

Anti-censorship with Tor

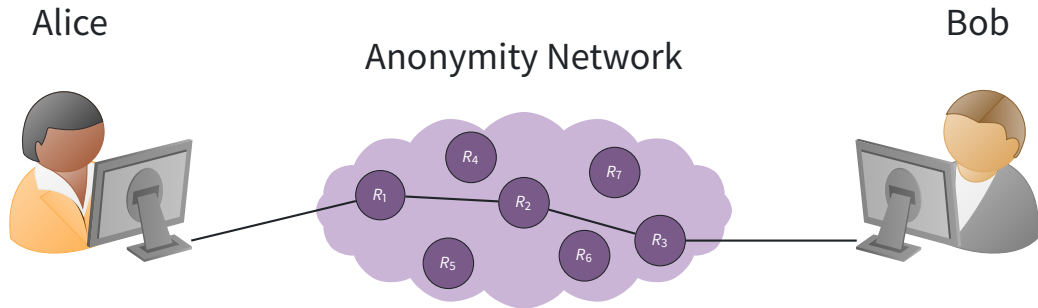
Alexander Færøy

November 10, 2019

Freedom not Fear

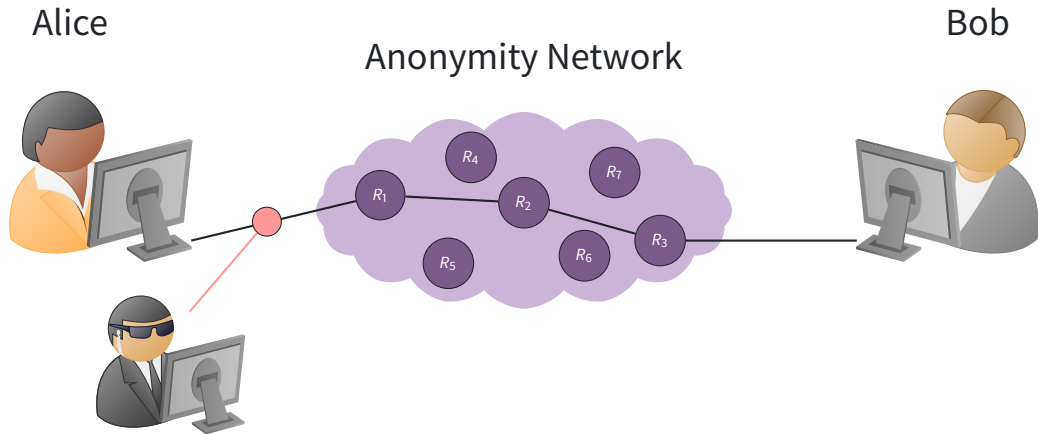


Threat Model

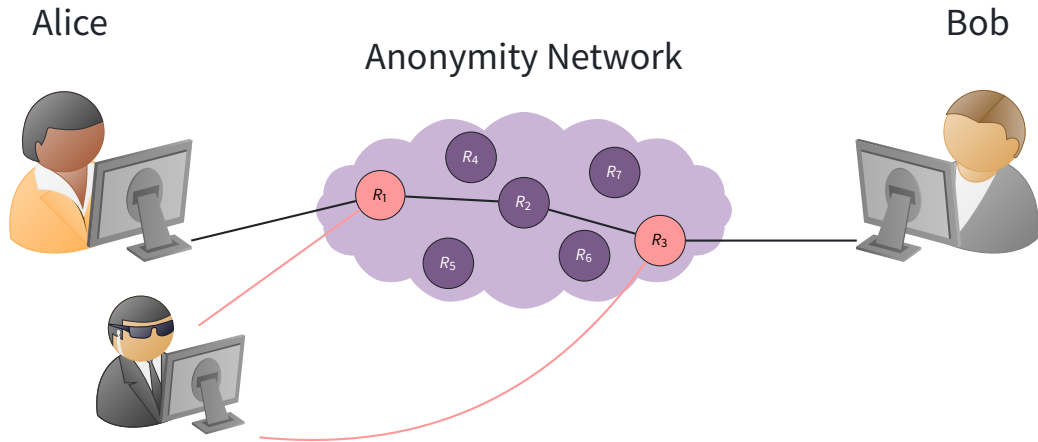


What can the attacker do?

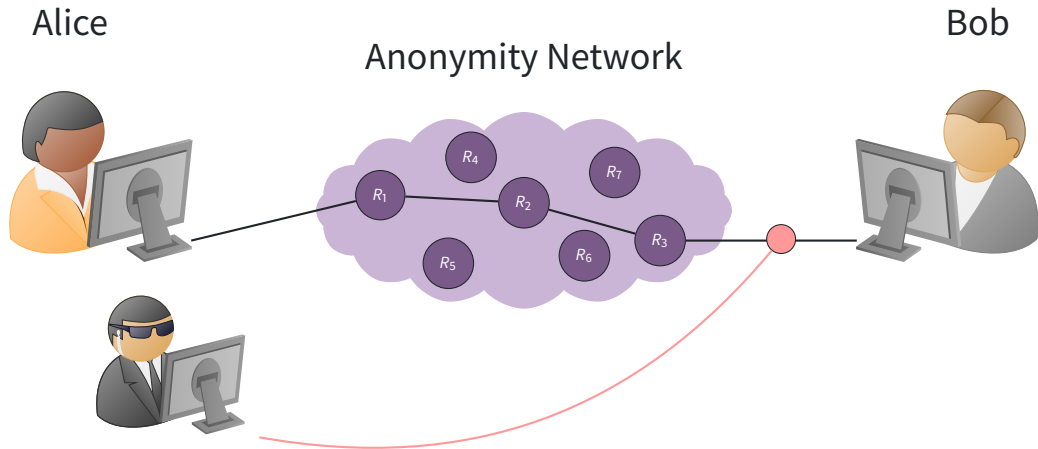
Threat Model



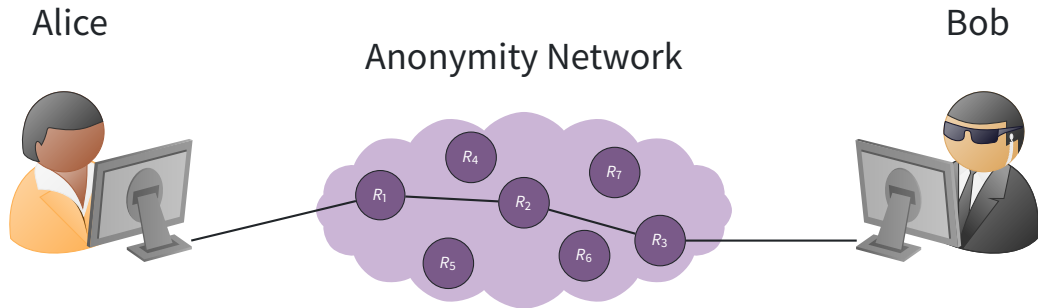
Threat Model



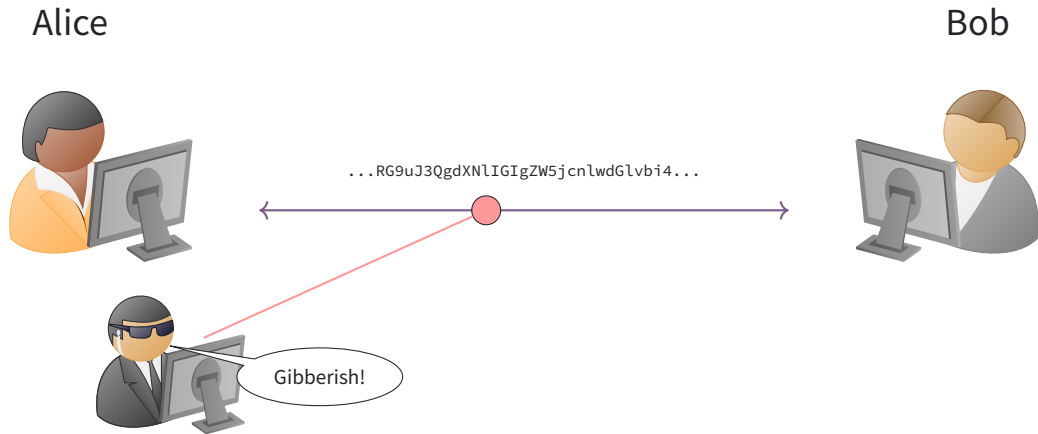
Threat Model



Threat Model



Anonymity isn't Encryption



Encryption just protects contents.

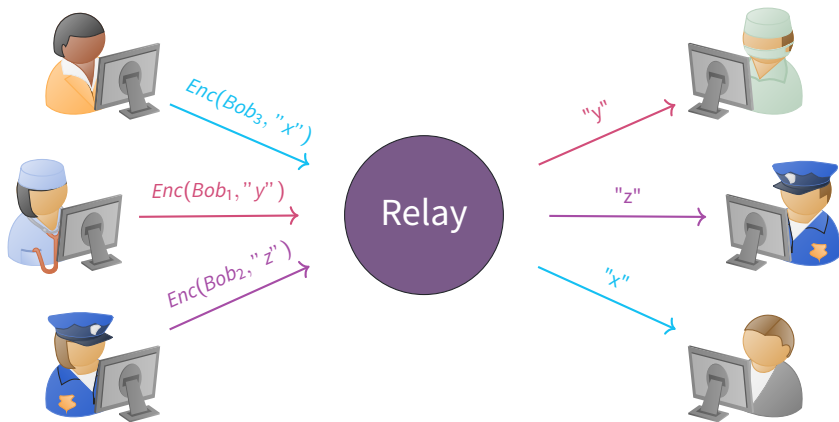
Metadata



"We Kill People Based on Metadata."

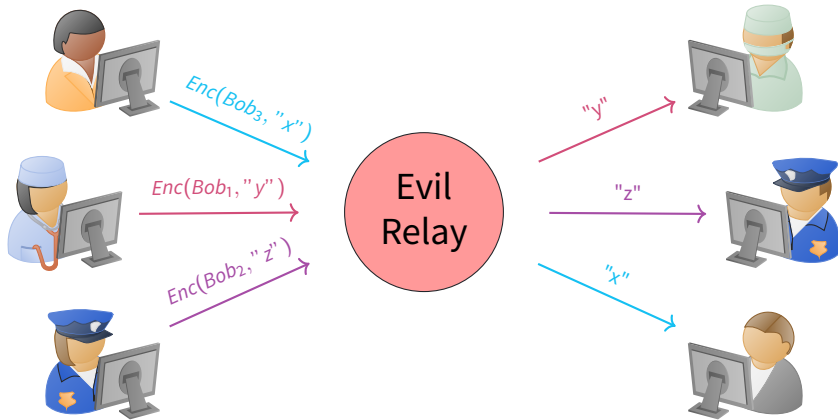
—Michael Hayden, former director of the NSA.

A Simple Design

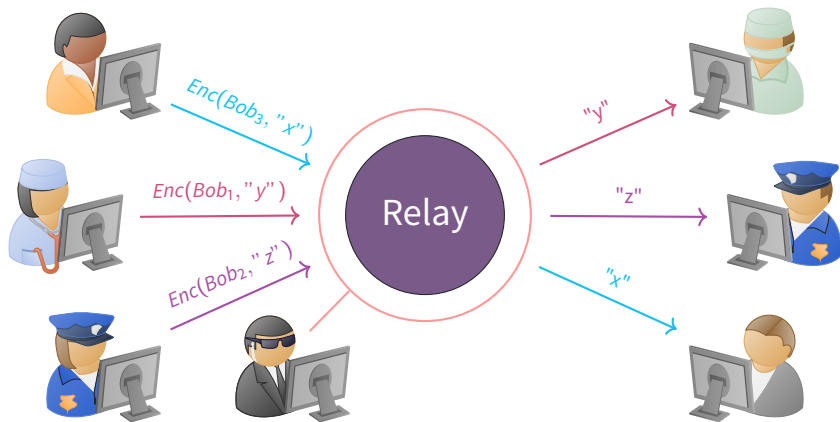


Equivalent to some commercial proxy providers.

A Simple Design

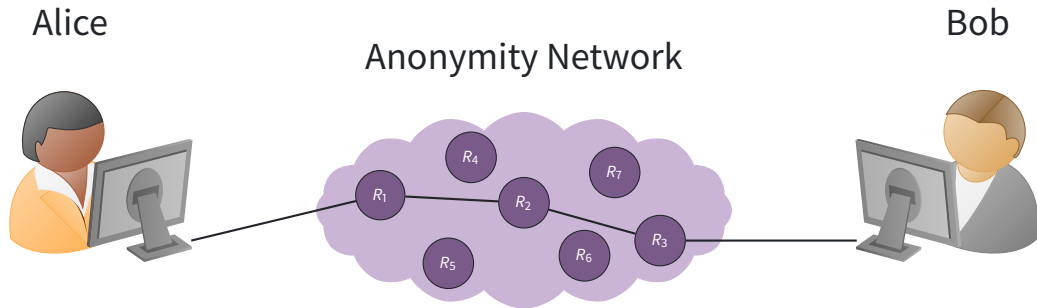


A Simple Design



Timing analysis bridges all connections going through the relay.

The Tor Design



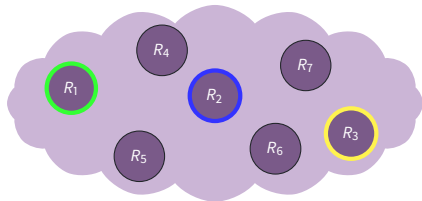
Add multiple relays so that no single relay can betray Alice.

The Tor Design

Alice



Anonymity Network



Bob



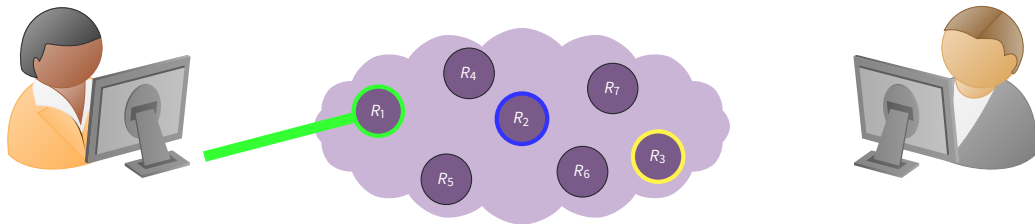
Alice picks a path through the network: R_1 , R_2 , and R_3 before finally reaching Bob.

The Tor Design

Alice

Bob

Anonymity Network



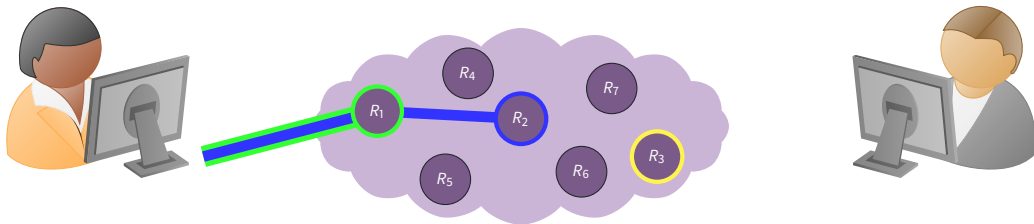
Alice makes a session key with R_1 .

The Tor Design

Alice

Anonymity Network

Bob



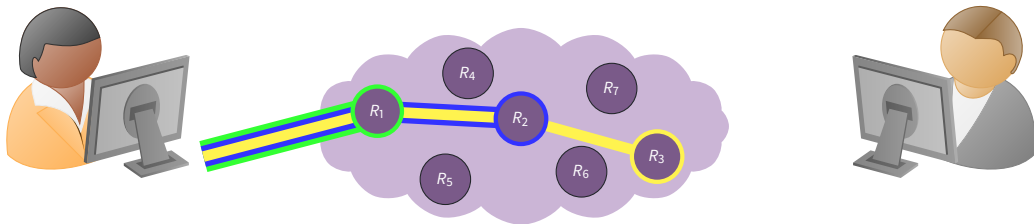
Alice asks R_1 to extend to R_2 .

The Tor Design

Alice

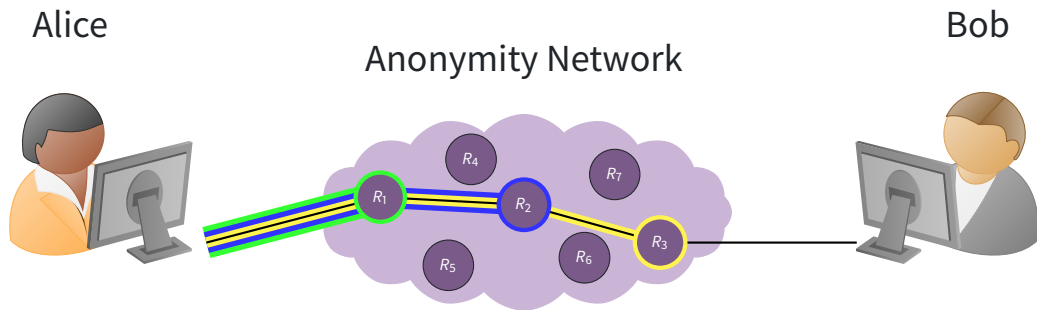
Anonymity Network

Bob



Alice asks R_2 to extend to R_3 .

The Tor Design



Alice finally asks R_3 to connect to Bob.

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!

عزيزي، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تتشكل شبكة الإنترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مرع لحد "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النظم للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كنت لديك وجهة نظر مختلفة، الرجاء انقر 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](#).



خطراً!

تصفح بأمان!

عزيزي، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الإنترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مرع لحد "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النظم للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كنت لديك وجهة نظر مختلفة، الرجاء انقر 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](#).



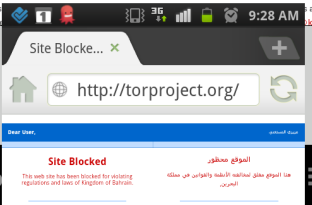
Access Denied

Your request was denied because of its content categorization: "Computers/Internet/Proxy Avoidance"

عزيزي العميل : تم حجب هذا الموقع بناء على القوانين

بأن هناك خطأ يرجى إرسال رسالة على البريد الإلكتروني unblock.kw@kw.zain.com مع ذكر عنوان الموقع الذي تم حجب.

Dear Customer: This site has been blocked for categorizing this site, please



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 محظور لانتهاكه الأنظمة والقوانين في مملكة البحرين.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

<http://torproject.org/>

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

هذه الصفحة ينبغي أن لا تحجب بل بالضغط هنا.

خدمة الإنترنت في المملكة العربية السعودية: www.internet.gov.sa

مبنى للإصالات
mada Mada Communications

ان الموقع الذي تحاول زيارته محظور
Access to this website is prohibited

ان الموقع الذي تحاول زيارته محظور وذلك لأسباب تتعلق بالسياسات والقوانين المعمول بها في دولة الكويت. نرجو من فضلكم تعبئة النموذج التالي لتتمكن من زيارة الموقع بشكل طبيعي.

This site is blocked according to the government filtering policy. If you feel this page has been blocked in error, kindly fill out the form and we will investigate. Thank You

Required fields are marked *

Full Name *

Email *

Blocked URL *

Comments

Submit

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

عذراً، للوفع المطلوب غير متاح.

إن كنت ترى أن هذه الصفحة ينبغي أن لا تحجب فعلياً [انقر هنا](#).

لرأه من المعلومات عن خدمة الإنترنت في المملكة العربية السعودية، يمكنك زيارة الموقع التالي: www.internet.gov.sa

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

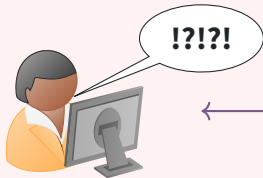
Hjemmesiden er blevet blokeret, fordi den er dømt ulovlig ved en dansk domstol. Brug Share With Care til at finde det, du leder efter, lovligt. På den måde passer du både på dig selv og på kulturen. **Læs mere om Share With Care**

Please email the stop page of your country to
ahf@torproject.org.

Introduction to Censorship

Censored Network

Alice



Bob



Alice is unable to reach Bob.

Introduction to Censorship

Censored Network

Alice



Bob



Alice can reach Bob, but their connection is throttled.

Introduction to Censorship

Censored Network

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.

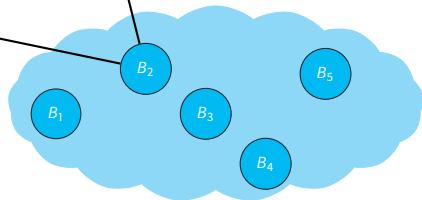
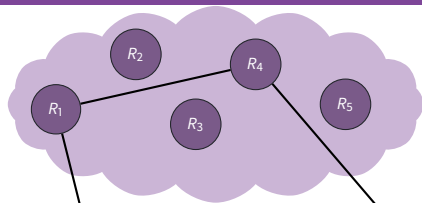
Bridges

Censored Network

Alice



Bob



Bridges

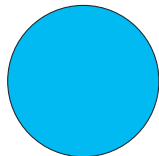
Censored Network

Alice



Tor Protocol

Bridge



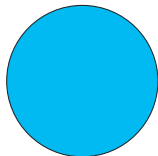
Active Probing Attack

Censored Network

Alice



Bridge



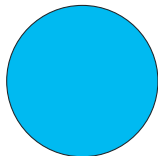
Active Probing Attack

Censored Network

Alice



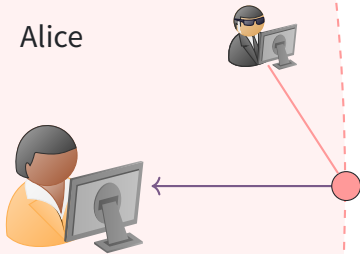
Bridge



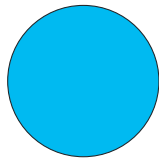
Active Probing Attack

Censored Network

Alice



Bridge



Bridges and Pluggable Transports

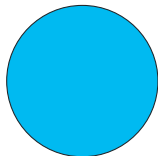
Censored Network

Alice



PT Client

Bridge



PT Server

Obfuscated Protocol



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

Censored Network

Alice



DNS

A? ajax.aspnetcdn.com

TLS

SNI: ajax.aspnetcdn.com

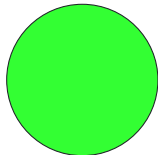
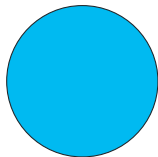
HTTP

POST / HTTP/1.1

Host: **meek.azureedge.net**

...

Bridge



Webserver

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

BridgeDB

The Tor Project

Step 1 Download [Tor Browser](#)

Step 2 Get [bridges](#)

Step 3 Now [add the bridges to Tor Browser](#)

What are bridges?

[Bridges](#) are Tor relays that help you circumvent censorship.

I need an alternative way of getting bridges!

Another way to get bridges is to send an email to bridges@torproject.org. Please note that you must send the email using an address from one of the following email providers: [Riseup](#) or [Gmail](#).

Source: bridges.torproject.org

Bridge Distribution using Moat

☒ Tor is censored in my country

☐ Select a built-in bridge ?

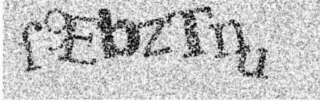
☒ Request a bridge from torproject.org


☐ Provide a bridge I know

☐ I use a proxy to connect to the Internet ?

☐ This computer goes through a firewall that only allows connections to certain ports

Solve the CAPTCHA to request a bridge.



Enter the characters from the image 

Snowflake

Censored Network

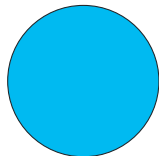
Alice



Snowflake PT Client

Snowflake Broker

Bridge



Snowflake PT Server



Snowflake

Censored Network

Alice

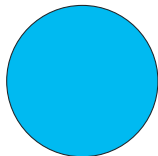


Snowflake PT Client

Snowflake Broker



Bridge



Snowflake PT Server

Snowflake

Censored Network

Alice

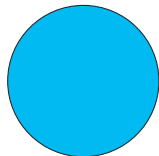


Snowflake PT Client

Snowflake Broker



Bridge



Snowflake PT Server

Snowflake

Censored Network

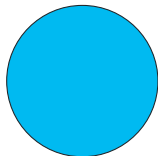
Alice



Snowflake PT Client

Snowflake Broker

Bridge



Snowflake PT Server



Snowflake

Censored Network

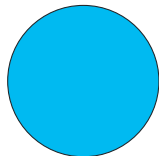
Alice



Snowflake PT Client

Snowflake Broker

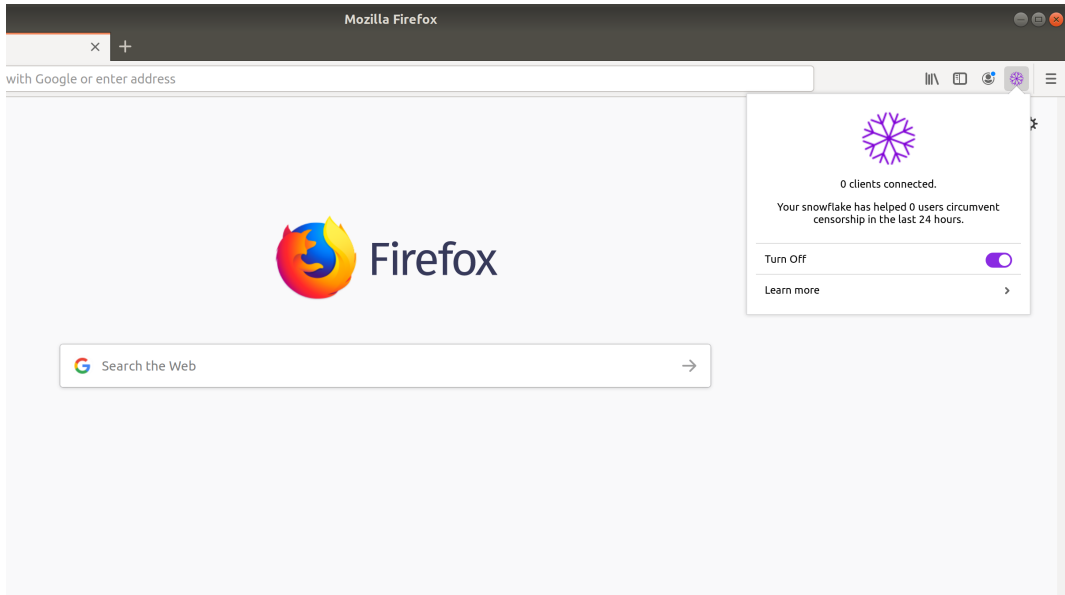
Bridge



Snowflake PT Server



Snowflake



Open discussion



This work is licensed under a
Creative Commons
Attribution-ShareAlike 4.0 International License

