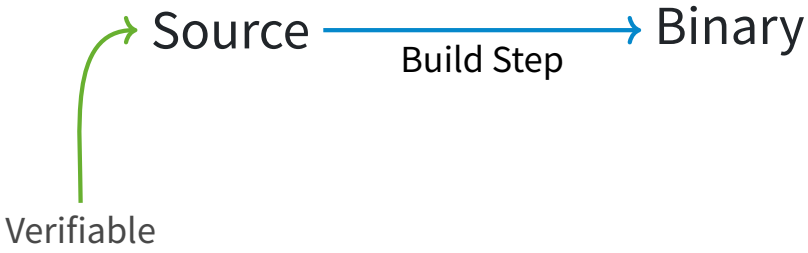

Censored Region
Snowflake Broker
Alice
Bridge
Snowflake PT Client
Snowflake PT Server

Snowflake

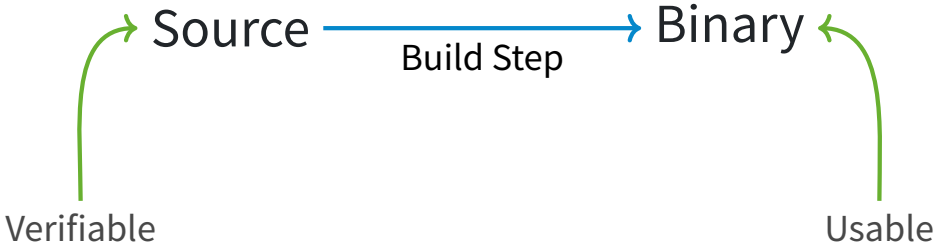

Mozilla Firefox
with Google or enter address
0 clients connected.
Your snowflake has helped 0 users circumvent censorship in the last 24 hours.
Turn Off
Learn more
Firefox
Search the Web

Reproducible Builds

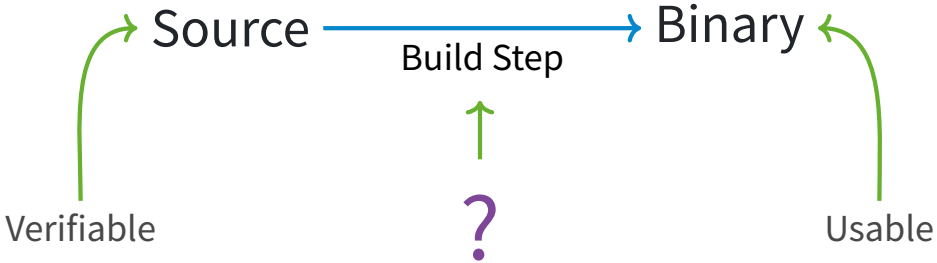
Reproducible Builds



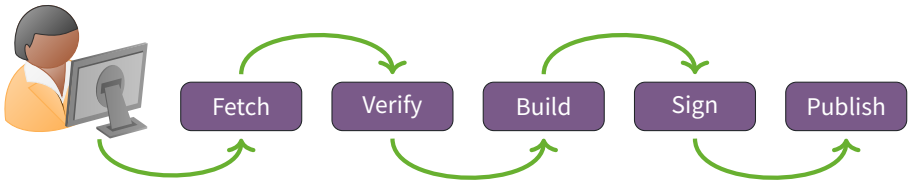
Reproducible Builds



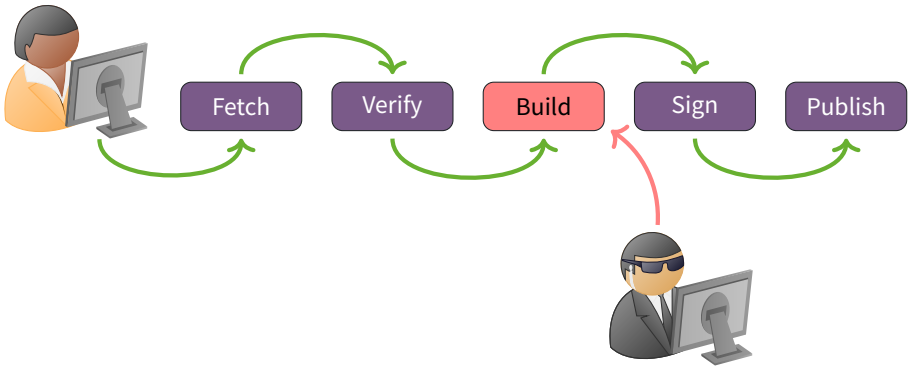
Reproducible Builds



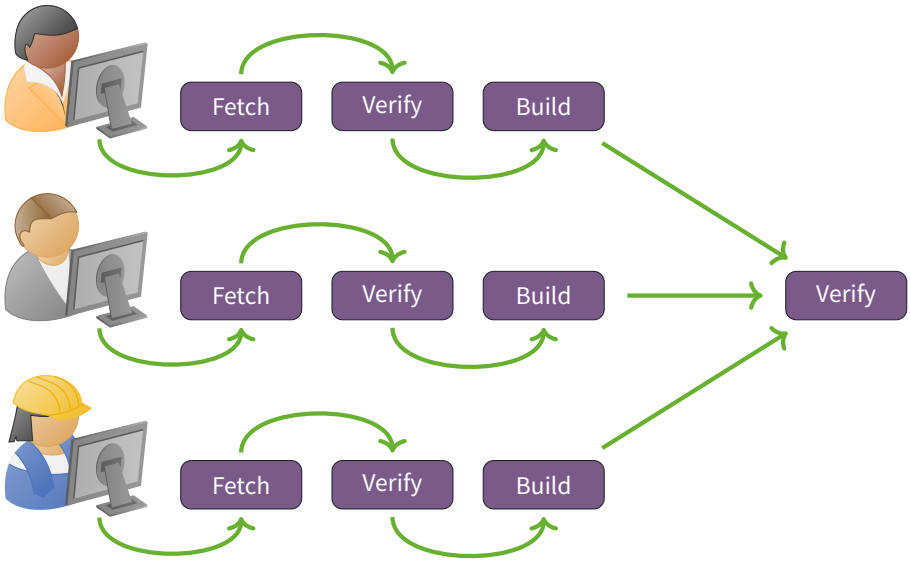
Build Process



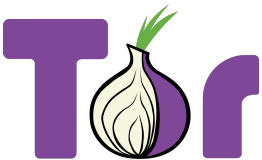
Build Process



Build Process



Reproducible Builds



Reproducible Builds Workflow

#29510 closed task (fixed)

Opened at 2019-02-15T11:18:49+01:00
Closed at 2019-02-23T10:05:18+01:00
Last modified at 2019-02-27T12:18:01+01:00

Check reproducibility of the build of 8.5a8

Reported by:	boklm	Owned by:	tbb-team
Priority:	Very High	Milestone:	
Component:	Applications/Tor Browser	Version:	
Severity:	Normal	Keywords:	
Cc:	pospeselr	Actual Points:	
Parent ID:		Points:	
Reviewer:		Sponsor:	

Description

I did the build of 8.5a8 that we are releasing:

↳ Reply – Delete

https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.txt
https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.txt-boklm.asc

https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.incrementals.txt
https://dist.torproject.org/torbrowser/8.5a8/sha256sums-unsigned-build.incrementals.txt-boklm.asc

In order to verify that the build of this release is reproducible, we need a second person to do a build. We usually do that before publishing a release. However we are having some delay doing it this time, and because this release includes an important security fix, we will be doing this verification after the release is published.

Reproducible Builds Workflow

Changed at 2019-02-27T12:02:14+01:00 by boklm

comment:2 follow-up: ↓ 3

pospeselr mentioned his build was matching, except the `mar-tools-mac64.zip` file.

I uploaded there the `mar-tools-mac64.zip` he sent me:
https://people.torproject.org/~boklm/bug_29510/mar-tools-mac64.zip

And the diff from diffoscope:
https://people.torproject.org/~boklm/bug_29510/mar-tools.diff

Reproducible Builds Workflow

```
--- mar-tools-mac64.zip
+++ /home/boklm/tor-browser-build/alpha/unsigned/8.5a8/mar-tools-mac64.zip
  zipinfo {}
@@ -1,20 +1,20 @@
-Zip file size: 2049025 bytes, number of entries: 18
+Zip file size: 2049012 bytes, number of entries: 18
 drwx------  3.0 unx        0 b- stor 19-Feb-12 08:50 mar-tools/

  [...]

--rwx------  3.0 unx    50216 b- defN 19-Feb-12 08:50 mar-tools/mar
--rwx------  3.0 unx    27112 b- defN 19-Feb-12 08:50 mar-tools/mbsdiff
+-rwx------  3.0 unx    50208 b- defN 19-Feb-12 08:50 mar-tools/mar
+-rwx------  3.0 unx    27104 b- defN 19-Feb-12 08:50 mar-tools/mbsdiff

  [...]

-18 files, 4637421 bytes uncompressed, 2046841 bytes compressed:  55.9%
+18 files, 4637405 bytes uncompressed, 2046828 bytes compressed:  55.9%
```

Reproducible Builds Workflow

```
readelf --wide --hex-dump=.strtab {}
@@ -2,15 +2,15 @@
 Hex dump of section '.strtab':
   0x00000000 00637274 73747566 662e6300 5f5f4a43 .crtstuff.c.__JC
   0x00000010 525f4c49 53545f5f 00646572 65676973 R_LIST__.deregis
   0x00000020 7465725f 746d5f63 6c6f6e65 73007265 ter_tm_clones.re
   0x00000030 67697374 65725f74 6d5f636c 6f6e6573 gister_tm_clones
   0x00000040 005f5f64 6f5f676c 6f62616c 5f64746f .__do_global_dto
   0x00000050 72735f61 75780063 6f6d706c 65746564 rs_aux.completed
-  0x00000060 2e363637 30005f5f 646f5f67 6c6f6261 .6670.__do_globa
+  0x00000060 2e363636 31005f5f 646f5f67 6c6f6261 .6661.__do_globa
   0x00000070 6c5f6474 6f72735f 6175785f 66696e69 l_dtors_aux_fini
   0x00000080 5f617272 61795f65 6e747279 00667261 _array_entry.fra
   0x00000090 6d655f64 756d6d79 005f5f66 72616d65 me_dummy.__frame
   0x000000a0 5f64756d 6d795f69 6e69745f 61727261 _dummy_init_arra
   0x000000b0 795f656e 74727900 2f766172 2f746d70 y_entry./var/tmp
   0x000000c0 2f627569 6c642f66 69726566 6f782d35 /build/firefox-5
   0x000000d0 38613433 39646434 6536662f 6d6f6475 8a439dd4e6f/modu
```

Reproducible Builds Workflow

```
readelf --wide --string-dump=.comment {}
@@ -1,6 +1,6 @@

 String dump of section '.comment':
-  [     0]  GCC: (Debian 4.9.2-10+deb8u1) 4.9.2
-  [    24]  clang version 3.9.1 (tags/RELEASE_391/final)
-  [    51]  GCC: (Debian 4.8.4-1) 4.8.4
+  [     0]  GCC: (Debian 4.9.2-10) 4.9.2
+  [    1d]  clang version 3.9.1 (tags/RELEASE_391/final)
+  [    4a]  GCC: (Debian 4.8.4-1) 4.8.4
```

Reproducible Builds Problems

Common problems includes:

- Timestamps as part of the build process.
- Usernames.
- Locale settings.
- Host settings (such as hostname and IP).

Tor is not foolproof

- Browser metadata fingerprinting.
- Browser exploits.
- Traffic analysis.
- Operational security mistakes.

How can you help?

Help test our Alpha releases

torproject.org/download/alpha/

How can you help?

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

Questions?

@ahfaeroey

ahf@torproject.org

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